



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: General Services Administration (GSA) Office of Inspector General (OIG) Policy and Procedures Manual, 2017

Requested date: 03-June-2018

Release date: 10-August-2018

Posted date: 01-July-2019

Source of document: FOIA Request  
General Services Administration  
OIG FOIA Officer  
1800 F Street, NW  
Room 5324  
Washington 20405  
E-mail: [OIGFOIA-PrivacyAct@gsaig.gov](mailto:OIGFOIA-PrivacyAct@gsaig.gov)  
Fax: 202-501-0414

The governmentattic.org web site ("the site") is a First Amendment free speech web site, and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



U.S. General Services Administration  
Office of Inspector General

---

AUG 10 2018

Re: Freedom of Information Act Request (OIG Tracking Number 18-069)

This is in response to your Freedom of Information Act (FOIA) request submitted online on June 3, 2018, to the General Services Administration Office of Inspector General, for:

“An electronic/digital copy of the GSA Office of Inspector General Policy and Procedures Manual.”

In response to your request, we are providing Chapters 100 through 600 of the OIG Policy Manual. The remaining chapters, 700 through 1000, are still under review. Upon review of the responsive material, I determined you are entitled to a redacted version of the responsive documents under the FOIA. The bases for any redacted information is Exemption 7(E) of the FOIA. Exemption 7(E) of the FOIA, 5 U.S.C. §552 (b)(7)(E), permits the withholding of information compiled for law enforcement purposes, the release of which "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." The OIG's Policy and Procedures Manual is not available on a public website. The manual provided was manually copied from the OIG's internal webpage.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirement of the FOIA. See 5 U.S.C. §552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirement of the FOIA. This is a standard notification that this office provides to all our requesters. You should not take it as an indication that excluded records do, or do not exist.

You have the right to file an administrative appeal within 120 days of the date of this letter. By filing an appeal, you preserve your rights under FOIA and give the agency a chance to review and reconsider your request and the agency's decision. The appeal must be in writing, include the GSA OIG FOIA Case Number (18-069), and contain a statement of

reasons for the appeal. In addition, please enclose copies of the initial request and responsive documents under appeal. The envelope and letter should be clearly marked as a "Freedom of Information Act Appeal" and addressed as follows:

Freedom of Information Act Officer  
Office of the Inspector General, General Services Administration  
1800 F Street, NW, Room 5332  
Washington, D.C. 20405

If you would like to discuss our response before filing an appeal to attempt to resolve your dispute without going through the appeals process, you can contact our FOIA Public Liaison Nancy Olson for assistance at:

Office of the Inspector General, General Services Administration  
1800 F Street, NW, Room 5332  
Washington, D.C. 20405  
(202) 501-1932  
oigfoia-privacyact@gsaig.gov

If you are unable to resolve your FOIA dispute through our FOIA Public Liaison, the Office of Government Information Services (OGIS), the Federal FOIA Ombudsman's office, offers mediation services to help resolve disputes between FOIA requesters and Federal agencies. The contact information for OGIS is:

Office of Government Information Services  
National Archives and Records Administration  
8601 Adelphi Road--OGIS  
College Park, MD 20740-6001  
ogis@nara.gov  
ogis.archives.gov  
202-741-5770  
877-684-6448

Sincerely,



Edward J. Martin  
Counsel to the Inspector General  
(FOIA Officer)

Enclosure



U.S. General Services Administration  
Office of Inspector General

---

**SEP 28 2018**

Re: Freedom of Information Act Request (OIG Tracking Number 18-069)

This is in response to your Freedom of Information Act (FOIA) request submitted online on June 3, 2018, to the General Services Administration Office of Inspector General, for:

“An electronic/digital copy of the GSA Office of Inspector General Policy and Procedures Manual.”

In response to your request, we are providing the remaining Chapters 700 through 1000 of the OIG Policy Manual. We previously provided Chapters 100 through 600 of the OIG Policy Manual on August 10, 2018. Upon review of the responsive material, I determined you are entitled to a redacted version of the responsive documents under the FOIA. The bases for any redacted information is Exemption 7(E) of the FOIA. Exemption 7(E) of the FOIA, 5 U.S.C. §552 (b)(7)(E), permits the withholding of information compiled for law enforcement purposes, the release of which "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." The OIG's Policy and Procedures Manual is not available on a public website. The manual provided was manually copied from the OIG's internal webpage.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirement of the FOIA. See 5 U.S.C. §552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirement of the FOIA. This is a standard notification that this office provides to all our requesters. You should not take it as an indication that excluded records do, or do not exist.

You have the right to file an administrative appeal within 120 days of the date of this letter. By filing an appeal, you preserve your rights under FOIA and give the agency a chance to review and reconsider your request and the agency's decision. The appeal must be in writing, include the GSA OIG FOIA Case Number (18-069), and contain a statement of

reasons for the appeal. In addition, please enclose copies of the initial request and responsive documents under appeal. The envelope and letter should be clearly marked as a "Freedom of Information Act Appeal" and addressed as follows:

Freedom of Information Act Officer  
Office of the Inspector General, General Services Administration  
1800 F Street, NW, Room 5332  
Washington, D.C. 20405

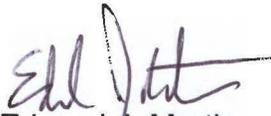
If you would like to discuss our response before filing an appeal to attempt to resolve your dispute without going through the appeals process, you can contact our FOIA Public Liaison Nancy Olson for assistance at:

Office of the Inspector General, General Services Administration  
1800 F Street, NW, Room 5332  
Washington, D.C. 20405  
(202) 501-1932  
oigfoia-privacyact@gsaig.gov

If you are unable to resolve your FOIA dispute through our FOIA Public Liaison, the Office of Government Information Services (OGIS), the Federal FOIA Ombudsman's office, offers mediation services to help resolve disputes between FOIA requesters and Federal agencies. The contact information for OGIS is:

Office of Government Information Services  
National Archives and Records Administration  
8601 Adelphi Road--OGIS  
College Park, MD 20740-6001  
ogis@nara.gov  
ogis.archives.gov  
202-741-5770  
877-684-6448

Sincerely,



Edward J. Martin  
Counsel to the Inspector General  
(FOIA Officer)

Enclosure

## CHAPTER 100 - AUTHORITIES, RESPONSIBILITIES, AND DELEGATIONS

### 101.00 AUTHORITIES AND RESPONSIBILITIES OF INSPECTOR GENERAL

101.01 Independent Authorities of the Inspector General

101.02 Delegated Authorities of the Inspector General

### 102.00 AUTHORITIES RESERVED FOR THE INSPECTOR GENERAL AND THE DEPUTY INSPECTOR GENERAL

102.01 Reserved Authorities

102.02 Designation of Acting Inspector General

### 103.00 AUTHORITIES DELEGATED BY THE INSPECTOR GENERAL TO OIG ORGANIZATIONS

103.01 IG's Delegation of Common Administrative Authorities to Component Heads

103.02 IG's Delegation of Specific Authorities to the Counsel to the IG

103.03 IG's Delegation of Specific Authorities to AIG for Administration

103.04 IG's Delegation of Specific Authorities to AIGs for Auditing and Investigations

103.05 IG's Delegation of Specific Authorities to AIG for Inspections

103.06 IG's Delegation of Redelegation Authority

### 104.00 ORGANIZATIONAL CHANGES INTERNAL TO THE OIG

Effective Date 10/27/2017

## 101.00 AUTHORITIES AND RESPONSIBILITIES OF THE INSPECTOR GENERAL

The Office of Inspector General (OIG) has independent authorities and responsibilities provided by the Inspector General Act of 1978, as amended (IG Act). The OIG additionally exercises authority under delegations of authority from the Administrator of the General Services Administration (GSA).

### 101.01 Independent Authorities of the Inspector General

The OIG/GSA is given statutory authority to conduct and supervise audits and investigations relating to GSA's programs and operations.

In carrying out these responsibilities, the IG Act gives the Inspector General (IG) authority to: (1) select, appoint and employ officers and employees; (2) contract and make necessary payments; and (3) obtain legal advice from its own counsel. The IG Act also makes the IG the head of a separate agency for its Senior Executive Service program as well as for certain other employment and personnel-related matters. In addition, the IG Act permits the Inspector General to take action as necessary to carry out the provisions of the IG Act. Such actions include, but are not limited to, formulating policies and making determinations and taking actions with respect to OIG operations. These operations include audits, investigations, evaluations and support activities including, but not limited to, information technology, personnel, finances and budget and legislative and congressional interaction.

The IG's independent statutory authorities are acknowledged in the GSA Delegations of Authority Manual (ADM P 5450.39D, CHGE 1).

### 101.02 Delegated Authorities of the Inspector General

The Administrator of GSA has made specific and general delegations of authority to the Inspector General (IG). See GSA Delegations of Authority Manual, ADM P 5450.39D, CHGE 1. The IG has not redelegated these authorities within the OIG beyond the Deputy IG (DIG) except as discussed later in this chapter.

The GSA Delegations of Authority Manual affirmatively states that nothing in the Administrator's delegation of authority is intended to limit the independent authority of the IG.

Effective Date 10/27/2017

## 102.00 AUTHORITIES RESERVED FOR THE INSPECTOR GENERAL AND THE DEPUTY INSPECTOR GENERAL

Certain authorities are reserved for the IG. All authority vested in the IG, to the extent permitted by law, is delegated to the DIG.

### 102.01 Reserved Authorities

Final approval and signatory authority is reserved for the IG and the DIG for the following and for all other matters that are not delegated by this Manual. This reservation does not limit the authority of the IG to delegate additional authority on a case-by-case basis:

- a. Correspondence to the GSA Administrator and Deputy Administrator; heads and Inspectors General of other departments and independent agencies; and heads of non-federal governmental units.
- b. Correspondence and transmittal of information to Members of Congress, Congressional Committees and congressional staffs.
- c. Correspondence to GSA's General Counsel for legal opinions on particularly sensitive matters.
- d. Approval of all reimbursable agreements for personnel.
- e. Concurrence (if appropriate) with correspondence prepared outside the OIG for signature by the Administrator, after appropriate reviews by OIG staff.
- f. Establishing policies that govern OIG activities.
- g. Reports to the Administrator, the Congress and the Council of Inspectors General on Integrity and Efficiency (CIGIE) that contain significant findings, such as Management Deficiency and other special reports that have agency-wide impact.
- h. Replies to Government Accountability Office (GAO) reports involving OIG activities or personnel.
- i. Issuance of OIG subpoenas and correspondence with the Attorney General.
- j. Organization and reorganization of the OIG.
- k. Oversight of the OIG Performance Management Program, including but not limited to the Strategic Plan, the Semi-Annual Report to the Congress and the Inspector General Awards Program.
- l. Rating approval and oversight of the OIG Senior Executive Service (SES) Management Program.
- m. Authorization to recruit, promote, detail or furlough OIG personnel, or initiate a reduction in force (RIF).
- n. Authorization of foreign travel.

- o. Approval of the OIG Congressional Budget Justification.
- p. Authorization of all recruitment, retention and relocation payments.
- q. Authorization of purchase requests in excess of \$5,000.
- r. Authorization for all conferences where the OIG net conference expenses will exceed \$100,000.

#### 102.02 Designation of Acting Inspector General

The DIG is the first assistant to the position of Inspector General for purposes of the Federal Vacancies Reform Act, 5 U.S.C. §§ 3345-3349d. GSA Order OIG 5450.2G designates the order by which certain officials of the OIG are to serve as Acting IG in the event the IG dies, resigns, or is otherwise unable to perform the functions and duties of the Office. Unless otherwise designated in writing by the IG or the Acting IG, the order for acceding to the position of Acting IG is as follows:

- a. Deputy Inspector General;
- b. Associate Inspector General;
- c. Assistant Inspector General for Audits;
- d. Assistant Inspector General for Investigations;
- e. Assistant Inspector General for Administration;
- f. Assistant Inspector General for Inspections;
- g. Counsel.

In the event the DIG by virtue of operation of the Federal Vacancies Reform Act reverts to his position as DIG before a new IG is sworn in, until there is an IG, the Associate Inspector General, or such other GSA/OIG career SES member as the DIG chooses, may exercise the authorities of the DIG as well under the overall authority of the DIG.

Effective Date 10/27/2017

## 103.00 AUTHORITIES DELEGATED BY THE INSPECTOR GENERAL TO OIG ORGANIZATIONS

To provide for the economic and efficient operation of OIG activities, the IG has, where necessary and not prohibited, delegated to appropriate personnel all authorities necessary to provide for the day-to-day function of OIG headquarters and field component offices. These delegations and redelegations are accomplished by the general delegations below and the assignment of responsibilities to individual components under the OIG Policy and Procedures Manual. GSA Order OIG 5450.2G incorporates the delegations made in this chapter.

### 103.01 IG's Delegation of Common Administrative Authorities to Component Heads

Heads of OIG components (Office of Audits (JA), Counsel (JC), Office of Inspections (JE), Office of Investigations (JI) and Office of Administration (JP)) are delegated the following common administrative and related signatory authorities within the areas of designated responsibilities under the OIG Policy and Procedures Manual:

- a. Communications, transmittals and actions in carrying out assigned areas of responsibilities not reserved to the IG or DIG.
- b. Requisitions and invoices for supplies and other services, including training, not to exceed \$3,500 for JA, JC, JE and JI, and not to exceed \$5,000 for JP. Services, such as those for experts and consultants, as authorized by 5 U.S.C. § 3109 may not exceed the equivalent daily rate prescribed for grade GS-15 of the General Schedule by 5 U.S.C. § 5332.
- c. Determinations whether to approve domestic travel and transportation for employees as required in the performance of their official duties.
- d. Determinations whether to approve training requests for employees.
- e. Selections of such officers and employees as may be necessary to carry out the functions, powers and duties of the office. Selections require concurrence of JP (for verification of pre-employment requirements and to ensure compliance with applicable statutes and regulations) and, for positions at the GS-15 level, consultation with the IG or DIG.
- f. Management of component performance, including employee evaluations and performance reviews and establishing performance goals and metrics (except that the DIG will function as the second level reviewer for persons rated by the component head as required). Updating and changing metrics should be completed in consultation with JPE.
- g. Determinations whether to issue notices of proposed adverse action to suspend, reduce in grade or pay, or remove component employees, and final letters of decision on these actions. Proposal and decision letters require the prior concurrence of JC and JP to ensure compliance with applicable statutes and regulations. When there is evidence of more than de minimus misconduct, decisions to take lesser action, including a decision not to take any action, must also be discussed with employee relations personnel before a final decision is made to ensure consistency throughout the OIG.

h. Acts as the deciding official on formal grievances and issues decision letters. Decision letters require the prior concurrence of JP and JC to ensure compliance with applicable statutes and regulations.

i. Determinations whether to approve requests for excused absences (administrative leave) up to 8 hours. This authority cannot be further delegated. The OIG follows GSA Policy 6010.4 OAD P Time and Leave Administration, Chapter 8. Excused Absence/Administrative Leave with the following exceptions: Delayed arrival policy (hazardous weather). The OIG follows OPM guidance and our own Inclement Weather Guidance, Chapter 415.

Professional examinations. Supervisors can only approve up to 8 hours of leave. Any additional request must be approved by the DIG.

Labor organization representation. As the OIG has no Labor organization we do not follow any part of this section of the GSA policy.

Appeals, hearing and grievances. The OIG has its own policy for Use Of Official Time, Chapter 417.

j. Requests to use leave without pay (LWOP) up to 40 hours and requests for advanced leave (with prior consultation with JP). This authority cannot be further delegated.

k. Determinations whether to modify working hours of individual employees, including situational telework.

l. Determinations whether to order and approve overtime consistent with budget allocations.

m. Determinations whether to grant requests for reasonable accommodation (upon concurrence from JP and JC).

n. Determinations whether to grant requests for FMLA (upon concurrence from JP and JC).

#### 103.02 IG's Delegation of Specific Authorities to the Counsel to the IG

The Counsel to the IG additionally is delegated approval and signatory authority for the following:

a. Correspondence relating to the Office of Counsel's areas of responsibilities, including legal matters and requests for legal guidance.

b. Civil referrals to, and correspondence concerning litigation and related matters with, the Department of Justice (DOJ) or U.S. Attorneys.

c. Documents reflecting GSA's position in response to proposed settlements submitted to the agency by DOJ in False Claims Act or Truth in Negotiation Act cases arising out of contracts awarded by the agency (reference Feb. 3, 1997 MOU from Emily Hewitt (L)).

d. Correspondence on matters pertaining to the release or denial of release of OIG information and documents, including the agency's response denying or granting disclosure on initial FOIA or Privacy Act requests.

#### 103.03 IG's Delegation of Specific Authorities to AIG for Administration

The AIG for Administration additionally is delegated approval and signatory authority for the following:

a. Correspondence and authorities relating to responsibilities assigned JP components, including budget formulation and execution, executive resources, human resources, space planning and management, COOP support, procurement actions in accordance with GSA's Contracting Officer Warrant Program, and information technology management and security.

b. Executive resource and human resource program management and implementation authorities includes general, blanket, and OPM agreement appointment and classification authorities; on-boarding; separation; benefits; employee relations; employee reductions in force; pay; pay allowances and differentials; time-in-grade waiver; part-time employment; conversion to career employment; hiring/retention bonuses; school loan forgiveness programs; details and extension of details; and awards programs, to the extent not reserved to the IG.

#### 103.04 IG's Delegation of Specific Authorities to AIGs for Auditing and Investigations

The AIG for Auditing (AIGA) and the AIG for Investigations (AIGI) additionally are delegated approval and signatory authority for the following:

a. Correspondence relating to the auditing (JA) and investigative (JI) responsibilities within the Office's respective assigned areas of responsibilities.

b. Policy direction for OIG audits (AIGA) and investigations (AIGI), in consultation with JC and with JE (for matters within JE's areas of responsibilities).

c. JA and JI reports released within GSA by headquarters to an official other than the Administrator or Deputy Administrator.

d. Correspondence with Associate Deputy Assistant Inspectors General (ADIAGAs)/Regional Inspectors General for Auditing (RIGAs) and Special Agents in Charge (SACs) on matters relating to:

1. Field office operations and utilization of personnel in the execution of assigned responsibilities;

2. Technical guidelines, direction and supervision in the conduct of audits, investigations and issuance of reports thereon;

3. Interpretations or application of investigation programs or guidelines;

4. Advice and counsel on liaison responsibilities with program officials, State and local governments, etc.;

5. Guidance on developing annual work plans; and

6. Correspondence disseminating FBI reports and recommending contractor suspension and debarment (AIGI).

### 103.05 IG's Delegation of Specific Authorities to AIG for Inspections

The AIG for Inspections additionally is delegated approval and signatory authority for the following:

- a. Correspondence with respect to the inspections, internal controls, internal review, records management and review and analysis responsibilities assigned to JE.
- b. Policy direction for areas of responsibilities assigned to JE, in consultation with JC and with JA and JI (for matters within JA and JI's areas of responsibilities).
- c. JE reports released within OIG or within GSA by headquarters to an official other than the Administrator or Deputy Administrator.
- d. Correspondence with deputies on matters relating to:
  1. Office operations and utilization of personnel in the execution of assigned responsibilities;
  2. Technical guidelines, direction and supervision in the conduct of inspections and issuance of reports thereon;
  3. Interpretations or application of inspection programs or guidelines;
  4. Advice and counsel on liaison responsibilities with program officials, State and local governments, etc.;
  5. Guidance on developing annual work plans.

### 103.06 IG's Delegation of Redelegation Authority

Unless restricted by other sections of this policy, component heads are authorized to redelegate authorities to GS-15 and lower level supervisors (including those designated to serve in an acting capacity).

Effective Date 10/27/2017

#### 104.00 ORGANIZATIONAL CHANGES INTERNAL TO THE OIG

In accordance with the IG Act, and as further memorialized in an agreement between the IG and the Administrator dated June 14, 1983, the OIG may make internal organizational changes without the approval or concurrence of other GSA officials.

The IG will provide GSA's Office of Organization and Chief People Officer with the information required to update the GSA Organization Manual.

## CHAPTER 200 - ORGANIZATION AND FUNCTIONS

### 201.00 OFFICE OF INSPECTOR GENERAL

- 201.01 Organization of the Office of Inspector General
- 201.02 Associate Inspector General
- 201.03 Counsel to the Inspector General

#### 201 FIGURES

- 201-01 OIG Organizational Chart

### 202.00 OFFICE OF AUDITS

- 202.01 Assistant Inspector General for Auditing
- 202.02 Staff Offices
- 202.03 Regional and Central Audit Offices
- 202.03A Regional Audit Offices
- 202.03B Central Office Audit Offices

### 203.00 OFFICE OF INVESTIGATIONS

- 203.01 Assistant Inspector General for Investigations
- 203.02 Operations Division (JIO)
- 203.03 Technical Support Branch (JIT)
- 203.04 Civil Enforcement Branch (JIC)
- 203.05 Intelligence Division (JII)
- 203.06 Digital Crimes and Forensics Unit (DCFU) (JIIF)
- 203.07 Regional Investigations Offices

### 204.00 OFFICE OF ADMINISTRATION

- 204.01 Assistant Inspector General for Administration
- 204.02 Budget and Financial Management Division
- 204.03 Human Resources Division
- 204.04 Information Technology Division
- 204.05 Facilities and Support Services Division
- 204.06 Contracting Division
- 204.07 Executive Resources

### 205.00 OFFICE OF INSPECTIONS

- 205.01 Assistant Inspector General for Inspections
- 205.02 Inspections
- 205.03 Quality Assurance
- 205.04 Questionable Charges and Delinquent Accounts

Effective Date 10/27/2017

## ORGANIZATION AND FUNCTIONS

### 201.00 OFFICE OF INSPECTOR GENERAL

#### 201.01 Organization of the Office of Inspector General

The OIG consists of the IG and the Deputy IG (DIG); the Associate IG, Counsel to the Inspector General; the Office of Audits (JA); the Office of Investigations (JI); the Office of Inspections (JE) and the Office of Administration (JP). The functions and activities of the OIG are accomplished through an organizational structure comprised of the Central Office in Washington, D.C. and field offices located in GSA regional cities. OIG resident duty stations are located in selected cities when deemed essential due to workload requirements. All field and resident office employees report, through their respective Associate Deputy Assistant Inspectors General for Auditing (ADAIGAs), Regional Inspectors General for Auditing (RIGAs), Deputy Directors, and Special Agents in Charge (SACs), to the appropriate Assistant Inspector General, who reports directly to the IG, or to the DIG.

#### 201.02 Associate Inspector General

- a. Responsible for OIG-wide management system planning, development, implementation, and assessment, including strategic, performance, resource, and succession planning.
- b. Provides executive leadership, direction, and oversight for program areas and functions in JE, including forensic auditing and analysis, internal assessments, external reviews and evaluations, and special reviews and projects.
- c. Provides higher level executive oversight for JP; including Executive Resources.
- d. Serves as a senior advisor to the IG and the Deputy IG.
- e. Conducts special reviews as directed by the IG or the Deputy IG.

#### 201.03 Counsel to the Inspector General

- a. Provides independent legal counsel to the IG, DIG, and all other OIG officials in all legal matters involving the OIG.
- b. Provides legal assistance in connection with ongoing investigations and audits of GSA programs and operations.
- c. Provides legal assistance in support of the issuance of IG subpoenas, including review of subpoena requests and the preparation of recommendations to the IG regarding issuance; represents the OIG in compliance matters; and initiates and assists in subpoena enforcement actions.
- d. Coordinates and controls civil litigation and related matters affecting the OIG, and provides guidance on civil potential of matters disclosed through audit and investigation. Coordinates OIG case support rendered to DOJ after referral of civil matters to the Department of Justice and/or U.S. Attorneys

(collectively DOJ). On behalf of the agency, IG Counsel approves all civil fraud settlements negotiated by DOJ in accordance with Section 708.05 of this manual. Also provides legal advice and support to GSA's Office of General Counsel (OGC) and/or DOJ in administrative fraud cases and other civil or administrative cases.

e. Assists DOJ in the preparation and conduct of criminal proceedings as appropriate.

f. Works closely with GSA OGC and DOJ in legal endeavors which require coordination and cooperation, and maintains liaison with other agencies and attorneys through groups such as the Council of Counsels to the Inspector General and otherwise.

g. Responsible for the statutory function of the IG to review existing and proposed legislation and regulations and make recommendations concerning their impact on the economy, efficiency and effectiveness of GSA programs or on preventing or detecting fraud, abuse or mismanagement.

h. Coordinates, evaluates, and serves as the deciding official on all requests submitted to the OIG under the provisions of the Freedom of Information Act and the Privacy Act (FOIA/PA). Provides legal advice and services for appeals and litigation of FOIA/PA denials.

i. Performs education and training of OIG personnel, other Government personnel and other groups.

j. Oversees the litigation aspect of employee relations matters, including adverse actions, workers compensation claims, Equal Employment Opportunity complaints, and other sensitive matters. Advises and coordinates with the director of Human Resources Division on employee relations matters.

k. Serves as the clearance office for the OIG, directing the review of proposed agency regulations/directives.

Effective Date 10/27/2017

## 202.00 OFFICE OF AUDITS

### 202.01 Assistant Inspector General for Auditing

Supervises, plans, directs, coordinates, and executes on an agency-wide basis all audit services, including conducting the internal audit and contract programs, program monitoring, and other technical reviews. Identifies and evaluates significant deficiencies disclosed by internal audit or investigative reports, Government Accountability Office (GAO) reports, and reports from other sources that may be impeding GSA's management effectiveness or that are of concern to top managers; and provides advice to managers to address and correct major deficiencies.

### 202.02 Staff Offices

The Audit Planning, Policy, and Operations Staff (JAO) and the Administration and Data Systems Staff (JAS) support and assist the Assistant Inspector General for Auditing (AIGA) and the DAIGs for Real Property and Acquisition Programs Audits (DAIGAs) with new initiatives, planning, policy development, operational oversight, quality assurance reviews, and management of budgeting and information systems.

### 202.03 Regional and Central Audit Offices

The Office of Audits (JA) has audit offices located in 7 of GSA's 11 regional offices and at Central Office headquarters. The regional and Central Office audit offices are led by RIGAs and ADAIGAs, respectively, under the direction of the DAIGAs. The regional and Central Office audit offices conduct programmatic performance audits of GSA's operations and activities, implementation reviews, and/or contract audits. The responsibilities of the regional and Central Office audit offices are discussed below.

#### a. Regional Audit Offices

1. Conduct performance audits of GSA's operations and activities in accordance with generally accepted government auditing standards.
2. Issue audit reports and make recommendations to appropriate officials for improving operations and for correcting deficiencies.
3. Review action plans submitted by management officials concerning report recommendations, appraise the adequacy of proposed actions, and recommend final resolution decisions.
4. Perform implementation reviews and prepare reports provided to appropriate management officials regarding the adequacy of actions taken.
5. Review proposed agency regulations/directives/legislation and make recommendations concerning the impact on the economy and efficiency of operations and adequacy of internal controls.
6. Represent the Office of Audits and maintain liaison with the GAO and other federal, state, and local audit organizations.

7. Advise and counsel GSA employees and management officials regarding audit activities and programs, and methods for promoting economy and efficiency and for detecting and preventing fraud, waste, and abuse.
8. Coordinate audit activities with and provide assistance, as necessary, to other OIG components, including subject matter or technical expertise to audit or investigative teams and task forces.
9. Conduct audits of various types of contracts administered in the assigned geographical area; which includes defining objectives, establishing priorities, scheduling, and performing field audit work.
10. Examine financial provisions and requirements of proposed contracts and advise contracting officers concerning these matters.
11. Review contractors' price proposals, estimating and accounting systems, general business practices and procedures, and related matters as provided for in the Federal Acquisition Regulations and the General Services Acquisition Manual.
12. Attend and participate in an advisory capacity, as appropriate, in contract negotiations and other meetings where contract cost matters, audit reports, or related financial matters are under consideration, and provide assistance to legal counsel for hearings before the Civilian Board of Contract Appeals.
13. Provide attestation engagement assistance to other government agencies and commissions, as appropriate.

b. Central Office Audit Offices

1. May perform and/or direct multiregional and agency-wide program, systems, internal control, financial, and compliance/regulatory audits in accordance with generally accepted government auditing standards. These audits focus on GSA's main service lines: PBS, FAS, TTS, other staff offices; and the National Capital Region.
2. May perform and/or direct multiregional and agency-wide contract audits in accordance with generally accepted government auditing standards and manage the Office of Audits Multiple Award Schedule Center of Expertise.
3. Respond to quick-turnaround projects, such as congressional inquiries and requests for assistance from other OIGs.
4. Lead the annual audit planning process, and develop GSA's management challenges.
5. The Central Office Audit Offices may also perform responsibilities 1 through 13 listed under the Regional Audit Offices section above.

Effective Date 10/27/2017

## 203.00 OFFICE OF INVESTIGATIONS

### 203.01 Assistant Inspector General for Investigations

- a. Supervises the management of a comprehensive nationwide program that provides for the detection and investigation of criminal activities against GSA by its employees, by vendors doing business with the agency, and by other individuals or groups of individuals. Also supervises civil and administrative investigations within the programs and operations of GSA.
- b. Directs and coordinates proactive investigations and programs designed to assess program vulnerabilities within GSA's services and staff offices.
- c. Serves as a principal adviser to the IG concerning all investigative activity within GSA and provides investigative advice and assistance to other elements of the OIG.
- d. Provides for close coordination of investigative activities with the Counsel to the Inspector General in matters requiring legal interpretations.

### 203.02 Operations Division (JIO)

- a. Manages the Investigative Data System.
- b. Manages the Office of Investigations (JI) training program and all law enforcement support activities.
- c. Manages responses to FOIA/PA requests and provides SAR data on behalf of JI.
- d. Directs JI administrative procedures and management; plans and coordinates support activities related to budget, personnel, policy, and office automation within JI.
- e. Oversees JI law enforcement equipment, badges and credentials.
- f. Conducts administrative investigations of OIG personnel and GSA senior officials as assigned. Supports criminal investigations at the direction of the AIGI. Conducts sensitive reviews at the direction of the IG.
- g. Coordinates leads from GSA's excess firearms program and disseminates cases as appropriate.

### 203.03 Technical Support Branch (JIT)

- a. Provides technical equipment investigative support to JI.

### 203.04 Civil Enforcement Branch (JIC)

- a. Coordinates the civil enforcement program to include contractor disclosures, Trade Agreements Act/Buy American Act cases, and qui tam investigations for JI.
- b. Manages the suspension and debarment program.

#### 203.05 Intelligence Division (JII)

- a. Directs the criminal intelligence program; responsible for direct investigative support to JI through identifying and consolidating databases, analysis of collected information and emergent trends, liaison with other law enforcement and intelligence agencies, and maximum utilization of information technology.
- b. Directs the background investigation program and conducts pre-employment suitability investigations for all OIG personnel.
- c. Operates the OIG Hotline/complaints program.
- d. Maintains continuous awareness of changes to applicable laws, regulations, procedures, and internal agency policies affecting areas of investigative concern, and makes appropriate recommendations.
- e. Plans and conducts proactive surveys and investigations of GSA and GSA-OIG operations. Presents observations and recommendations for appropriate action.
- f. Reviews investigative results for technical sufficiency and compliance with GSA-OIG and Council of Inspectors General on Integrity and Efficiency (CIGIE) policies and practices.
- g. Analyzes and maintains nationwide files and databases. Utilizes these databases to prepare periodic reports to support Presidential and congressional requirements.

#### 203.06 Digital Crimes and Forensics Unit (DCFU) (JIIF)

- a. The DCFU is the primary unit charged with seizing and analyzing computers and related digital media.
- b. Provides support to JI investigations in seizing digital evidence during search warrant operations and covert activities.
- c. Prepares detailed reports documenting their analysis and activities which are made part of the investigative files.
- d. Conducts investigations involving digital or computer related crimes, which affect GSA programs, personnel or operations.
- e. Maintains continuous awareness of changes to applicable laws, regulations, procedures, and internal agency policies affecting areas of computer forensics and digital crime; and makes appropriate recommendations.

#### 203.07 Regional Investigations Offices

- a. Region offices and the resident investigations offices within their jurisdiction are as follows:
  - 1. National Capital Region Investigations Office, Washington, DC (JI-W)  
Responsible for investigative coverage of National Capital Region (Region 11)

2. New England and Caribbean Region Investigations Office Boston, MA (JI-1)  
Responsible for investigative coverage of New England and Caribbean Region (Region 1)
  3. Northeast Region Investigations Office, New York, NY (JI-2)  
Responsible for investigative coverage of Northeast Region (Region 2)
  4. Mid-Atlantic Region Investigations Office, Philadelphia, PA (JI-3)  
Responsible for investigative coverage of Mid-Atlantic Region (Region 3)
  5. Southeast Sunbelt Region Investigations Office, Atlanta, GA (JI-4) and Ft. Lauderdale, FL (Resident Office)  
Responsible for investigative coverage of Southeast Sunbelt Region (Region 4)
  6. Great Lakes Region Investigations Office, Chicago, IL (JI-5)  
Responsible for investigative coverage of Great Lakes Region (Region 5)
  7. Heartland Region Investigations Office, Kansas City, MO (JI-6) and Denver, CO (Resident Office)  
Responsible for investigative coverage of Heartland Region and Rocky Mountain Region (Regions 6 and 8)
  8. Greater Southwest Region Investigations Office, Fort Worth, TX (JI-7)  
Responsible for investigative coverage of Greater Southwest Region (Region 7)
  9. Pacific Rim Region Investigations Office, San Francisco, CA (JI-9), Laguna Niguel, CA (Resident Office) and Sacramento, CA (Resident office)  
Responsible for investigative coverage of Pacific Rim Region (Region 9)
  10. Northwest/Arctic Region Investigations Office, Auburn, WA (JI-10)  
Responsible for investigative coverage of Northwest/Arctic Region (Region 10)
- b. Within the region, each office is responsible for the following functions:
1. Represents JI in the regions.
  2. Conducts criminal, civil and administrative investigations.
  3. Conducts GSA employee misconduct investigations.
  4. Conducts proactive investigations of GSA operations.
  5. Conducts investigations related to GSA programs and operations, including tort investigations.
  6. Maintains liaison with Federal, state and local law enforcement.
  7. Maintains liaison with U.S. Attorney's Offices and state and local prosecutors in the regional area.

8. Makes arrests, with or without a warrant, executes search warrants, serves subpoenas, and obtains records and information in connection with any official inquiry or investigation by the Office of Investigations.

9. Administers the oath to any person in connection with any official inquiry or investigation by the Office of Investigations.

10. Coordinates investigative activities with other operational components.

Effective Date 10/27/2017

## 204.00 OFFICE OF ADMINISTRATION

### 204.01 Assistant Inspector General for Administration

The Assistant Inspector General for Administration supports and advises the IG through executive oversight of integrated administrative services. JP includes the Budget and Financial Management Division (JPB), Facilities and Support Services Division (JPF), Contracting Division (JPC), Human Resources Division (JPH), Information Technology Division (JPM) and Executive Resource (JPE). These components and staff implement services, develop programs, provide data collection within the OIG and ensure that office policies are updated.

### 204.02 Budget and Financial Management Division

a. Establishes annual and multi-year funding requirements for the OIG nationwide.

b. Plans and directs the formulation of budget and cost estimates to support financial management plans, programs, and activities.

c. Designs and implements internal control systems to monitor and control the financial plans and budget activities of the OIG nationwide.

d. Develops OIG budgetary policies and practices.

e. Reviews OIG financial and personnel resources plans in relation to planned objectives and recommends allocation of these resources. Reviews requests for changes and recommends revisions to allocations in resource requirements.

f. Prepares OIG responses to Agency, Congressional, and Office of Management and Budget (OMB) budgetary requests and requirements. Prepares other financial and budget based documents as required.

### 204.03 Human Resources Division

a. Directs and coordinates comprehensive human resources operations for the OIG, other than those governed by the OIG Senior Executive Service Management Policy.

b. Implements and administers resource programs in accordance with applicable laws and policies. Program responsibilities include: position management and classification, recruitment and hiring,

suitability and security processing, employee orientation, placement, pay administration, employee benefits, performance management and recognition, merit promotion, employee management support, and employee relations and worklife programs. Programs are implemented and administered in accordance with legal requirements to ensure there is equal opportunity for all employees and applicants for employment.

c. Provides advice and assistance to management on personnel programs, including occupational staffing patterns, career ladder promotions, design and structure of positions, and reorganizations.

d. Provides interpretations of personnel policies; proposes internal policies and procedures for OIG; and responds to requests for information on benefits, retirement, and other personnel-related matters.

e. Develops and maintains good working relations and conditions within the OIG; provides information to employees regarding worklife balance, reasonable accommodations, and grievance procedures. Furnishes other services to promote employee welfare.

f. Processes and controls personnel documents, prepares regular and special reports, and answers routine inquiries regarding current and former employees.

#### 204.04 Information Technology Division

a. Provides the full range of information technology (IT) services to the OIG, including email, communications, and digitally stored document retrieval services. Coordinates with OIG managers and offices to develop the OIG 5-year Information Resources Plan. Serves as the official representative with the General Services Administration Chief Information Office (GSA CIO) and prepares all information technology reports as a result of acquiring and operating information technology within the OIG.

b. Directs the development and maintenance of the OIG General Support System (OIG GSS) in accordance with Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) requirements and GSA CIO directives. Ensures that the OIG GSS is fully operational, meets the federal requirements, and effectively supports the business needs of the OIG.

c. Serves as the central point of coordination within the OIG for review and approval of all IT hardware and software requirements prior to development or acquisition. Oversees the Enterprise Architecture Committee (EAC) and assists the IT Steering Committee in the review and approval process. Supports the Contracting Division in developing detailed procurement specifications for IT hardware and software acquisitions.

d. Provides the technical support to maintain confidentiality, integrity, and availability of the OIG GSS. Makes modifications in accordance with established configuration management procedures to meet changing OIG business procedures. Oversees the OIG IT Change Control Board to ensure modifications and changes are appropriate and maintain the security of the system.

e. Promotes and monitors the OIG IT security program, ensuring that policies and procedures are in place and OIG staff is properly trained in accordance with governing directives and requirements.

f. Provides instructions, operational guidance, and technical assistance to all OIG employees concerning the use of OIG IT systems.

g. Participates in audits or investigations of agency programs involving IT systems where expert technical support and experience is required.

#### 204.05 Facilities and Support Services Division

a. Plans, maintains, and coordinates comprehensive space and office management programs. Provides efficient use of office and program related space on a nationwide basis. Integrates furniture systems design, electrical support systems, communications systems design, specialized automated data processing (ADP), and OIG program requirements.

b. Serves as the central point of contact to ensure OIG space is maintained in a safe, operational, and functional manner. Analyzes and coordinates requirements to maintain and operate various kinds of facilities, office space, and equipment.

c. Serves as a central point of contact for planning and controlling the OIG response in the event of national crisis or disaster.

#### 204.06 Contracting Division

a. Serves as the OIG acquisition point of contact for all procurements ensuring that all contracts go through appropriate points of approval and review before being awarded. Develops internal contracting policies and procedures and procurement plans.

b. Coordinates all OIG acquisition programs to include Government Purchase Card and Travel Card programs.

c. Provides contracting support and/or advice to all OIG components to include guidance and assistance in developing, negotiating, and finalizing pertinent contract agreements.

#### 204.07 Executive Resources

a. Provides executive resources services by administering the OIG Senior Executive Service (SES) program and performance management system, including recruitment, selection, appraisals and compensation of SES members. Provides guidance on policies, procedures and requirements related to the OIG's SES system. Supports the IG, Deputy IG, the Executive Resources Board and the annual SES Performance Review Board.

b. Provides policy advisement in human capital management issues used to develop, train, and retain a high quality workforce. Performs workforce analysis on administrative programs to improve workforce performance and recommendations. Provides recommendations, interpretations and comments on relevant administrative policies, practices and procedures, including alternatives and solutions.

Effective Date 10/27/2017

## 205.00 Office of Inspections

### 205.01 Assistant Inspector General for Inspections

The Assistant Inspector General for Inspections supervises, plans, directs, coordinates, executes on an agency-wide basis all inspection and evaluation services, including program monitoring, and other technical reviews. Identifies and evaluates significant deficiencies disclosed by inspection and evaluation reports, and reports from other sources that may be impeding GSA's management effectiveness or that are of concern to top managers; and provides advice to managers to address and correct major deficiencies.

### 205.02 Inspections

- a. Conduct inspections and evaluations of GSA's operations and activities in accordance with Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspections and Evaluation.
- b. Issue reports and make recommendations to appropriate officials for improving operations and for correcting deficiencies.
- c. Review action plans submitted by management officials concerning report recommendations, appraise the adequacy of proposed actions, and recommend final resolution decisions.
- d. Perform implementation reviews and prepare reports provided to appropriate management officials regarding the adequacy of actions taken.
- e. Review proposed agency regulations/directives/legislation and make recommendations concerning the impact on the economy and efficiency of operations and adequacy of internal controls.
- f. Represent the Office of Inspections and maintain liaison with other federal, state, and local inspection and evaluation organizations.
- g. Advise and counsel GSA employees and management officials regarding inspection activities and programs, and methods for promoting economy and efficiency and for detecting and preventing fraud, waste, and abuse.
- h. Conduct other special reviews or projects as appropriate.

### 205.03 Quality Assurance

- a. Formulates, directs, and coordinates the OIG's Federal Managers' Financial Integrity Act program to evaluate the Office's management controls in order to ensure programs achieve their intended results; resources are used consistent with the Office's mission; programs are protected against waste, fraud, abuse, and mismanagement; laws and regulations are followed; the reliable and timely information is used for decision making. The FMFIA program encompasses the annual assurance statement and periodic internal control reviews.

b. Plans, directs, and coordinates the OIG internal evaluation and analysis program, which provides quality assurance for the organization. As part of the program, JE conducts reviews of central and field offices to impartially assess the Office's: administrative, managerial, records management, and organizational culture in support of the OIG mission; compliance with quality standards adopted by the Federal IGs, as well as OIG policies and procedures; and efficiency and effectiveness in meeting mission responsibilities.

c. Plans, directs, and coordinates the OIG records management program. Provides guidance, advice and assistance to OIG officials on records management issues. Coordinates and liaises with GSA's records management officials. Houses the OIG Records Management Coordinator.

#### 205.04 Questionable Charges and Delinquent Accounts

a. As part of the OIG quality assurance function, JE administers the questionable charges and delinquent account inquiries pertaining to OIG purchase cards and travel cards. JE serves as liaison with GSA's Travel & Purchase Card Program Division (H1D) for questionable purchase card and travel card matters on the part of OIG employees. For such matters, JE initiates an inquiry within the OIG to determine whether an OIG official authorized the transaction and whether the transaction appears both necessary and for official use. If appropriate, the inquiry also seeks to determine whether corrective action occurred.

CHAPTER 300 - MANAGEMENT SYSTEMS AND PROCEDURES

301.00 POLICY DEVELOPMENT AND PROMULGATION

301.01 OIG Manual

301.02 Preparation, Review, Approval and Issuance of OIG Manual Updates

302.00 through 326.00 RESERVED

327.00 COMPLAINTS AGAINST OIG EMPLOYEES

327.01 OIG Policy on Handling Complaints Against OIG Employees

327.02 Responsibilities for Handling Complaints Against OIG Employees

327.03 Procedures for Handling Complaints Against OIG Employees

Effective Date 12/30/2016

### 301.00 POLICY DEVELOPMENT AND PROMULGATION

The OIG policy system has been consolidated into the OIG Policies and Procedures Manual, now available on the OIG intranet. Policies and procedures are reviewed yearly.

#### 301.01 OIG Manual

The OIG Manual will be available on the IG Intranet.

The OIG Manual contains the OIG's permanent operational and administrative policies, standards, and procedures. The administrative policies and procedures in the Manual are based on and conform to the extent practicable with GSA directives.

Subsequent to OIG issuance of the Manual on May 1, 1984, GSA Order OIG P 5410.1 incorporated the Manual into the GSA Internal Directives System. This action was necessary to ensure that: (1) the Manual is referenced within the overall GSA directives numbering system; and (2) it therefore represents a definitive statement of GSA policy and procedure. Under the criteria of the GSA Internal Directives System, the Manual constitutes a handbook; and formal Internal Directives references are therefore amendments to the OIG Policies and Procedures Handbook.

Although the Manual is part of the GSA Internal Directives System, the IG retains sole authority over its content and distribution.

#### 301.02 Preparation, Review, Approval and Issuance of OIG Manual Updates

For changes proposed for Chapters 100 – 700, components initiating proposed Manual changes shall provide JC a summary of the proposed changes, the Manual text showing the proposed changes, and the Manual text showing both deleted and new material. JC shall forward the proposal package to JP after JC's preliminary review.

JP shall circulate the proposal package to all major component heads for comment. Component heads have 15 workdays to respond; additional time may be requested and granted by the proposing entity or the Deputy Inspector General (DIG). After all comments are received, JP will coordinate with JC in making revisions, and will if necessary circulate a revised version to all component heads for further comment. Component heads have another 15 workdays to respond. This process will be repeated as appropriate. After the final round of comments, JC shall review the proposal. Upon receiving JC clearance, JP shall forward the final proposal package, including any unresolved comments, to the DIG for determination.

For changes proposed for Chapters 800, 900, and 1000, the component initiating the proposed changes shall provide JC a summary of the proposed changes, the Manual text showing the proposed changes, and the Manual text showing both deleted and new material. JC shall forward the proposal package to JP after JC completes its review. JP shall forward the final proposal package to the DIG for determination.

Only substantive changes to any chapter will be circulated for comment and DIG approval. Changes of a ministerial nature do not require component comment or DIG approval.

Upon final approval of any change to the Manual, JP shall effect changes by updating the Manual and publicizing the changes on the intranet. Approvals for Manual changes shall be maintained by JP.

Effective Date 12/30/2016

## 327.00 COMPLAINTS AGAINST OIG EMPLOYEES

The following procedures will be used by the OIG to handle misconduct allegations involving OIG employees.

### 327.01 OIG Policy on Handling Complaints Against OIG Employees

Any OIG employee who receives information indicating misconduct by an OIG employee must report the misconduct to his/her supervisor, who in turn will report the allegation to the Component Head. The Component Head will report the allegation to the Deputy Inspector General (DIG), who will decide whether further investigative action is needed. Examples include potential violations of criminal laws, administrative regulations, and ethical standards, and allegations of professional misconduct.

OIG employees should report allegations of harassment or discrimination to the OIG Employee Relations Officer.

The Employee Relations Officer will provide additional information regarding the EEO process and can provide additional contact information for the GSA Office of Civil Rights.

Allegations of sexual harassment must be reported to the Counsel to the IG by the Employee Relations Officer or by any management official who receives an allegation or complaint of sexual harassment in the workplace. Counsel will report the allegation to senior leaders with a need to know.

Pursuant to the Inspector General Act, as amended, the Inspector General is required to refer allegations of wrongdoing against the Inspector General and some OIG senior staff to the Integrity Committee of the Council of Inspectors General on Integrity and Efficiency (CIGIE). Allegations that must be referred to the Integrity Committee can be found on the CIGIE website.

### 327.02 Responsibilities for Handling Complaints Against OIG Employees

The DIG has the responsibility for deciding whether investigative action is needed in response to a complaint against an OIG employee. Once a complaint or allegation is received, the DIG in determining the need for any further investigation may consult with JI and JC as appropriate. Those complaints not requiring an investigation will be referred to the responsible senior manager for any appropriate follow-up and/or administrative action in consultation with the OIG Employee Relations Officer and JC.

OIG managers should collect any available information from the complainant, but make no further inquiries pending discussion with JC, the OIG Employee Relations Officer, and/or the DIG. The manager shall safeguard the complaint and the Report of Investigation (ROI). Access to this information shall be limited to those employees who have an official need to know. All OIG employees are required to cooperate fully with any inquiry or investigation.

### 327.03 Procedures for Handling Complaints Against OIG Employees

At the direction of the DIG, JI will conduct an investigation of complaints or allegations of wrongdoing by OIG Employees. The selection of a special agent will include consideration of any potential conflicts or

recusals. The special agent who conducts the investigation will follow applicable investigative techniques and standards to pursue the complaint to its logical conclusion including criminal prosecution.

The results of any administrative violation may be discussed with JC and the OIG Employee Relations Officer, as appropriate. The ROI shall be forwarded through the DIG to the responsible senior manager for information or administrative action.

Investigations where there are reasonable grounds to believe there has been a criminal violation are referred to the U.S. Attorney and/or Department of Justice. In the event the matter is declined for prosecution, the ROI will be forwarded through the DIG to the responsible senior GSA OIG manager for any action that GSA OIG management officials deem appropriate.

All documentation of an internal OIG investigation will be kept confidential.

## CHAPTER 400 - ADMINISTRATIVE SYSTEMS AND PROCEDURES

### 401.00 LEAVE, TIME AND ATTENDANCE

- 401.01 Time and Attendance Clerks
- 401.02 Certifiers
- 401.03 Procedures
- 401.04 Hours of Duty
- 401.05 Sick Leave
- 401.06 Leave Changes
- 401.07 Concurrence, Consultation, and Approvals

### 402.00 OFFICE HOURS AND WORK SCHEDULES

- 402.01 Basic Work Requirement
- 402.02 Tour of Duty
- 402.03 Alternative Work Schedules
- 402.03A Flexible Work Schedules
- 402.03B Compressed Work Schedules
- 402.04 Tardiness and Brief Absences
- 402.05 Training
- 402.06 Participation in Civil Activities

### 403.00 OIG ASSOCIATE PERFORMANCE PLAN AND APPRAISAL SYSTEM

- 403.01 Purpose
- 403.02 Applicability
- 403.03 Legal Authority
- 403.04 Responsibilities
- 403.05 Rating Period

### 404.00 OIG POLICY ON COMPENSATION AND PAID OVERTIME WORK

- 404.01 Overview
- 404.02 Applicability
- 404.03 Legal Authority
- 404.04 General Approvals
- 404.05 Procedures

### 405.00 PERSONNEL SECURITY

- 405.01 OIG Personnel Security Program
- 405.02 OIG Pre-Employment Investigation
- 405.03 OIG Personnel Security Requirements
- 405.04 OIG Personnel Security Requirements for OPM Background Investigations

### 406.00 OFFICIAL TRAVEL

- 406.01 Purpose
- 406.02 Local Travel
- 406.02A Designation of Local Travel Areas
- 406.02B Use of Privately Owned Vehicles
- 406.02C Tokens, Tickets and Passes ("Transit Passes") Maintained by the OIG

- 406.02D Public Transit and Private Transportation
- 406.05E Use of Government Owned Vehicles
- 406.03 Special Travel Situations
- 406.03A Allowable Upgrades
- 406.03B Non-Federal Source Travel
- 406.03C Interview Trips
- 406.04 Actual Expense Method
- 406.05 Miscellaneous Expenses
- 406.05A Necessary Use of Communication Services
- 406.06 Foreign Travel
- 406.06A Authorization
- 406.06B Official Passport
- 406.06C Visas
- 406.06D Department of State Country Clearance
- 406.06E Security Briefing/Debriefing
- 406.07 Travel Reservations
- 406.08 Travel Authorizations
- 406.08A Annual Authorizations
- 406.09 Travel Advances
- 406.10 Moving Expense Allowances
- 406.11 Travel Card
- 406.11A Delinquency

#### 406 FIGURES

- 406-01 Appendix A: Fare Card Log
- 406-02 Appendix B: Interview Travel Instructions and Guidance

#### 407.00 RECORDS MANAGEMENT, INCLUDING HANDLING ELECTRONIC RECORDS

- 407.01 "Record" Defined
- 407.02 Responsibilities
- 407.03 File Plan
- 407.04 File Naming Conventions
- 407.05 Approved Storage Systems
- 407.06 Transfer of Records to Official File Systems
- 407.07 Email Systems
- 407.08 Capstone
- 407.09 Disposition
- 407.10 Senior Official Exit Briefing
- 407.11 Quality Assurance
- 407.12 Vital Records
- 407.13 Litigation Holds
- 407.14 Controlled Unclassified Information [RESERVED]
- 407.15 Information Technology
- 407.16 Former Employees' Data

#### 408.00 CREDENTIALS AND/OR BADGES

- 408.01 OIG Policy on Issuance of Credentials and/or Badges

- 408.02 Carrying Badges and/or Credentials
- 408.03 Use of Badges and/or Credentials
- 408.04 Proper Presentation of Badges and/or Credentials
- 408.05 Loss of Badges and/or Credentials
- 408.06 Failure to Safeguard Badges and/or Credentials
- 408.07 Issuance of Retired Law Enforcement Credentials
- 408.07A Background
- 408.07B Policy for Retired Special Agents
- 408.07C Procedures for Retired Special Agents
- 408.07D Procedures for Current Special Agents
- 408.07E Procedures for Re-issuing Photographic Identification
- 408.08 Procedures for Returning Credentials and Badges

#### 409.00 STAFF REASSIGNMENT

- 409.01 Reassignment Policy
- 409.02 Positions Subject to Reassignment or Relocation

#### 410.00 CORRESPONDENCE CONTROL

- 410.01 General Correspondence

#### 411.00 RESERVED

#### 412.00 AWARDS

- 412.01 Purpose
- 412.02 Applicability
- 412.03 Legal Authority
- 412.04 Types of Awards
- 412.05 Policy
- 412.06 Performance-Based Awards
- 412.07 Special Act Awards
- 412.07A Inspector General (IG) Awards
- 412.07B Time-Off Awards
- 412.08 OIG Appreciation Plaques
- 412.09 Prohibition on Acceptance by OIG Employees of Certain GSA-Conferred Cash Awards

#### 413.00 POLICY AND PROCEDURES RELATED TO TRAINING AND DEVELOPMENT

- 413.01 Purpose
- 413.02 Legal Authority
- 413.03 Objectives
- 413.04 Eligibility for Training and Development Programs
- 413.05 OIG Annual Training Cycle
- 413.06 Mandatory Training
- 413.07 Payment of Training Expenses
- 413.08 Authorization, Agreement and Certification of Training
- 413.09 Expectations for Employees Attending Training
- 413.10 Continuing Service Agreement (CSA)
- 413.11 Educational Assistance Programs
- 413.12 Recording Training

#### 413 FIGURES

- 413-01 SF-182
- 413-02 Continuing Service Agreement
- 413-03 Appendix A - Mandatory Training for New OIG Employees
- 413-04 Appendix B - Mandatory Training for OIG Employees
- 413-05 Appendix C - Instructions for Entering Completed Training in CHRIS

#### 414.00 SUPERIOR QUALIFICATIONS AND SPECIAL NEEDS PAY SETTING AUTHORITY

414.01 Purpose

414.02 Applicability

414.03 Legal Authority

414.04 Definitions

414.05 Responsibilities

414.06 Procedures for Requesting Approval for a Superior Qualification Appointment (SQA)

414.07 Documentation and Recordkeeping

#### 415.00 OIG INCLEMENT WEATHER GUIDANCE

##### 415 FIGURES

- 415-01 Decision Matrix on the Application of the Updated Leave Practice

#### 416.00 SES PERSONNEL POLICIES, REGULATIONS, AND PROCEDURES

#### 417.00 USE OF OFFICIAL TIME

417.01 Introduction

417.02 Requesting Official Time

417.03 EEO Complaints

417.04 MSPB Appeals

417.05 Administrative Grievances

417.06 Other Proceedings

417.07 Response to Proposed Suspensions or Adverse Actions and Proposals based on Unacceptable Performance

417.08 Additional Discretionary Time-Extenuating Circumstances

417.09 Coordination with JP

#### 418.00 POLICY GOVERNING EXPENSES FOR PROFESSIONAL CREDENTIALS

418.01 Introduction

418.02 Definitions

418.03 Eligibility

418.04 Provisions Governing Reimbursement of Expenses for Professional Credentials

418.05 Administrative Procedures

#### 419.00 OIG TELEWORK POLICY

419.01 Introduction

419.02 OIG Telework Policy

419.03 Employee Participation in Telework is Voluntary

419.04 The Nature of Telework

419.05 Responsibilities

419.06 Eligibility

- 419.07 Pay, Leave, Etc.
- 419.08 Telework Agreements
- 419.09 Training
- 419.10 Information Technology (IT) - Generally
- 419.11 Definitions

419 FIGURES

- APPENDIX 1: RMOs
- APPENDIX 2: Telework Agreement
- APPENDIX 3: Extended Situational Teleworker - Daily Log

420.00 OIG POLICY ON COLLABORATIVE RESOURCES AND SOCIAL MEDIA

- 420.01 Applicability
- 420.02 Rules and Responsibilities
- 420.03 Penalties for Non-Compliance

421.00 INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) FOR INDIVIDUALS WITH DISABILITIES - SECTION 508 OF THE REHABILITATION ACT OF 1973

- 421.01 Purpose
- 421.02 Scope and Applicability
- 421.03 Policy
- 421.04 Contracting Personnel
- 421.05 Exceptions

421 FIGURES

- Request for Exception to Section 508 Requirement

422.00 PURCHASE AND USE OF KITCHEN APPLIANCES

- 422.00 Purchase and Use of Kitchen Appliances
- 422.01 Policy
- 422.02 Procedures
- 422.03 Business Need Justification: Criteria

423.00 CONFERENCE PROCEDURES

- 423.01 Purpose and Scope
- 423.02 Definitions
- 423.03 Designation
- 423.04 Conferences Hosted or Sponsored by OIG
- 423.04A Planning
- 423.04B Approval Requirements
- 423.04C Process for Requesting Approval
- 423.04D Required Submittals After the Conference
- 423.05 Attendance at Conferences Not Sponsored or Hosted by OIG
- 423.06 Website Reporting

Meeting and Training Form

#### 424.00 IT EQUIPMENT REQUEST POLICY

- 424.01 Purpose
- 423.02 GSA Policy References
- 423.03 Policy
- 423.04 Exceptions

#### 425.00 OIG WAIVER OF CLAIMS FOR OVERPAYMENT OF PAY AND ALLOWANCES AND OF TRAVEL, TRANSPORTATION, AND RELOCATION EXPENSES AND ALLOWANCES

- 425.01 Introduction
- 425.02 Authority and Responsibilities
- 425.03 Definitions
- 425.04 Applicability
- 425.05 Waiver Requirements
- 425.06 Waiver Processing
  - 425.06A Requests
  - 425.06B Report of Investigation
  - 425.06C Appeals
  - 425.06D Repayment
- 425.07 Recordkeeping

#### 426.00 OPERATIONS IN THE ABSENCE OF APPROPRIATIONS

- 426.01 Purpose
- 426.02 Implementing Action
- 426.03 Exempt and Excepted Personnel and Activities
- 426.04 Prohibition on the Use of Mobile Devices and Remote Access to OIG Systems
- 426.05 Recall System

#### 427.00 SELECTION AND ASSIGNMENT OF OIG EMPLOYEES FOR TEMPORARY ASSIGNMENT OR DETAIL TO THE LEGISLATIVE BRANCH

- 427.01 Purpose
- 427.02 Authority
- 427.03 Delegation
- 427.04 Implementing Actions

#### 428.00 REASONABLE ACCOMMODATION POLICY

- 428.01 Purpose
- 428.02 Applicability
- 428.03 Definition
- 428.04 Legal Authority
- 428.05 Responsibilities
- 428.06 Consultation and Review of Medical Documentation

#### 429.00 POLICY AND PROCEDURES RELATED TO MERIT PROMOTION OR PLACEMENT

- 429.01 Noncompetitive Candidates
- 429.02 Release for Placement

#### 430.00 SUPERVISOR TRAINING

- 430.01 Purpose
- 430.02 Applicability
- 430.03 Legal Authority
- 430.04 Mandatory Training Requirements
- 430.05 Additional Training
- 430.06 Completion and Reporting of Training

#### 431.00 POLICY AND PROCEDURES FOR MEMORANDA OF UNDERSTANDING (MOU)

- 431.01 Purpose
- 431.02 Applicability
- 431.03 Legal Authority
- 431.04 Approvals
- 431.05 MOU Requirements
- 431.06 MOU Procedures

#### 432.00 MISCELLANEOUS REIMBURSEMENTS

- 432.01 Purpose
- 432.02 Applicability
- 432.03 Authorized Miscellaneous Claims
- 432.04 Unauthorized Miscellaneous Claims

#### 433.00 POLICY REGARDING INTERN ACCESS TO OIG INFORMATION TECHNOLOGY (IT)

- 433.01 Purpose
- 433.02 Policy

#### 434.00 OIG INFORMATION TECHNOLOGY (IT) SECURITY POLICY

- 434.01 Purpose
- 434.02 Incident Response Reporting Procedures
- 434.03 OIG Rules of Behavior for Accessing Personally Identifiable Information (PII)
- 434.04 Personally Owned Mobile Devices
- 434.05 OIG Password
- 434.06 OIG Electronic Messaging and Collaboration Services (EMCS)
- 434.07 International Travel
- 434.08 HSPD-12 Personal Identity Verification (PIV) Cards

#### 435.00 SEE INFORMATION TECHNOLOGY (JPM) PROCEDURES

436.00 OIG TELECOMMUNICATIONS POLICY

- 436.01 Purpose
- 436.02 Telecommunications Support
- 436.03 Wireless Device Services
- 436.04 Waste, Fraud and Abuse
- 436.05 Remote Networks and Printing
- 436.06 Personal Devices
- 436.07 Lost or Stolen Mobile Devices

437.00 - 440.00 SEE INFORMATION TECHNOLOGY (JPM) PROCEDURES

441.00 PROPERTY MANAGEMENT PROGRAM POLICY

- 441.01 Purpose and Scope
- 441.02 Definitions
- 441.03 Responsibilities
- 441.04 Inventory Management
- 441.05 Lost or Stolen Personal Property
- 441.06 Disposal of Property

441 FIGURES

- 441-01 Exhibit A - Types of Sensitive Property

442.00 RECRUITMENT, RELOCATION AND RETENTION INCENTIVES

- 442.01 Purpose
- 442.02 Applicability
- 442.03 Legal Authority
- 442.04 Definitions
- 442.05 Designated Employment Categories
- 442.06 Responsibilities
- 442.07 Procedures for Requesting Approval for a Recruitment, Relocation and Retention

Incentive

- 442.08 Documentation and Recordkeeping

443.00 IT SOFTWARE LICENSE MANAGEMENT POLICY

- 443.01 Purpose
- 443.02 Scope and Applicability
- 443.03 Policy
- 443.04 References

443 FIGURES

- 443-01 Appendix: Configuration Items List

444.00 IT INTEGRATION POLICY

- 444.01 Purpose

- 444.02 Applicability
- 444.03 Scope
- 444.04 Policy

#### 445.00 IT CONFIGURATION MANAGEMENT

- 445.01 Purpose
- 445.02 Scope
- 445.03 Objectives
- 445.04 Roles and Responsibilities
- 445.05 Configuration Management Process
- 445.06 Request a Change
- 445.07 Configuration Audits

#### 446.00 OIG SHAREPOINT GOVERNANCE POLICY

- 446.01 Purpose
- 446.02 Applicability
- 446.03 Scope
- 446.04 Definitions
- 446.05 Roles
- 446.06 Content
- 446.07 Policy
- 446.08 References

#### Information Technology (JPM) Procedures

- 435.00 IT Service Desk Standard Operating Procedures (Effective 2/26/2018)
- 436.00 See OIG Telecommunications Policy
- 437.00 Enterprise Architecture Committee (EAC) Guide (Effective 2/6/2017)
- 438.00 IT Steering Committee (ITSC) Guide (Effective 1/5/2018)
- 439.00 Change Control Board (CCB) Guide (Effective 2/6/2017)
- 440.00 Asset Management Procedures (Effective 12/9/2015)

#### Contracting (JPC) Procedures

- OIG Procurement Procedures (Effective 10/30/2017)
- Annual Recurring Services Process (Effective 3/17/2017)
- Annual Recurring Services Guidelines (Effective 3/17/2017)

#### Human Resources (JPH) Procedures

Hiring Procedures for OIG Supervisors (Effective 3/10/2017)  
Federal Cybersecurity Coding Procedures (Effective 4/5/2017)

Appendix 1 Factors to be considered by RMOs in making determinations concerning telework agreements

Telework Agreement Form.pdf Appendix 2 Telework Agreement Form

Appendix 3 Extended Situational Teleworker – Daily Log fillable.pdf Appendix 3 Extended Situational Teleworker – Daily Log

Appendix 4 GSA 2578 OIG Waiver of Claims

Effective Date 12/1/2014

#### 401.00 LEAVE, TIME AND ATTENDANCE

Specific guidance governing the requesting, approval, and administration of annual and sick leave can be found in 5 C.F.R. Parts 610 and 630, and GSA Orders OAD P 6010.4 Time and Leave Administration and CFO P 4282.1B Time Keeping Handbook. The OIG generally will follow GSA Orders OAD P 6010.4 and CFO P 4282.1B, except where the OIG has adopted a different policy.

##### 401.01 Time and Attendance Clerks

Each component head is responsible for designating time and attendance clerks within his/her unit. Time and attendance clerks are responsible for being thoroughly familiar with the provisions of GSA Order OAD P 6010.4 GSA Time and Leave Administration Policy and maintaining the time and attendance records accordingly. Each clerk should also review the following reference documents available on GSA's FEDdesk: TimeKeeper Manual and Base Schedule Orientation.

##### 401.02 Certifiers

Each component head is responsible for designating time and attendance certifiers within his/her unit or by making arrangements with another component. Certifiers should be supervisors or managers and are responsible for being thoroughly familiar with the provisions of GSA Order OAD P 6010.4 and certifying the time and attendance records accordingly. Each certifier should also review the Certifier Manual available on GSA's FEDdesk.

##### 401.03 Procedures

The OIG uses OPM Form 71, or a variation thereof, to submit leave requests. Employees generally should request leave in advance by submitting the OPM Form 71 to their supervisor. The form can be signed electronically as well as manually. Once the OPM Form 71 has been approved, it is the responsibility of the employee to submit the OPM Form 71 to their time and attendance clerk to ensure it is recorded in ETAMS timely. Leave slips should be submitted to the time and attendance clerk at the end of each week or at a minimum at the end of each pay period.

##### 401.04 Hours of Duty

Office hours and work schedules are discussed in Section 402.00 of the OIG Policies and Procedures Manual, GSA Order 5410.1B OIG P.

##### 401.05 Sick Leave

In accordance with OPM guidance, contrary to GSA policy, the OIG will allow employees to use sick leave to make arrangements necessitated by the death of a family member or attend the funeral of a family member, and the OIG authorizes supervisors to advance up to 240 hours of sick leave to an employee for a serious health condition of a family member.

#### 401.06 Leave Charges

Section 402 of the OIG Manual discusses leave charges for tardiness and brief absences. Per Chapter 100 of the OIG Manual, Heads of OIG components and directors of OIG staff offices are authorized to approve requests for other types of leave, including:

- Excused absences up to 8 hours (administrative leave)
- Requests to use leave without pay (LWOP) of 40 hours or more in a single instance (with prior consultation with JP as appropriate)
- Requests for advanced annual leave (with prior consultation with JP as appropriate).

#### 401.07 Concurrence, Consultation, and Approvals

References to GSA officials will be interpreted as references to the appropriate OIG position in all OIG policies. Examples follow.

GSA policy frequently refers to the Associate Administrator for Administration; in the OIG, generally those references are to the Office of Administration (JP).

GSA policy also refers to the Office of General Counsel; in the OIG, those references will be to the OIG Office of Counsel (JC).

GSA also refers to the Director of Personnel or the Chief People Officer; in the OIG those references will be to the Director of Human Resources (JPH).

Effective Date 7/5/2016

## 402.00 OFFICE HOURS AND WORK SCHEDULES

The policy sets forth the standards and procedures governing the requirements for scheduling work time for OIG employees. The GSA policy on time and attendance and work schedules is contained in GSA Order OAD P 6010.4, "Time and Leave Administration." Except where it would be inconsistent with the policy below, the OIG will generally follow GSA Order OAD P 6010.4.

### 402.01 Basic Work Requirement

The basic work requirement of the OIG is the number of hours, excluding overtime hours, employees are required to work or otherwise account for by leave, holiday hours, excused absence, compensatory time off, or time-off award hours. Full-time OIG employees must account for 40 hours per workweek (i.e. 80 hours during a biweekly pay period). The default work schedule for OIG employees is 8:30 a.m. to 5:00 p.m. Monday through Friday.

### 402.02 Tour of Duty

The tour of duty defines the limits within which an employee must complete his or her basic work requirement. The normal tour of duty, absent a Compressed Work Schedule, for OIG employees is an 8 ½ hour workday, scheduled Monday through Friday between 6:00 a.m. and 6:00 p.m. The standard tour of duty includes an unpaid half hour for lunch.

### 402.03 Alternative Work Schedules

The OIG supports the use of flexible work schedules and compressed work schedules, collectively referred to as "alternative work schedules" (AWS). The AWS Program allows the OIG to meet the needs of a changing workforce by providing employees with increased workplace flexibilities to help balance work, personal and family responsibilities.

OIG employees may participate in either a flexible work schedule or a compressed work schedule, but not both. Supervisors may require an employee to submit a written request to start, change, or discontinue an AWS. When reviewing an employee's request for an AWS, supervisors must consider the organizational needs of the office. Factors to be considered include the effect of AWS on the productivity and efficiency of the office; services provided by the office; technical and administrative staffing required during office hours for successful day-to-day coordination with other offices including the regions; and the availability of appropriate supervision, if necessary.

OIG employees who wish to make long-term changes to their work schedules (as opposed to one-time variations) should make such requests in advance, under conditions directed by their supervisors. Supervisors retain the right to require an employee or groups of employees to suspend an AWS, temporarily or permanently, to meet agency needs.

#### A. Flexible Work Schedules

Flexible Work Schedules (FWS) for OIG employees refer to arrangements in which the fixed times of arrival and departure are changed, either permanently or daily as determined by the component head

and supervisor. FWS consist of workdays with core hours and flexible hours. The employee's arrival and departure times must be consistent with the duties and requirements of his/her position.

### 1. Core Hours

Core hours are the designated period of the workday, within the tour of duty, during which FWS employees are required to be present for work (or otherwise account for their hours). OIG component heads may set the core hours for their organizations; in the absence of a component head designation, the OIG's core hours are 9:30 a.m. to 2:30 p.m. (which includes ½ hour for lunch).

### 2. Flexible hours

Flexible hours are the workday hours within the tour of duty during which employees may choose their time of arrival and departure, subject to limits or "time bands." OIG component heads may set the flexible hours for their organizations; in the absence of a component head designation, the flexible time bands for OIG employees on FWS are 6:00 a.m. to 9:30 a.m. (arrival) and 2:30 p.m. to 6:00 p.m. (departure).

### 3. Flexitour

Under flexitour, employees work an 8 hour day (plus 1/2 hour lunch) but are able to select their arrival and departure times, subject to management approval. Once the flexitour schedule has been approved, it becomes a fixed schedule. For example, an OIG employee may request a schedule where they would begin work at 7 a.m. and work an 8 hour day (plus 1/2 hour lunch) ending at 3:30 p.m., or the employee could request to work from 8 a.m. until 4:30 p.m. All proposed flexitour schedules need advance supervisory approval.

### B. Compressed Work Schedules

A Compressed Work Schedule modifies the basic work requirement to less than 10 days within a biweekly pay period. For OIG employees, the approved Compressed schedule is 5-4/9, in which employees have eight 9-hour workdays, one 8-hour workday and one non-workday ("AWS off-day") during each 80-hour pay period. Once established, the employee's Compressed schedule is fixed and does not change; there is no flexibility in the arrival or departure time each day.

OIG component heads may set the Compressed schedule arrival and departure times for their organizations; in the absence of a component head designation, arrival times must be scheduled between the hours of 6:00 a.m. and 9:30 a.m., and departure times must be scheduled between the hours of 3:30 p.m. and 7:00 p.m. for OIG employees on compressed schedules. Employees must account for all hours scheduled for each 9-hour or 8-hour workday.

When a holiday falls on an employee's AWS off-day, the employee has the right to have a day off in lieu of the holiday ("ILOH"). The day to be treated as his/her holiday can be set by the supervisor to avoid an adverse agency impact. If the supervisor does not set an alternate day, the default "in lieu of holiday" is the workday immediately before or after the AWS off-day. In either scenario, the "in lieu of holiday" must be within the same bi-weekly pay period as the holiday. Also, when an employee's AWS off-day falls on the same workday that OIG offices are closed due to an emergency (e.g., weather or other

event), the employee is not entitled to another AWS day off "in lieu of" the workday on which the Federal offices were closed.

#### 402.04 Tardiness and Brief Absences

At the discretion of the supervisor, employees may be excused without charge to leave or loss of pay for unavoidable or necessary absences of less than 1 hour in nonroutine or emergency situations or when it is in the interest of the OIG to excuse the employees.

In addition, supervisors may allow employees on fixed work schedules (whether standard, flexitour or compressed schedules) to voluntarily make-up the time for brief and infrequent absences. An employee makes-up the time by staying late the same day, equivalent to the period of absence or tardiness. The ability to make-up the time for absences is subject to the following limitations:

- Employees must submit a request to their supervisor and receive approval in advance of staying late.
- Make-up time can be requested for absences of two hours or less. Employees will generally be charged leave for absences greater than two hours.
- Make-up time must generally be performed within the time bands (6:00 a.m. to 7:00 p.m.) tour of duty.
- Make-up time is generally limited to one absence/occurrence per pay period.

When reviewing an employee's request to make-up time, supervisors must consider the organizational needs of the office, specifically: the effect on the productivity and efficiency of the office; services provided by the office; technical and administrative staffing required during the proposed make-up time for successful coordination with other offices, including the regions; and the availability of appropriate supervision, if necessary.

#### 402.05 Training

An employee on a flexible or compressed work schedule may be required to convert to a traditional 40-hour workweek during pay periods in which he or she has training.

#### 402.06 Participation in Civil Activities

With the approval of the component head, supervisors may excuse full-time employees, without charge to leave or loss of pay, to participate in civil activities that the government has an interest in encouraging. Excusal requests should include documentation establishing government encouragement for the civil activity (i.e. It is in the public interest).

Effective Date 2/26/2018

## 403.00 OIG ASSOCIATE PERFORMANCE PLAN AND APPRAISAL SYSTEM

### 403.01 Purpose

The Associate Performance Plan and Appraisal System is a critical component of OIG's overall Performance Management Process and its purpose is to improve OIG's performance results in achieving its mission while enhancing opportunities for career success of OIG associates.

The OIG follows GSA Order CPO P 9430.1 Extended, "GSA Associate Performance Plan and Appraisal System," except where the provisions in that Order conflict with OIG policy.

### 403.02 Applicability

The policy applies to all OIG non-SES employees.

### 403.03 Legal Authority

In addition to the legal authority cited in CPO P 9430.1, the Inspector General Act of 1978 as amended provides the OIG with independent personnel authority.

### 403.04 Responsibilities

1. The Inspector General has responsibility for the overall direction of OIG's Associate Performance Plan and Appraisal System.
2. The Human Resources Director (JPH) is responsible for overall administration of OIG's Associate Performance Plan and Appraisal System.

### 403.05 Rating Period

The rating period is normally 12 months. Beginning in January 2016, the established period of time for which performance will be reviewed and a performance appraisal (rating of record) will be prepared is January 1 through December 31. Performance appraisals must be completed and entered into CHRIS within 30 days after the end of the rating period unless granted an extension by JP.

The reviewing official may review any and all ratings of associates within their purview.

Effective Date 1/5/2015

## 404.00 COMPENSATION AND PAID OVERTIME WORK

### 404.01 Overview

Overtime work is work performed by an employee in excess of 8 hours in a day or in excess of 40 hours in an administrative workweek. (Time spent in official duty status in excess of 8 hours a day due to work travel does not constitute overtime work.) For employees on compressed schedules (such as AWS 5/4/9), any time worked in excess of the specified scheduled tour of duty is considered overtime. To meet the requirements of Title 5 of the U.S. Code, overtime work must be officially ordered or approved in advance in writing, and the official ordering or approving the overtime work must be authorized to do so. These rules also apply to compensatory time off in lieu of overtime.

### 404.02 Applicability

This policy addresses only overtime for OIG employees who are exempt under the Fair Labor Standards Act. All employees (other than Special Agents and members of the Senior Executive Service) have eligibility for overtime, as set forth in this policy.

### 404.03 Legal Authority

The basic rules for overtime are found in 5 CFR Part 550. The OIG generally follows GSA Order OAD P 6010.4 OAD P, Time and Leave Administration, regarding overtime except where that policy differs from the OIG policy.

### 404.04 General Approvals

Overtime will be approved only to meet an essential need of the OIG. Supervisors and managers should keep all overtime to a minimum and should only approve overtime to meet an essential mission need. Supervisors and managers should authorize overtime only when an exigency precludes the employee from performing the work during the regularly scheduled tour of duty. Exigencies include an immovable deadline or other immediate need. Supervisors and managers should also consider alternatives, such as assigning additional employees to work on the project, the overall importance of the needed task, and whether other options exist. When supervisors and managers approve overtime, they should strive to keep the number of hours reasonable and to a minimum.

Overtime must be approved in advance by officials who have the authority to do so. In emergencies when it is impossible to get advance written authorization, overtime may be permitted but must still be verbally approved in advance.

In addition to the requirements discussed below, OIG personnel should also refer to the GSA Time and Leave Administration Policy when making or approving overtime requests.

JPB does not generally provide overtime budgets for components. If there is a specific need for overtime a request should be made to the Budget Director so that funding can be set aside in advance.

#### 404.05 Procedures

The following procedures apply both to overtime pay and to compensatory time off in lieu of overtime. (The OIG does not use the Authorized Leave and Overtime Help Application used by GSA.)

1. Each approval of overtime remains in effect for only one pay period. Thereafter the approving authority must make a new determination of essential need.
2. Supervisors generally should not grant annual leave on the same day, the day before, or the day after a day for which overtime has been authorized; rather, the supervisor should schedule the work so overtime is not required.
3. The employee requesting overtime should fill out GSA Form 544, Request, Authorization, and Report of Overtime, allowing enough time for approval before the overtime is worked. The employee is responsible for obtaining prior written approval from his/her supervisor by getting the supervisor's signature on the Form 544.
4. The budget director should be made aware of the overtime request via email. If funds are adequate, the budget director will respond back to the requesting official indicating that funding is available for the overtime. This step is not required when the employee is requesting compensatory time off in lieu of overtime.
5. After the overtime work is performed, the requesting employee must fill in the back of the form to report the actual overtime worked. If the hours of overtime worked are higher than the previously estimated hours by 10 percent or more, then the employee must explain the reason on the form and bring it to the attention of the approving official. The approving official signs the bottom of the Form 544 verifying the hours worked and providing final approval of the overtime.
6. In emergencies, overtime work may be requested orally or via email; approval must be obtained before the work is performed and the request must be followed up with a properly executed Form 544 as soon as possible.

Effective Date 12/29/2016

#### 405.00 PERSONNEL SECURITY

GSA policy concerning personnel security is contained in the Suitability and Personnel Security Handbook (ADM P 9732.1D) which the OIG follows except where doing so would be inconsistent with the process explained below. The OIG Policy Manual Chapter 927 details the procedures for pre-employment investigations of OIG applicants.

##### 405.01 OIG Personnel Security Program

All aspects of the OIG personnel security program -- except the pre-employment investigation -- are the responsibility of the OIG Human Resources Division (JPH). The OIG Office of Investigations, Internal Operations Division (JII) is responsible for pre-employment investigations of OIG employees. As noted in ADM P 9732,1D, the GSA Personnel Security Office (GSA PSO) is responsible for the oversight and conduct of investigations to determine an individual's eligibility for a security clearance and ultimately adjudicating completed Office of Personnel Management (OPM) initial investigations and reinvestigations.

##### 405.02 OIG Pre-Employment Investigation

All persons being considered for OIG employment must successfully complete a JI pre-employment investigation prior to entry on duty. The process is as follows:

- a. Once a candidate has been selected, the JPH Staff is responsible for contacting the candidate and initiating the pre-employment investigation. One condition for receiving a formal offer of employment is that the candidate passes a JII pre-employment background investigation. JPH will send the candidate pre-employment paperwork via email, and if the candidate is located in the Washington, DC, metropolitan area, they will also schedule an appointment for the candidate to be fingerprinted. If the candidate is located outside of the Washington, DC, metropolitan area, JPH mails fingerprint cards to the candidate for him/her to take to any local law enforcement office for fingerprinting. The candidate returns the prints by mail back to JPH. JPH then submits the fingerprint cards to JII for processing. JII will notify JPH if the resulting records contain derogatory information; JPH will add this information to the other paperwork received from the candidate.
- b. After JPH receives all pre-employment paperwork from the candidate, they review the initial paperwork for derogatory information. If there is no derogatory information, the paperwork is submitted to the Assistant Inspector General (AIG) for Administration for review and signature. If approved by the AIG for Administration, JPH forwards the paperwork to JII to begin the pre-employment background investigation. If derogatory information is disclosed in the initial paperwork, JPH will notify the AIG for Administration. The AIG for Administration will notify the hiring component head, and together they will determine whether, considering all facts available, it is in the interest of the OIG to proceed with the candidate's pre-employment background investigation.
- c. It generally takes two to six weeks for JII to complete the pre-employment background investigation report. Once the report is completed, JII sends the investigative report to JPH for review. If no derogatory information is found, JPH submits the report to the AIG for Administration for final review and authorization to hire the candidate. If the investigation report discloses derogatory information,

JPH will notify the AIG for Administration. The AIG for Administration will notify the component head and together they will determine whether, considering all facts available, it is in the interest of the OIG to proceed with hiring the candidate.

d. In addition to the pre-employment investigation, Criminal Investigator candidates must pass medical tests and drug screening before they are extended an official offer. JPH is responsible for the drug screen and JI is responsible for the medical testing.

e. When the component head and the AIG for Administration conclude that the applicant's pre-employment investigation is unfavorable and it is not in the interest of the OIG to proceed with hiring the candidate, JPH will notify the candidate via the Quickhire system that he or she was not selected for the position.

Once JPH receives the proceed-to-hire notification from the AIG for Administration, the candidate is extended an official offer. If a candidate is not extended an official offer of employment and seeks to obtain a copy of his or her pre-employment investigative file, he or she must submit a request to the Office of Counsel in accordance with the instructions on the OIG webpage for filing a FOIA or Privacy Act request.

#### 405.03 OIG Personnel Security Requirements

Positions in the OIG are classified in accordance with ADM P 9732.1D. Some OIG positions require Top Secret (TS) security clearances. If an employee holds a TS and requires access to Classified National Security Information (NSI), the supervisor must complete a justification for access. The supervisor writes a justification memo and the component head approves and forwards the memo to JPH. JPH submits the justification to the GSA PSO.

In accordance with ADM P 9732.1D, all OIG employees who hold a TS security clearance and require access to Classified NSI material must receive a GSA security briefing. JPH ensures that all such employees receive the briefing. The employee must complete a Standard Form 312 (SF 312), Classified Information Nondisclosure Agreement, before being granted access to classified material. JPH will send the SF 312 to the GSA PSO for processing via email.

All OIG employees who hold a TS security clearance and sign an SF 312 granting them access to NSI must be debriefed when they leave the OIG. JPH ensures that all such employees are debriefed and sign the SF 312 under the Security Debriefing Acknowledgement section. JPH is responsible for submitting the acknowledgment to the GSA PSO.

#### 405.04 OIG Personnel Security Requirements for OPM Background Investigations

All new OIG employees. Once new employees are on board, JPH arranges for a full background investigation to be conducted by OPM. JPH acquires a Pegasys number for funding the investigation and submits required paperwork to GSA PSO to begin the investigation.

Reinvestigations. All OIG employees are required to complete a reinvestigation every five years. When an employee's reinvestigation is due, JPH will obtain a Pegasys number for funding, enter the employee in e-QIP, and send the employee instructions for completing the investigation.

Effective Date 3/16/2018

## 406.00 OIG TRAVEL POLICY

### 406.01 Purpose

The policy sets forth the standards and procedures governing OIG employee travel in connection with OIG operations. In addition to the Federal Travel Regulations, GSA policy on travel is contained in GSA orders:

- 5700.1 CHGE 1 OAS Temporary Duty (TDY) Travel Policy
- 5730.1 OAS GSA Relocation Allowances
- 5735.1 OAS Travel Advances
- 5740.1 OAS Government Travel Charge Card Program
- 5765.1 OAS GSA Non-Federal Source (NFS) Travel Policy
- 5770.1 OAS Local Travel
- 5775.1 CHGE 2 OAS Foreign Travel Policy

### 406.02 Local Travel

Local travel is defined as that travel performed within and adjacent to the official station of an employee when the travel is necessary to conduct official business for the OIG and is performed by the most direct route within and adjacent to an employee's official worksite/duty station or appropriate alternative worksite. Reimbursement will be limited to the constructive amount of using the most advantageous method of travel.

#### 406.02A Designation of Local Travel Areas

The local travel area for Central Office employees whose official worksite/duty station is in the Washington, DC metropolitan area has been established as follows: The District of Columbia, the cities of Alexandria, Fairfax, and Falls Church in Virginia; Arlington and Fairfax Counties in Virginia; and Montgomery and Prince George's Counties in Maryland.

The GSA Regional Administrator will designate the local travel area for GSA employees, including OIG employees whose (1) official station is outside of the Washington, DC metropolitan area and (2) offices are co-located with GSA offices.

The local travel area for regional OIG employees whose offices are not co-located with GSA offices is comprised of the fifty mile radius from the employee's duty station.

#### 406.02B Use of Privately Owned Vehicles

Privately owned vehicles (POV) may be used to perform local travel on a mileage basis at rates not to exceed those specified at [GSA.gov](http://GSA.gov) (POV Mileage Reimbursement). Reimbursement for local travel by POV will be for the actual distance traveled in excess of normal commuting mileage. For employees who engage in local travel on non-commute or no-cost commute days (e.g., telework), reimbursement will be based on the actual distance traveled.

NOTE: When an employee uses a mode of transportation for commuting that is different from what he/she normally uses, all expenses an employee normally incurs when commuting are non-reimbursable expenses. Employees will not be reimbursed for any "unused" public transportation expenses such as Metro or buses.

#### 406.02C Tokens, Tickets and Passes ("Transit Passes") Maintained by the OIG

OIG offices located where mass transit services are available may find it advantageous to have a set number of transit passes available for travelers to use when taking mass transit on official agency business. The transit passes may only be used for official business and may not be used for travel between a duty site and the employee's residence.

Any office that chooses to purchase such transit passes must keep adequate records to account for the purchases and official uses by using the fare card log, which shows amounts spent on cards and usage by each employee. See Appendix A.

#### 406.02D Public Transit and Private Transportation

OIG employees who incur expenses for private (e.g. taxis, commercial shuttles, etc.) or public transportation (e.g., transit passes, bus fare) for official local travel between duty sites may be reimbursed; reimbursement will be based on the actual fare between the duty sites. Employees who incur expenses for private or public transportation for official local travel between their residence and the duty site (not their official station) may be reimbursed the actual fare minus their normal commuting costs; employees who incur expenses for private or public transportation for local travel between their residence and the duty site on a non-commute or no-cost commute day (e.g., telework), reimbursement will be based on the actual fare.

NOTE: When an employee uses a mode of transportation for commuting that is different from what he/she normally uses, all expenses an employee normally incurs when commuting are non-reimbursable expenses.

#### 406.02E Use of Government Owned Vehicles

OIG employees that have been individually-assigned a Government Owned Vehicle (GOV) should use their GOV for local travel.

#### 406.03 Special Travel Situations

##### 406.03A Allowable Upgrades

OIG-funded upgrades, if allowable, must be approved by the Deputy Inspector General (DIG) or the Assistant Inspector General (AIG) for Administration. The OIG will not approve reimbursement for expenses associated with early boarding or changing seats for personal preference.

#### 406.03B Non-Federal Source Travel

Acceptance in kind of travel and subsistence expenses in connection with official travel by OIG personnel from a non-federal source must be approved in advance by the DIG and shall be coordinated with the Office of Counsel to the Inspector General (JC).

#### 406.03C Interview Trips

(1) Eligibility. Authorizing officials shall limit payments to no more than two candidates for positions at the GS-15 level or higher. Any additional interview travel must be authorized by the DIG.

(2) Interviewing offices' responsibilities. Each interviewee should be provided a Fact Sheet which includes all OIG travel requirements. See Appendix B. The interviewee should work with JPB in making travel arrangements through the travel management center contractor (e.g., AdTrav).

Authorizing officials should not approve expenses for rental car fees or internet access charges. With respect to other expenses, authorizing officials should not approve any expenses outside those normally approved for OIG employee travel (e.g., hotel charges, meals and incidental expenses, tolls, taxis). Authorizing officials may approve lodging expenses for one night per candidate and only if the interview site is located outside the 100 mile radius from the candidate's home.

#### 406.04 Actual Expense Method

Travel on an actual expense basis due to unusual circumstances may be authorized only by the DIG.

#### 406.05 Miscellaneous Expenses

##### 406.05A Necessary Use of Communication Services

Supervisors may authorize reimbursement for internet access charges incurred while on official travel. OIG employees should connect portable computing devices to the internet using their government-issued mobile phones (tethering) or wireless aircards, if available. Reimbursement for internet charges will normally be limited to \$15 per day; supervisors may approve reimbursement at a higher rate when unusual circumstances exist.

#### 406.06 Foreign Travel

##### 406.06A Authorization

Official travel to locations outside the conterminous United States (CONUS) must be authorized by the Inspector General (IG) or Deputy Inspector General (DIG). This approval can be obtained via email.

This rule does not apply to official travel by OIG employees in Regions 2, 9 and 10 to areas within their respective regions. Thus, AIGs (or their designees) may approve travel to locations outside CONUS that are still within GSA regions for OIG employees in Regions 2, 9 and 10.

There are three necessary steps, outlined below, for official foreign travel:

1 – Obtain an Official Passport

- 2 – Obtain a Visa if required by the particular country of travel
- 3 – Obtain Country Clearance
- 4 – Contact GSA Threat Management Office for briefing/debriefing

#### 406.06B Official Passport

OIG employees proceeding abroad on official business are issued an official passport of a distinctive maroon color by the Department of State, Passport Office. An official passport must not be used for personal business or pleasure travel; however, it may be used by the bearer for incidental personal travel while abroad, en route to, or returning from a foreign destination on official business, providing the foreign government(s) do not object. Official passports are valid for a 5 year period, if the bearer maintains his official status. There is no fee for issuance or renewal of an official passport.

(1) Eligibility. Obtaining an official passport is mandatory in the OIG for official foreign travel.

(2) Responsibility of traveler. The employee going on official travel shall access the following GSA website for instructions and procedures on obtaining an official passport  
<https://insite.gsa.gov/portal/content/617606>.

Please note this website states the employee "may" request a no-fee official passport, however, it is a mandatory requirement for OIG employees to obtain an official passport for foreign travel.

(3) Control of Passports.

Travelers will receive their passport from GSA, Office of Administration, Travel Policy and Charge Card Program either in person or via express mail. It is extremely important that passports be safeguarded while in the possession of the traveler.

Passports are the property of the United States. The traveler must return the passport to GSA as stated in the above mentioned GSA website for cancellation upon leaving the agency.

#### 406.06C Visas

A visa is an endorsement made on a passport by proper authorities of the country to be visited. Not all countries require visas.

The employee going on official travel shall access the following GSA website for instructions and procedures on obtaining a Visa: <https://insite.gsa.gov/portal/content/617606>. Access the Department of State link at this website – Visa Requirements for specific country information.

#### 406.06D Department of State Country Clearance

All proposed official travel by any OIG employee regardless of grade or position that involves travel to a foreign country may require prior clearance and coordination with the Department of State.  
<https://ecc.state.gov>

Official travel to Mexico and Canada do not require State Department clearance unless the travel is to the U.S. Embassy in Mexico City or Ottawa.

The traveler is responsible for obtaining the clearance. The Department of State ECountry Clearance (eCC) User Manual provides guidance on obtaining the country clearance.

#### 406.06E Security Briefing/Debriefing

The OIG generally follows ADM P 5400.1, Meetings with Representatives of Foreign Governments or Foreign Industry, Foreign Travel, and Foreign Contacts, except where it prohibits GSA employees from taking Government-furnished electronic devices on foreign travel unless cleared by the CSO and IT support (OCIO). In accordance with that policy, all OIG employees are encouraged to contact the GSA Threat Management Office before embarking on foreign travel, and all OIG employees with a security clearance (top secret) are required to notify the GSA Threat Management Office at least two weeks before they travel outside the United States (threat-management-office@gsa.gov). This includes personal travel. The OIG employee may be provided a travel briefing before departure and a security debrief upon return.

If electronic loaner devices are requested by OIG employees on foreign travel, then JPM will issue any necessary devices and ensure they are wiped immediately upon their return to JPM. JPM devices are not authorized to store or process any Top Secret (TS) or Sensitive Compartmented Information (SCI).

#### 406.07 Travel Reservations

OIG employees must use the GSA electronic travel system (e.g., ConcurGov) to make all travel reservations for common carrier (airplane and rail), lodging and rental cars, except in limited circumstances. Where circumstances warrant (i.e. security and viability of an OIG operation), OIG employees may book hotel rooms directly through the Fedrooms.com website or, if lodging is not available through Fedrooms, through the websites of non-Fedrooms properties. Supervisory approval is required to use this exception.

#### 406.08 Travel Authorizations

##### 406.08A Annual Authorizations

OIG JI employees may continue to use Annual Travel Authorizations or open authorizations (OA).

#### 406.09 Travel Advances

Use of cash advances must comply with the Federal Travel Regulation and GSA Order OAS 5735.1, should be kept to a minimum, and should be limited to pay for official government travel expenses that cannot be charged to a travel card.

#### 406.10 Moving Expense Allowances

Travel, transportation and other applicable relocation/moving expenses must be approved by the IG or DIG. Once approved, JPB will work directly with the employee or candidate to ensure that all paperwork is completed and approved as required by the GSA Order OAS 5730.1 GSA Relocation Allowances.

## 406.11 Travel Card

### 406.11A Delinquency

Travel vouchers must be filed within five working days after completing travel to avoid delinquency.

The travel card is a charge card, not a credit card; cardholders are not authorized to carry a balance forward. A cardholder must make payment for all undisputed charges on their travel bill in full by the statement billing due date (30 calendar days from the closing date on the statement in which a charge appeared). The due date is printed on the bill. Failure to pay the monthly bill in a timely manner may result in the loss of charging privileges. If the account is suspended, the cardholder will be unable to use it until the bank receives payment. If the account is canceled due to non-payment, the delinquency maybe reported to credit bureaus, be referred to collection agencies, or lead to other collection actions and the cardholder may not be eligible to receive a new account.

There are no exceptions to this requirement. Delinquent cardholders are subject to administrative or disciplinary action in accordance with GSA policy CPO 9751.1, Maintaining Discipline.

As part of the OIG quality assurance function, JE administers the OCFO questionable charges and delinquent account inquiries pertaining to OIG purchase cards and travel cards. (Please see Chapter 1005.12). JE sends a Travel Card Delinquency Memorandum to the employee's component head and/or supervisor in the event of an outstanding travel card balance. In the event of a third offense, the supervisor must contact JP and JC for guidance.

Effective Date 10/21/2016

## 407.00 RECORDS MANAGEMENT, INCLUDING HANDLING ELECTRONIC RECORDS

This section provides guidance to OIG officials on managing the electronic records, legacy (paper) records, and other electronic information that OIG personnel create or receive during the course of their official duties. This section supplements GSA's records management policy and procedure established through OAS P 1820.1, GSA Records Management Program, which the OIG follows except to the extent that it is inconsistent with any OIG policy.

### 407.01 "Record" Defined

44 U.S.C. § 3301 defines a record as any item, "regardless of physical form or characteristics," that is "evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government" or that is appropriate for preservation "because of the informational value of the data" in it. Put another way, records consist of documentary information that a federal agency preserves, or that is otherwise appropriate for preservation, as evidence of the agency's actions. Records may exist as books, papers, electronic materials, photographs, video, or other documentary materials, regardless of physical form or characteristics.

An item most likely constitutes a record if it meets any of these criteria:

- It was distributed to employees to perform government business, such as approval, comment, action, recommendation or follow-up, or to otherwise communicate agency business;
- The OIG or another government entity required the creation of the item;
- The item is kept in agency files (as opposed to the employee's personal possession); or
- The item is a duplicate of a record and contains annotations that add to understanding of the organization's policies, decisions, actions, or responsibilities.

An item most likely does not constitute a record if it meets any of these criteria:

- The item does not contain substantive information about agency business (for example, communications setting up meeting times are generally not substantive);
- The item was created solely for an employee's convenience and own use;
- The item serves merely as a sample, "go by," generic reference, etc.; or
- The item is a mere duplicate of a record (only one copy of a record need be kept).

Additional information on whether an item constitutes a record can be obtained by viewing the local file plan, consulting with the component Records Liaison, OIG Records Officer or GSA Senior Records Officer, or checking NARA's records management guidance at 36 C.F.R. parts 1220 through 1239.

### 407.02 Responsibilities

44 U.S.C. § 3101 requires that the "head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities."

All OIG employees are responsible for managing the records that they create and receive, as follows:

- Preserve all records
- In an appropriate format
- In an approved storage location and
- Not destroy such documentary information prior to the end of the lifecycle maintenance period designated in the applicable NARA-approved schedule.
- Additionally, for records maintained in a storage location that only the employee has access to (such as the limited circumstances of storing records on an individual network drive ("I Drive")) the employee must dispose of the record at the end of its lifecycle per the instructions of the applicable NARA-approved schedule.

OIG managers have the following records management responsibilities:

- Ensure that the offices and staff under their supervision preserve all documentary information that they create and receive in appropriate format in an approved storage location;
- Ensure that the offices and staff under their supervision maintain all records for the required lifecycle and dispose of all records in the fashion authorized at the end of the lifecycle; and
- Ensure that the offices under their supervision maintain an accurate file plan.

Each OIG component will designate a Records Liaison, who has the following responsibilities:

- Serve as the primary point of contact for the component on records management issues;
- Provide guidance and assistance component-wide on records management; and
- Maintain a component-wide file plan, and update the OIG Records Officer when changes occur.

The OIG Records Officer has the following responsibilities:

- Serve as the OIG's Records Management Coordinator (RMC);
- Liaise with the agency on records management issues;
- Provide guidance and assistance OIG-wide on records management;
- Maintain an OIG-wide file plan, and notify both JPM and the GSA Senior Records Officer when changes occur;
- Identify new and unscheduled records, and work with NARA appraisal staff to schedule all unscheduled records;
- Promptly disseminate newly approved records schedules and General Records Schedule items to OIG staff; and
- Recommend changes to the OIG records management policy when appropriate.

#### 407.03 File Plan

A file plan consists of a list of each series of records (e.g., leave slips, purchase card documentation, supporting documentation for the Semiannual Report) controlled by an organizational entity (such as a field office or an OIG component). A file plan must also contain the following information pertaining to each series: schedule number or identifier, maintenance period (lifecycle), cutoff (formula for determining the date when the maintenance period begins), approved storage location, and disposition instructions.

Each individual OIG office (i.e., field offices, support offices, and program offices) and each OIG component must keep an accurate file plan. Offices should review and update their file plans periodically. Offices should report file plan changes to component Records Liaisons, who in turn report changes to the OIG Records Officer.

#### 407.04 File Naming Conventions

Components will establish a naming convention for electronic records stored on the shared drive. File and folder conventions may include the official project name, the year in which the project began, and the OIG official assigned primary responsibility for working on the project.

#### 407.05 Approved Storage Systems

OIG components must designate the official file system (storage location) for every record that the component creates or receives. Key OIG approved file systems include the following:

- IBM Notes mailbox and Archive/Capstone Vault
- E-IDEAS;
- TeamMate;
- Counsel Information System (CIS);
- Local shared drives (if approved by an OIG office head as an official repository for records);
- Individual network drives, as approved by supervisors in those instances in which sensitive materials must not be accessible by other members of an office (e.g., a supervisor's materials regarding employee performance or discipline, or electronic leave submissions);
- Certain GSA-operated systems, such as Pegasys (financial records) and ConcurGov (travel records);
- Portable media (CDs, DVDs and flash drives) if approved by a component head; and
- File cabinets for paper files.

The following media do not constitute approved file systems and cannot be used to store records:

- Voicemail inboxes; and
- Portable electronic communications devices (i.e., text or SMS messages).

#### 407.06 Transfer of Records to Official File Systems

If an employee receives or creates a record using a non-approved file system, the employee must transfer the record to an approved system. The preserved record must contain all pertinent information, including metadata, needed to meet agency business needs, such as the names of the sender and all participants, the date, and any attachments that are an integral part of the record. These documents (when they are official records) should be transferred as follows:

- Email: employees should save emails (or printed or PDF copies of emails) in an official file system.
- Instant messaging: employees should save the conversation into an official file system by selecting "Save Chat As..." from the IM window's "File" menu as soon as they have completed the conversation. (This method preserves more metadata than saving the text of the conversation in a Word document.)
- Text messaging, BlackBerry and iPad documents: employees should email copies of conversations to themselves as soon as the conversation or document is finished, and save the email in an official file system.
- Digital photography: employees should send photographs to themselves via email, and save the email in an official file system.
- Video chatting and Video Conferencing (VTC): at this time, these materials are not preserved, with the exception of employee training presentations. JPM assistance is necessary to record training presentations.
- Voicemail messages: employees should save digital voicemail messages that constitute official agency records as digital recordings in an official file system, with the assistance of JPM. If the message is in an

analog voicemail system (i.e., on a phone that does not have VOIP), the employee should transcribe the content of the message and save the transcription in an official file.

- Portable media and items on network and hard drives: except where these media are part of an office's approved method of maintaining official files, employees should transfer records stored on these media into an official file system.
- Other platforms, including web-based: employees should save these materials in the format best suited to preserve the entire content (i.e., pasting text into a document; making a screen capture; saving a webpage using the "Convert Web Page to PDF" tool; etc.), and save the material in an official file system.

Because many electronic media are transient, and because employees may not remember to transfer records if they delay in doing so, employees who use portable electronic devices to conduct substantive agency business should preserve them as soon as possible or at the latest within five workdays of creation or receipt.

#### 407.07 Email Systems

For conducting official business, OIG employees may only use their agency-administered email account; they may not use personal email accounts to conduct official OIG business. JPM is responsible for ensuring that the agency-administered email accounts retain the intelligent full names on directories or distribution lists to ensure identification of the sender and addressee(s) of messages relating to OIG business.

#### 407.08 Capstone

Management Directive M-12-18 requires that agencies electronically manage temporary and permanent email records by December 31, 2016. "Email records" are email messages that fall within the definition of federal records. NARA advises that all agency-administered email accounts likely contain federal records. Generally, all email messages pertaining to official duties constitute federal records, except blast emails sent to large groups of employees. (See 407.01 for the full definition of a federal record.)

To meet the M-12-18 requirement, the OIG adopts the National Archives and Records Administration (NARA) "Capstone Approach" for managing email records. Under the Capstone approach, the OIG manages email records and attachments at the account level, meaning OIG personnel use their assigned email accounts for official communications, when deemed appropriate, and by default an automated process manages their email records. Email users have the flexibility to manipulate and organize their email account, including:

- Sending, receiving, forwarding, and printing email messages.
- Creating folders and subfolders, and moving email messages within those folders.
- Culling personal messages and email not related to their official capacity during the first 90 days after the message enters the system (LotusNotes), whether sent or received.
- Deleting email messages when they do not meet the definition of a record.

OIG personnel may not delete an email message when it meets the definition of a record, as the willful destruction of a federal record constitutes a felony (see 18 U.S.C. § 2071). However, personnel may delete an email message from their OIG-assigned account after they have cross-filed the email in a different approved storage system (407.05). For example, once an auditor preserves an email message in TeamMate as part of an audit file, the auditor may delete the original email message in LotusNotes, as

TeamMate now holds the official copy of the record. Additionally, OIG personnel may remove non-records by "culling" within the first 90 days of when the email arrives in the system. After 90 days, the Capstone process labels the email as a federal record, which the user no longer has authority to delete. NARA requires internal controls to protect against records destruction, such as preventing deletion.

Pursuant to the Capstone implementation authority granted by NARA (Form NA-1005), the OIG designates the following positions as Capstone officials:

- Inspector General
- Any person acting as the Inspector General longer than 60 days

JPH will notify JPM when it processes any individual into or out of a Capstone position, including someone temporarily in an acting capacity, such as under the Federal Vacancies Reform Act of 1998, 5 U.S.C. §§ 3345-3349d.

The cutoff period for all OIG email records occurs at the end of the fiscal year. For Capstone officials, the OIG will accession (transfer) their email records to NARA as permanent records 15 years after cutoff. For all other accounts, the automated system will delete (destroy) their email records 10 years after cutoff.

OIG personnel may preserve email messages for a longer period by using these options, when applicable:

- Cross-file the email record in another OIG-approved records management system, when the email falls within the definition of a different records group with a longer life cycle.
- Click on the "Submit Permanent Record" button, when a non-Capstone official has a permanent email message and the user's office does not have an approved storage system (407.05) for that type of record.
- Print or save the email outside of the email system, as a non-record convenience copy, "go-by," sample, or reference document (see 407.01). This process does not negate the requirement to keep the official record copy in the email system for the required life cycle.

The Capstone approach applies to legacy email records (meaning the process applies retroactively). To implement Capstone for legacy email records, the system will allow a safe harbor period of one year, during which personnel may cull (delete) non-records and preserve email older than 10 years, using the methodologies described above.

#### 407.09 Disposition

At the end of a record's lifecycle, the record custodian should follow the required disposition instructions, as noted on the file plan. Temporary records must be destroyed to such an extent that the content cannot be retrieved. Permanent records must be accessioned to NARA. Unscheduled records may not be destroyed until NARA approves a schedule for the records.

If an OIG employee believes that the NARA-approved maintenance period no longer meets OIG business needs for keeping records, then the employee should contact the component Records Liaison or OIG Records Officer immediately to report this issue. If the component head agrees with this assessment, then the OIG Records Officer shall apply to NARA to have the applicable schedule changed. The employee should refrain from destroying the pertinent record(s) until the OIG Records Officer resolves the matter with the component head and/or NARA.

Employees must obtain supervisory approval before taking any copies of records when they leave the OIG.

#### 407.10 Senior Official Exit Briefing

The exit briefing required by GSA policy on the appropriate disposition of the records, including email, under the immediate control of senior officials may be given by the OIG Records Officer or designee, or the GSA Senior Records Officer, who must document the briefing for inclusion in the senior official's exit papers.

#### 407.11 Quality Assurance

JE operational reviews should include a review of the subject office's records management operations to ensure that it is efficient, effective, and compliant with applicable records management laws and regulations. Managers should also conduct their own internal reviews of their records management program.

#### 407.12 Vital Records

Vital records are defined by regulation as those records needed to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities. JP has responsibility for administering the OIG's vital records program, including the following:

- Identifying the vital records of all OIG program and administrative areas;
- Reviewing the vital records inventory annually; and
- Including the vital records plan as part of the Continuity of Operations (COOP) plan.

#### 407.13 Litigation Holds

JC oversees litigation holds within the OIG, including initiating, reviewing, and lifting freezes on the disposition of records. OIG personnel must cooperate with JC when notified of a litigation hold. When JC identifies a category of records as falling within a litigation hold, the records' disposition requirement becomes frozen until JC declares the litigation hold lifted. In other words, no custodian may destroy a record that is subject to an active litigation hold even when the file plan calls for destruction.

#### 407.14 Controlled Unclassified Information [RESERVED]

#### 407.15 Information Technology

When migrating stored records and associated metadata to new storage system, JPM must ensure that records are retrievable and usable as long as needed to conduct agency business and to meet NARA-approved dispositions. JPM must ensure that the records management functionality, including the capture, retrieval, and retention of records according to agency business needs and NARA-approved schedules, is incorporated into the design, development, and implementation of all new systems.

JPM will involve the OIG Records Officer or the affected component Records Liaison when migrating records from retired systems or when designing, development and implementing new systems. When

the OIG rolls out new electronic systems, JPM should ensure that the user documentation includes guidance on the systems' records management considerations.

JPM must maintain an inventory of electronic information systems and whether each system is covered by an approved NARA disposition authority. Additionally, JPM must maintain an inventory of all cross-component shared drives, including the name of the records custodian for the drive.

#### 407.16 Former Employees' Data

As noted above, employees have an ongoing duty to preserve documents in an official agency file system. "Former employee's data" means electronic data that was stored by the employee such that only he/she had access to it (i.e., email, hard drive (C: drive), individual network drive (I: drive), portable hard disk drives, external memory storage media and devices), and accordingly it is not in an official agency file system. JPM will coordinate with JC to determine if a former employee is on a litigation hold or if that employee's data should be retained for litigation purposes. Even though all employees are required to preserve documents in official agency file systems, the OIG will err on the side of document preservation when litigation is involved. When an employee leaves the OIG, in addition to coordinating with JC, JPM will notify the former employee's supervisor(s), who will assess whether agency records are being kept outside of an official agency file system and, as appropriate, migrate the former employee's data into an official agency record system, another OIG employee's files or a group repository (e.g., the H: drive). The former employee's supervisor(s) may request that the files be retained for some period of time while the migration is completed. If JC and the supervisor advise that the documents do not have to be preserved for litigation or other purposes, then JPM may destroy the former employee's data 90 days after the employee leaves the OIG. If JC or the supervisor asks for the documents to be kept, then JPM will preserve them until it is advised that the documents can be destroyed.

Effective Date 5/4/2017

## 408.00 CREDENTIALS AND/OR BADGES

### 408.01 OIG Policy on Issuance of Credentials and/or Badges

Credentials and/or badges are issued to assist OIG employees in the performance of official duties. After being sworn for duty with GSA OIG, (1) special agents are issued badges and credentials and (2) all other employees are issued credentials.

JI is responsible for issuing and reissuing credentials and badges when necessary. OIG employees are responsible for: (1) safeguarding credentials and/or badges issued to them; and (2) exercising due care to prevent the loss, defacing, altering, and mutilating of issued credentials and badges. The employee is responsible for returning his/her badge and/or outdated credential to JI.

The following specific policies and procedures apply to the carrying, use, presentation, loss, and updating of OIG badges and/or credentials.

### 408.02 Carrying Badges and/or Credentials

Special agents must carry their credentials and badges when carrying their issued firearm as specified in Subchapter 902. All other OIG employees may carry their credentials when on duty. All employees may carry their badges and/or credentials when off duty; however, employee use of these items is governed by section/paragraph 408.03 below.

### 408.03 Use of Badges and/or Credentials

OIG badges and/or credentials may be used only as identification when conducting official OIG business.

### 408.04 Proper Presentation of Badges and/or Credentials

When conducting official OIG business, special agents shall present their credentials and badges and verbally identify themselves as OIG Special Agents unless precluded from doing so by the nature of the specific assignment, (b) (7)(E).

All other OIG staff should identify themselves through the presentation of their credentials to avoid any situation that might lead to embarrassment, misunderstanding, or complaints for failure to present proper identification.

### 408.05 Loss of Badges and/or Credentials

OIG employees are to exercise every precaution necessary to prevent the loss of credentials and/or badges. Special agents who lose their credentials and/or badges shall follow the procedures below:

- The employee shall: (1) immediately report the loss (verbally or in writing) to the office head (SAC or AIG for Investigations) through his/her immediate supervisor, if applicable; and then (2) compose and submit a written statement to the SAC (in the case of regional employees) or AIG for Investigations (in

the case of Central Office employees) detailing the circumstances of the loss and the steps taken to locate the credential and/or badge.

- The SAC or AIG for investigations will then notify both the Deputy Inspector General and the appropriate local, state, and Federal law enforcement agencies to affect entry into the National Crime Information Center system. If it is more expeditious, entry may be accomplished through the Federal Protective Service Regional Control Center.
- The SAC or AIG for Investigations shall examine all circumstances involved in the loss and send a written statement of findings to his/her supervisor along with the employee's statement.
- The responsibilities of the SAC and AIG for Investigations listed above may be delegated.

All other OIG employees who lose their credentials shall follow the procedures below:

- The employee shall: (1) immediately report the loss (verbally or in writing) to the office head (RIGA/SAC, AIG for Audits, AIG for Investigations, AIG for Administration, Counsel to the IG or division/staff director), through his/her immediate supervisor, if applicable; and then (2) compose and submit a written statement detailing the circumstances of the loss and the steps taken to locate the credential to the office head.
- The office head shall examine all circumstances involved in the loss and send a statement of findings to his/her supervisor along with the employee's statement.
- Information copies of both the office head and employee statements shall be sent to the SAC (in the case of regional employees) or to the AIG for Investigations (in the case of Central Office employees).
- The responsibilities of the office head above may be delegated.

If the loss of the badge and/or credential is deemed to be the result of theft, the RIGA/SAC, AIG for Audits, AIG for Investigations, AIG for Administration, Counsel to the IG or division/staff director, may request a full investigation by JI of circumstances surrounding the loss. Reissuance of the credential and/or badge in all cases shall be approved by the AIG for Investigations.

#### 408.06 Failure to Safeguard Badges and/or Credentials

Employees who fail to safeguard their badges and/or credentials may be subject to disciplinary action up to and including removal from federal service. Supervisors of the employee in question, who have been delegated the appropriate authority, must follow section 103.01(g) to discuss potential action.

If the loss of the badge and/or credential is deemed to be the result of theft, the RIGA/SAC, AIG for Audits, AIG for Investigations, AIG for Administration, Counsel to the IG or division/staff director, may request a full investigation by JI of circumstances surrounding the loss. Reissuance of the credential and/or badge in all cases shall be approved by the AIG for Investigations.

#### 408.07 Issuance of Retired Law Enforcement Credentials

Section 408.07 updated April 17, 2013.

#### 408.07A Background

The Law Enforcement Officers Safety Act Improvements Act of 2010 (Act), as amended, exempts qualified retired law enforcement officers from State laws prohibiting the carrying of concealed firearms. The Act specifically excludes from the definition of firearm a machinegun, silencer, or any destructive device defined in section 18 U.S.C. § 921 (including a bomb, grenade, poison gas or mine). Also, the Act does not override State laws that permit private persons or entities to prohibit the possession of a concealed firearm on their property, or the possession of firearms on any State or local government property, installation, building, base, or park.

The Act does not convey any law enforcement authority. Thus, it does not authorize the carrying of a firearm on a commercial airline. In addition, the test for obtaining Department of Justice representation in connection with a critical incident is not affected by the Act. There are no circumstances in which retired agents will be deemed to be acting within the scope of official government duties.

The Act specifically excludes from its coverage any retired agent who is under the influence of alcohol or another intoxicating or hallucinatory drug or substance while carrying a concealed firearm and any individual who is prohibited by Federal law from receiving a firearm. Under Title 18 of the United States Code, prohibited persons include:

- (1) those under indictment for or convicted of a crime punishable by imprisonment for a term exceeding one year;
- (2) fugitives from justice;
- (3) unlawful users and/or addicts of any controlled substances;
- (4) those adjudicated as mentally defective or who have been involuntarily committed to a mental institution or otherwise judged incompetent to handle their own affairs;
- (5) illegal aliens or aliens admitted to the United States under a nonimmigrant visa;
- (6) those dishonorably discharged from the U.S. Armed Forces;
- (7) those who have renounced their U.S. citizenship;
- (8) subjects of a protective order; and
- (9) those convicted of a misdemeanor crime of domestic violence.

#### 408.07B Policy for Retired Special Agents

Upon written application, the OIG will provide photographic identification indicating that the holder is a retired law enforcement officer to any OIG Special Agent who meets the following standards:

- separated from service in good standing;
- before such separation, was authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law, and had statutory powers of arrest;
- before such separation, was regularly employed as a law enforcement officer for an aggregate of 10 years or more; or separated from service with such agency, after completing any applicable probationary period of such service, due to a service-connected disability, as determined by such agency;

- has not been officially found by a qualified medical professional employed by the agency to be unqualified for reasons relating to mental health and as a result of this finding will not be issued the photographic identification described in the Act; or, has not entered into an agreement with the agency from which the individual is separating from service in which that individual acknowledges he or she is not qualified under this section for reasons relating to mental health and for those reasons will not receive or accept the photographic identification as described in the Act;
- attests that he or she is not prohibited by Federal law from receiving a firearm; and
- provides authorization for the OIG to perform a check of the National Crime Information Center (NCIC) database for the purpose of verifying that the retiree is not prohibited by Federal law from receiving a firearm.

In addition to obtaining photographic identification, in order to carry a concealed weapon, separated agents must possess a certification issued by the State in which they reside that indicates that they have, within the last year, met, at the expense of the individual, the standards for qualification in firearms training for active law enforcement officers, as determined by the former agency of the individual, the State in which the individual resides or, if the State has not established such standards, either a law enforcement agency within the State in which the individual resides or the standards used by a certified firearms instructor that is qualified to conduct a firearms qualification test for active duty officers within that State. The OIG will not reimburse retired agents for any cost associated with this qualification requirement or provide firearm qualification testing for retired Special Agents.

#### 408.07C Procedures for Retired Special Agents

Upon receipt of written request for issuance of retired law enforcement official credentials, the OIG will forward standard letter (Figure 408-01), including an application for law enforcement credentials (Figure 408-02) to the applicant. The application must be notarized before submission to the OIG. Upon receipt of the application, the OIG will conduct all necessary checks to ensure that the retiree is qualified to receive credentials. If the application is approved and applicant is deemed qualified, the OIG will notify the applicant of the approval by letter (Figure 408-03) and require the applicant to submit a color passport photograph and sign a credential card.

Upon receipt of the photograph and signed card, law enforcement credentials will be issued to the applicant. All documents obtained during the application process will be maintained on file in GSA OIG headquarters.

#### 408.07D Procedures for Current Special Agents

Upon separation of current GSA OIG Special Agents, retired law enforcement official credentials will be issued to an OIG Special Agent who meets the following standards:

- separated from service in good standing;
- before such separation, was authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law, and had statutory powers of arrest;

- before such separation, was regularly employed as a law enforcement officer for an aggregate of 10 years or more; or separated from service with such agency, after completing any applicable probationary period of such service, due to a service-connected disability, as determined by such agency;
- has not been officially found by a qualified medical professional employed by the agency to be unqualified for reasons relating to mental health and as a result of this finding will not be issued the photographic identification described in the Act; or, has not entered into an agreement with the agency from which the individual is separating from service in which that individual acknowledges he or she is not qualified under this section for reasons relating to mental health and for those reasons will not receive or accept the photographic identification as described in the Act.

The supervisory official for the retiring Special Agent will transmit via email a request for retired law enforcement official credentials to the AIG for Investigations. Upon approval by the AIG for Investigations, JI will issue a set of retired law enforcement official credentials for the retiring Special Agent.

Retiring Special Agents will be provided a copy of the Act (Figure 408-04) and advised of the necessity of obtaining State certification prior to carrying a concealed weapon.

#### 408.07E Procedures for Re-issuing Photographic Identification

Replacement of qualified retired law enforcement officers' identification is authorized only where the former employee: (1) substantiates in writing that his or her previously-issued qualified retired law enforcement officer identification has been lost, stolen, or destroyed; (2) provides a copy of the police report attesting to such loss or theft; and (3) includes a notarized copy of their State of residence's certification that they have, not less recently than one year before the date the individual intends to carry a concealed firearm, been tested or otherwise found by the State to meet standards established by the State for training and qualification for active law enforcement officers to carry a firearm of the same type as the concealed firearm. Costs for replacing lost or stolen photographic identification may be charged, at the discretion of the GSA OIG, to the retired employee.

Upon receipt of written request for re-issuance of retired law enforcement official credentials, the OIG will forward standard letter (Figure 408-01), including an application for law enforcement credentials (Figure 408-02) to the applicant. The application must be notarized before submission to the OIG. Notwithstanding the required additional documentation, requests for replacement photographic identification will be processed under the same standards as initial requests.

#### 408.08 Procedures for Returning Credentials and Badges

JI is responsible for issuing and disposing of all GSA OIG credentials and badges. Upon separation of current GSA OIG employees, credentials and badges must be returned to JI. The office head of a retiring GSA OIG employee, may submit a request (verbally or in writing via email) to JI to have the employees credentials voided. The request should be submitted to the SAC (in the case of regional employees) or to the Director of Operations for Investigations (JI-O) (in the case of Central Office employees) prior to voiding the credentials.

Effective Date 3/26/2013

#### 409.00 STAFF REASSIGNMENT

##### 409.01 Reassignment Policy

Fulfillment of the OIG mission may require the reassignment of employees to different positions and geographic locations. To the maximum extent possible, reassignments are made consistent with the employee's preference and concurrence. However, mission related requirements of the organization may require reassignment without employee concurrence.

##### 409.02 Positions Subject to Reassignment or Relocation

Management retains the right to reassign employees at any grade level to different organizational or geographic locations in order to promote the efficiency of the service. 5 U.S.C. § 7106 outlines management authority to reassign employees. This regulation is maintained in JPH.

Effective Date 3/26/2013

#### 410.00 CORRESPONDENCE CONTROL

The IG and other Central Office elements of the OIG routinely receive myriad requests for information, materials, or the status of projects. To assure that all correspondence receives an appropriate and timely reply, the OIG maintains a correspondence control system using Optional Form 102, Correspondence Control Record; GSA Form 2458, Mail Log; and a suspense control file.

##### 410.01 General Correspondence

General correspondence received by the OIG is to be answered within 10 working days in accordance with OAD P 5410.1, Chapter 5, Section 8.

Effective Date 11/21/2017

## 412.00 AWARDS

### 412.01 Purpose

This chapter establishes policy for the Awards Program for all GSA Office of Inspector General (OIG) employees.

### 412.02 Applicability

The policy applies to all non-SES OIG employees.

### 412.03 Legal Authority

The statutory basis for performance and incentive awards is Title 5, United States Code (USC), Chapters 43, 45 and 53; implementing regulations are at 5 C.F.R. Part 451. Although the OIG manages its own awards program, the OIG generally follows GSA's awards policy, CPO P 9451.1 extended, except where doing so would be inconsistent with OIG independence or conflict with any of the specific guidance below.

### 412.04 Types of Awards

#### A. Performance-Based Awards

#### B. Special Act Awards

##### 1. Inspector General Awards

###### a. Individual

###### b. Teamwork

##### 2. Time-Off

### 412.05 Policy

The OIG grants awards to recognize its employees for such things as their superior accomplishments or other personal effort that contributes to the efficiency, economy, or other improvement of government operations, or for the performance of a special act or service in the public interest related to or in connection with their official employment. These awards are designed to be a motivating tool contributing to improving employee performance, strengthening morale, increasing productivity and unlocking workforce potential.

The Inspector General (IG), annually, may decide performance awards will not be given or adjust the amount of awards that will be available consistent with applicable authorities.

#### 412.06 Performance-Based Awards

Individual Performance-Based Awards (IPA) are rating based and link directly to the yearly performance appraisal. These cash awards will be distributed sometime between the end of the rating cycle and the end of the fiscal year, based on the availability of funds, most likely in the third quarter. Employees who receive a Level 4 summary rating are eligible to receive up to 4% of their adjusted basic pay in an IPA, and those who receive a Level 5 summary rating are eligible to receive up to 6% of their adjusted basic pay in an IPA. Award amounts are always subject to change due to the OIG budget, OPM Awards Policy Guidance, and GSA Awards Policy. All final award levels are approved by the IG and DIG. The following rules apply to IPAs.

- A. The OIG's performance rating cycle runs from January 1 through December 31. Ratings must be issued within 30 days of the end of the rating cycle.
- B. Individual performance awards are based upon performance during the rating period. Therefore, the award may be pro-rated based upon the date of hire, date of promotion, or assumption of position.
- C. To be eligible to receive a performance award, an employee must have been an OIG employee for at least 120 days by December 31.

An employee may also receive a Quality Step Increase (QSI) in lieu of a cash award. QSI awardees will be nominated by their supervisors. All QSI's are approved by the IG and DIG.

#### 412.07 Special Act Awards

Special Act Awards are based on contributions either within or outside job responsibilities that are not already covered under Individual Performance-Based Awards for award recognition. In lieu of a monetary award for a Special Act Award, an associate may be granted time off. Special Act Awards require specific justification detailing how the accomplishment saved time, saved money, overcame unexpected difficulties, and provided greater quality and/or better results achieved. There must also be an estimate of the tangible and/or intangible benefits of the accomplishment for which the award is being generated. [9451.1 CPO P Extended, GSA Associate Performance Recognition System (APRS)].

#### 412.07A Inspector General (IG) Awards

IG Awards are presented to those employees who have demonstrated to an outstanding degree either a superior accomplishment or other personal effort that contributes to the efficiency, economy, or other improvement of government operations. Information regarding awards criteria, nomination format, and submission procedures will be provided in the call for nominations package. Monetary recognition may accompany some of the awards, at the IG's discretion. Nomination categories may include the following:

##### THE INSPECTOR GENERAL'S DISTINGUISHED ACHIEVEMENT AWARD

This is the highest award granted by the Inspector General within the Agency. It is awarded to an employee who provides exceptional service or contributions over and above normal requirements to the OIG or to the Agency.

## THE INSPECTOR GENERAL'S EXCEPTIONAL TEAMWORK AWARD

This award is granted by the Inspector General for exceptional teamwork, including effective collaboration across organizational lines, or an effective team effort within a specific component, in achieving the goals and objectives of the OIG or the Agency.

## THE INSPECTOR GENERAL'S SPECIAL ACHIEVEMENT AWARD

This award is granted by the Inspector General for exceptional performance, dedication, and professionalism which has contributed significantly to the overall operation of the Office of Inspector General.

### 412.07B Time-Off Awards

Time-Off awards, are based on beneficial contributions either within or outside job responsibilities that are not already covered under Performance-Based Awards or IG Awards. The Office of Administration (JP) will provide each component with the total number of hours it may use for Time-Off Awards during the fiscal year. The value of Time-Off Awards is also counted toward the percentage of salary limitation on total awards given by the OIG, as stated in GSA policy. Like other awards, Time-Off Awards must be supported by written justifications, as described above in 412.07. To ensure consistency, each component head shall appoint one person to review and oversee all Time-Off Awards for that component. All Time-Off Awards must be submitted with proper justification to JP reasonably close to the completion of the special act. An exception to this timeframe would occur if an employee has been nominated for an IG Award and isn't selected. The DIG may set a limit on how many hours of Time-Off Awards an individual employee may receive during the fiscal year, but as stated in GSA policy, in no case may one award exceed 80 hours.

### Time-Off Award Procedures

- A. Employees must use their time off within one (1) year after receiving the Time-Off Award. Employees forfeit the Time-Off Award if not used within the allotted time period.
- B. Time-Off Award(s) can be used in conjunction with any regularly scheduled absence, such as Alternate Work Schedule (AWS) day off, and/or approved paid leave.
- C. Employees may use Time-Off Award(s) in conjunction with other requested leave; however, employees must submit both leave requests at the same time for approval.
- D. Time-Off Awards are not interchangeable for any monetary amount, or any other OIG approved award. A Time-Off Award cannot be converted to cash, such as a day's pay.
- E. Employees cannot donate the Time-Off Award to another OIG employee through the Leave-Share Program.
- F. The Time-Off Award time off must be scheduled in advance, with supervisor approval.
- G. When employees leave the OIG – retire, transfer to another federal agency, resign, or otherwise separate – they forfeit any unused Time-Off Awards.

H. Awards shall not be used to compensate or reward an employee for working outside of the basic workweek or in lieu of premium pay, such as overtime.

#### 412.08 OIG Appreciation Plaques

OIG Appreciation Plaques may be presented to an individual as a departing recognition of a job well done (contractor personnel may receive certificates of appreciation). Plaques can be given to employees of other agencies, consistent with legal authorities. OIG Appreciation Plaques for non-GSA/OIG employees must be approved by the DIG by sending an email with a justification. All Appreciation Plaques can be purchased by JPC.

#### 412.09 Prohibition on Acceptance by OIG Employees of Certain GSA-Conferred Cash Awards

OIG employees may be considered for a variety of sponsored GSA awards. It is vital to the OIG that it be perceived to be independent in its operations. Likewise, OIG employees are required to be objective in the performance of their duties vis-à-vis agency programs, activities, or employees. Therefore, it is generally inappropriate for OIG employees to receive cash awards of any kind from GSA sources in connection with the performance of their official OIG duties. However, GSA-conferred cash awards that are not directly related to an employee's OIG duties—for example, awards for savings bond coordination activities—may be accepted. Inquiries as to whether it is appropriate to accept a particular award should be directed to IG Counsel's Office.

Effective Date 2/26/2018

## 413.00 OIG POLICY AND PROCEDURES RELATED TO TRAINING AND DEVELOPMENT

### 413.01 Purpose

The purpose of this policy is to establish policy and identify roles and responsibilities regarding training and development for the OIG.

### 413.02 Legal Authority

As stated in 9410.1A HRM P, GSA Workforce Learning and Development Policy, the OIG has independent personnel authority, including employee training and development, under the Inspector General Act of 1978 as amended. Accordingly, after considering 9410.1A HRM P, which may be used for guidance in certain areas, the OIG has adopted the following training policy. Further guidance is provided in supplemental instructions and guidelines found in the Office of Personnel Management (OPM) Training Policy Handbook: Authorities and Guidelines (May 11, 2007) and 5 CFR Parts 410 and 412. The statutory authority governing service after training is found in 5 U.S.C. 4108.

### 413.03 Objectives

The OIG is committed to attracting, retaining, and developing a high performance workforce through skills training, education, and professional development. We increase our efficiency and productivity when employees have the knowledge and skills to succeed. The complexity and scope of our mission requires continual upgrading of competencies to perform in a dynamic work environment.

The OIG's mission is to promote economy, efficiency, effectiveness and integrity in GSA programs and operations. This mission includes reducing the operating costs of the federal government. Therefore, OIG employees shall first seek out suitable no-cost and low-cost learning and development options before undertaking more expensive options. In particular, OIG employees shall avoid or minimize travel expenses and enrollment fees when other viable options are available.

All employees shall have access to training, learning, and developmental opportunities to maintain and improve skills and competencies required to perform their job duties successfully, and to grow in their professions.

### 413.04 Eligibility for Training and Development Programs

All OIG employees are eligible to participate in formal and informal individual and career development opportunities unless otherwise excluded by statute, regulation, policy, or program limitation.

OIG employees seeking to participate in training:

1. Must meet OIG employment eligibility and performance requirements for participation in the selected program.
2. Must meet all program eligibility requirements for participation, including assigned pre-work, experience, or other prerequisites.

3. Will be selected in accordance with Equal Employment Opportunity, Merit Systems Principles, and OIG-identified processes as prescribed in law, rule, regulation, and agency policies.

4. Shall consider the appropriate GSA On-Line University (OLU) E-learning, no-fee Computer Based Training (CBT) program(s), GSA University for People (U for P), or equivalent, before pursuing a fee-based program.

Additional eligibility restrictions may apply to some programs, such as time with the OIG, performance, grade level, or competitive requirements.

#### 413.05 OIG Annual Training Cycle

At the beginning of each fiscal year, a yearly training plan should be completed for each OIG component and submitted to the Deputy Inspector General (DIG) for approval. The plan should then be forwarded to the Office of Budget (JPB) for budgetary planning purposes. The plan should be submitted no later than October 31.

#### 413.06 Mandatory Training

This is training that all OIG employees (or all employees of a type, such as supervisors, without regard to their business role) need. Mandatory training is delivered primarily by electronic means (GSA On-line University).

Examples:

- Training required for federal employees by statute, regulation, or policy\*;
- Security Awareness Training;
- Supervisory Training;
- Ethics Training.

\*Please note, specific roles or positions designated as Secret or Top Secret, may require additional annual training. Separate notifications will be sent to these employees.

See Appendix A for New Hire Training, See Appendix B for GSA OIG Annual Training

#### 413.07 Payment of Training Expenses

Each OIG employee bears the responsibility to ensure he or she is eligible and approved to attend training, and that he or she receives reimbursement. The OIG may pay for or reimburse employee learning and development expenses in two broad categories:

1. Normal, Job-Related Learning and Development

Most employee learning and development is directly related to the employee's current role. These activities result in knowledge or skills that the employee usually can apply immediately upon completion. They address gaps in job-related skills, knowledge, and abilities that allow the employee to improve performance or take on additional responsibility related to the role. Examples include technical skills training or academic course work that is directly related to the current role, project management training for employees who currently lead project teams or are ready to begin doing so, and the like.

## 2. Career Development

- a. Some learning and development activities relate to future roles within the organization that the employee may reasonably be expected to pursue given his or her current role. These activities instill knowledge or skills that may take time after the learning activity for the employee to develop and master, and which may prepare the employee to take on roles of increased responsibility in his or her current field.
- b. Training that qualifies an employee to enter a field different from the employee's current job, such as training that would allow someone to obtain a license to practice in a new field unrelated to his or her current position, should not be requested.

### 413.08 Authorization, Agreement and Certification of Training

A Standard Form 182 (click text for link: [SF-182](#)) must be submitted in advance to the employee's supervisor for all required training approvals unless there is an MOU in place or a Conference/Training form for group training. (The SF-182 is separate from the requirement to enter completed training in CHRIS as discussed below.) The form should be signed by the immediate supervisor and/or second-line supervisor. If the training cost exceeds \$3,500, the form is then submitted to JP for processing. If under \$3,500, the component should ensure funding is available and then may use a government purchase card to procure the training. (That form also contains a Continuing Service Agreement that must be signed as indicated later in this chapter.)

Component heads are authorized to approve training up to \$3,500. However, certain training (e.g., in excess of \$1,000) at conferences must also be approved by the DIG as stated in Chapter 423.

SF-182s are not required for training that does not impose an additional cost to the agency as a result of the employee's participation.

An employee may also pay for training themselves and may request reimbursement via miscellaneous reimbursement but it still must be approved in advance via the SF-182.

### 413.09 Expectations for Employees Attending Training

All OIG employees are expected to complete satisfactorily any training covered by this policy. Any OIG employee who fails to meet requirements for successful completion of the program or course shall be obligated to repay the cost of tuition, books, and other related expenses. There are limited exceptions and questions should be directed to the Office of Human Resources (JPH). For information regarding Certifications, Accreditations, and Licenses, please see Chapter 418 Policy Government Expenses for Professional Credentials of this manual.

For university, college, professional certification prep, or other approved and accredited courses, successful completion or "passing" is understood to mean:

1. A minimum grade of "C" for an undergraduate course.
2. A minimum grade of "B" for graduate-level courses.
3. "Pass" in a pass/fail course.
4. The minimum passing score established by the professional accreditation board or training delivery organization for the intended course, or program of study.

#### 413.10 Continuing Service Agreement (CSA)

The Continuing Service Agreement (CSA), may be attached to the SF-182 and must be completed whenever an employee is selected for a single training course requiring 80 hours or more to complete, or costing up to \$3,000.00 or more inclusive of all related expenses (includes travel, per diem, books and materials, fees, and other related costs). The CSA is subject to the following requirements:

1. The employee agrees to continue in the service of GSA OIG after the end of the training period for a work period at least equal to ten (10) times the length, in hours, of the training period (usually the total classroom hours) NTE one year, unless he or she is involuntarily separated from the Federal Government.

For example, an employee attending an 80-hour-long (e.g., 2 week) course agrees to remain employed by the Federal Government for not less than 800 working hours (80 hours x 10 = 800 hours / 8 hour-day = 100 working days, or 20 weeks) after course completion.

2. In the event that an employee voluntarily separates from the GSA OIG within the period covered by the continuing service agreement, the employee shall repay the amount the GSA OIG paid for that training, plus any related expenses. The amount due shall be pro-rated according to the service agreement schedule. For example, if the employee completes only 50 days of a 100-day continuing service agreement, the employee shall repay half the total amount paid by the GSA OIG in connection with that training.
3. Repayment within the period covered by the CSA is required of an employee who leaves the service of the GSA OIG to enter into the service of another agency in any branch of the Federal Government.
4. Once an employee has signed a CSA, the component will monitor the date the obligation service commitment expires. No employee will be separated from the GSA OIG until there is a resolution of any active continued service obligation.
5. Should an employee, who is under a CSA, decide to leave GSA OIG service:
  - a. The employee must provide a written notice of resignation to his/her supervisor of record at least 10 working days in advance of the effective date of departure.
  - b. The employee's supervisor of record will ensure that the notice of resignation is sent to the applicable senior manager, the Counsel to the IG (JC), and JP and will inform JC and JP that an outstanding debt is owed.
6. If an employee fails to complete training covered by a CSA, the employee is required to reimburse the Government for the total cost of that course, and the CSA is voided.

7. Waivers from the service requirements or other obligations established in this policy may be made under extraordinary circumstances (such as a death in the family requiring an employee to leave training early). A waiver must be requested in writing accompanied by documentation or other evidence detailing the extraordinary circumstances that justify the request. Requests for waivers of amounts up to \$1,500 are submitted to the head of the OIG component. Waiver requests for amounts between \$1,500 and \$9,999 are routed to the head of the component with the concurrence of the Office of Counsel (JC) and the Office of Administration (JP). Requests for waivers of \$10,000 or more are submitted to the Deputy Inspector General (DIG) with the concurrence of the head of the component, JC, and JP. The DIG may reject the request or grant a full or partial waiver.

#### 413.11 Educational Assistance Programs

The OIG does not participate in any tuition assistance programs.

#### 413.12 Recording Training

All training attendance must be recorded and submitted to OPM as required by 5 CFR 410.601. GSA uses CHRIS to gather this information. Upon completion of training, within 30 days all employees should key required information into their CHRIS training record. (Completion of a course through GSA's on-line university will automatically be populated in CHRIS.) See Appendix C

Effective Date 1/3/2017

#### 414.00 SUPERIOR QUALIFICATIONS AND SPECIAL NEEDS PAY SETTING AUTHORITY

##### 414.01 Purpose

The Superior Qualifications and Special Needs Pay Setting Authority is a critical component of OIG's overall recruitment process and its purpose is to improve OIG's hiring.

With the exception of the provisions discussed below, the OIG adopts GSA Order HRM 9531.1, "Superior Qualifications and Special Needs Pay Setting Authority."

##### 414.02 Applicability

The policy applies to GS appointees who have superior qualifications or who meet a special OIG need who are entering the Federal service for the first time or returning to Federal employment after a break in service of 90 calendar days or more from their last period of Federal employment or employment with the District of Columbia. Limited exceptions to the 90-day limitation are provided in 5 CFR 531.212(a)(3).

##### 414.03 Legal Authority

The authorities cited for this policy are 5 U.S.C. 5333 and 5 CFR 531.212.

The Inspector General Act of 1978 as amended ensures that the OIG can provide policies and procedures separate from those of GSA to ensure independence.

##### 414.04 Definitions

###### a. Recommending Official.

The supervisor or manager making the hiring selection is the recommending official.

###### b. Reviewing Official.

The Human Resources (HR) Director has managerial responsibility to ensure the OIG's use of superior qualifications appointments conform to the requirements established in 5 CFR 531.212 and HRM 9531.1.

###### c. Approving Official.

The Deputy Inspector General is the approving official for all special qualification authorities

##### 414.05 Responsibilities

###### a. Recommending Official

Preparing the written recommendation with appropriate supporting documentation, justifying the request for a superior qualifications appointment.

b. Office of Human Resources

- 1.Reviews package to ensure the justification and documentation support use of the incentive and the request is in compliance. Consults with requesting organization, as necessary, to request additional information or documentation.
- 2.Submits package for final approval or disapproval to the Deputy Inspector General.

c. Assistant Inspector General for Administration

Coordinates with the HR Director for review and final action and submission to the Deputy Inspector General to approve or disapprove the request.

414.06 Procedures for Requesting Approval for a Superior Qualification Appointment (SQA)

a. The recommending official will prepare the request for superior qualifications appointment and forward it in accordance with the OIG paragraph on "Responsibilities" for concurrences and approval. Candidates should be advised not to decline other offers of employment or notify current employers of their intent to leave before the request is approved. The request maybe submitted via email.

b. Notification of approval or disapproval will be sent to the recommending official and to the reviewing official.

c. JPH will:

- 1.Proceed with the pre-employment processing and if favorable and the SQA is approved, prepare the official job offer letter stating the grade and step;
2. Process the Request for Personnel Action (SF52) for the appointment, and maintain all supporting documents.

414.07 Documentation and Recordkeeping

The records and documentation will be maintained for a minimum of 2 years by JPH.

Effective Date 6/16/2016

#### 415.00 OIG INCLEMENT WEATHER GUIDANCE

This guidance is to remind employees of their work status options when OPM announces that Federal offices in a particular geographical area are closed, or that Federal offices are open, or open with a delayed arrival or early departure with an option for unscheduled leave or telework due to inclement weather or some other emergency that causes disruption to Government operations. The OIG follows OPM's guidance, available at <https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/dcdissmissal.pdf>. As a reminder, OPM made a change last year that an employee on pre-approved paid leave will generally remain on leave if the Federal office at which the employee works is closed.

These basic rules and options apply in the regions when they have similar determinations to the ones made by OPM for the DC area. In the event of a closure or delay in a regional office, the SAC, RIGA, or ASAC should notify their component head and the Deputy AIG for Administration.

Please consult with the OIG's Telework Management Officer (HR Director) if you have any questions. The attached pages include examples of possible scenarios.

Any time you are scheduled to telework on an inclement weather day, you must telework. You will not be given an excused absence unless you cannot telework because the weather or other emergency affects your ability to telework. You may also have the option to situational telework in accordance with OIG policy. The following examples provide further guidance for situations where you have approval to situational telework on an inclement weather day.

\*If Federal offices are closed on the employee's regular alternative work schedule (AWS) day off, they are not entitled to an additional "in lieu of" day off. [1]

[1] See OPM Dismissal and Closure Procedures (2014)

Ex. 1- OPM announces that Federal offices are CLOSED due to a snowstorm.

(1) If it is your regular telework day, you must telework the entire day unless you take leave or your manager grants you an excused absence because of an emergency situation, which affects your ability to successfully telework.

(2) If you were NOT SCHEDULED to telework on this day, (e.g. you did not request to telework because of the impending snowstorm), but were scheduled to report to the worksite, you will receive an excused absence for the entire day.

(3) If you requested in advance and received approval for paid annual leave for the entire day, you will be charged paid leave for the entire day if you are not available for work.

(4) If you requested in advance and received approval to situational telework, you must telework the entire day, unless you take leave or your manager grants you an excused absence because of an emergency situation which affects your ability to successfully telework.

Ex. 2- Due to a snowstorm, OPM announces Federal offices are OPEN, or OPEN WITH A DELAYED ARRIVAL or EARLY DEPARTURE – WITH OPTION FOR UNSCHEDULED LEAVE OR UNSCHEDULED TELEWORK.

(1) If it is your regular telework day, you must telework the entire day even if Federal offices open late (or close early), unless you take leave or your manager grants you an excused absence because of an emergency situation, which affects your ability to successfully telework.

(2) If you requested and received approval for situational telework, you must telework the entire day even if Federal offices open late (or close early), unless you take leave or your manager grants you an excused absence because of an emergency situation which affects your ability to successfully telework.

(3) If you choose to report to the worksite, you should report to the worksite within the timing announced by OPM, and you will receive an excused absence (i.e. no charge to leave) for the late arrival/early departure closure periods.

(4) If you choose to request unscheduled leave, you will be charged leave for the entire day even if Federal offices open late or close early.

See Figure 415-01 Decision Matrix on the Application of the Updated Leave Practice

Effective Date 8/27/2014

416.00 SES PERSONNEL POLICIES, REGULATIONS, AND PROCEDURES

OIG SES Policies are updated and approved by OPM and OMB periodically. For updated policies please see the Deputy AIG for Administration or the AIG for Administration.

Effective Date 5/11/2015

## 417.00 USE OF OFFICIAL TIME

### 417.01 Introduction

All OIG employees are entitled to use available administrative processes, such as Equal Employment Opportunity (EEO) complaints and pre-complaint processing, administrative grievances, and Merit Systems Protection Board (MSPB) appeals. By law, OIG managers and supervisors must not interfere with this right. In such matters, the OIG affords its employees the use of a reasonable amount of official time (i.e., no charge to leave or loss of pay) if the employee is in a duty status.

The OIG affords to its employees two categories of official time: automatic time and discretionary time. OIG employees are afforded a reasonable amount of automatic time. However, the OIG has established a limit governing the use of discretionary time. It is the agency policy to allow up to four (4) hours of discretionary time. The amount of discretionary time granted is determined on a case-by-case basis. The supervisor should consider the gravity and complexity of the charges, the amount of legal or regulatory research that may be appropriate, and the employee's knowledge of the proceedings. Supervisors may consider granting more than four (4) hours of discretionary time in unusual situations, such as a matter involving extraordinarily complex issues or circumstances or pro se (without representation) litigation, but only upon a showing of adequate justification by the employee and in consultation with Employee Relations (JP) (see § 417.08 below).

When an OIG employee exhausts the discretionary time allotted or the automatic time permitted, the employee has the option of pursuing the matter during times when not in duty status (i.e., outside of the employee's normal hours of work), or requesting Annual Leave, Compensatory Time Off, or Leave Without Pay.

For administrative processes not specifically described herein, please consult with JP.

### 417.02 Requesting Official Time

When an OIG employee in duty status desires to use official time to pursue recourse through an available administrative process, the employee must request official time in advance from her or his immediate supervisor. Official time may be granted if requested after an event in limited circumstances. The OIG will not automatically record an employee's time as official time; the employee is responsible for making the request. The OIG employee must make the request in writing, such as by email. OIG employees need not seek authorization for occasional telephone calls or other events lasting under fifteen minutes. OIG supervisors should grant or deny, as the case may warrant, requests for official time in writing and, when denying a request, should provide a basis for the denial. Reasons for denial include, but are not limited to, workload or coverage priorities (managers should suggest alternate times) or exhaustion of the time allotted.

OIG employees who desire anonymity or request confidentiality have the option of pursuing the matter during times when not in duty status, or requesting Annual Leave, Compensatory Time Off, Travel Compensatory Time Off or Leave Without Pay. OIG employees who use Annual Leave to ensure anonymity or confidentiality will have their leave restored as appropriate upon request, when and if they elect to disclose their identity.

### 417.03 EEO Complaints

Automatic Time: In cases where an OIG employee alleges discrimination or is a witness in a discrimination complaint, OIG supervisors should grant official time to the employee for any and all of the following or similar events:

1. Meeting with an agency official, such as with the Office of Civil Rights or agency representative;
2. Meeting with an EEO counselor;
3. Time spent in a mediation session or any other Alternative Dispute Resolution program;
4. Meeting/Interview with an EEO counselor or investigator or time responding to an investigator's questions or request for documents;
5. Attending the employee's own deposition (taken by the agency);
6. Attending a deposition as a witness, i.e. as an agency witness when you are not the claimant;
7. Pro se litigant deposing agency witnesses (pro se litigants may also require additional Discretionary Time for other discovery matters as well);
8. Meetings and other pre-hearing sessions with Administrative Judges;
9. Attending the hearing of the case;
10. Time spent in Administrative Judge and Judge initiated settlement conferences where all parties are present;
11. If a complaint is appealed to a U.S. District Court, attending pre-trial sessions with Department of Justice attorneys;
12. If a complaint is appealed to a U.S. District Court, attending the trial;
13. Complainant actual travel time to any of the above of not more than one hour each way, per event (travel time in excess of one hour must be accounted for as discretionary time or leave); and
14. Witness and agency representative travel and preparation time for any of the above.

OIG employees must make reasonable attempts to schedule meetings to minimize interference with workload and productivity (time sensitive projects, for example).

Automatic time is not capped. If a manager believes an employee's request for automatic time is unreasonable, he or she should consult with employee relations. Managers must consult with employee relations prior to denying a request for automatic time.

Discretionary Time: In addition to automatic time, OIG employees alleging discrimination shall receive up to four (4) hours of discretionary time for use during the entire EEO pre-complaint counseling,

complaint, and appeal process. The OIG employee shall determine how to use his or her discretionary time. Discretionary time may be used for matters such as, but not limited to, complainant's preparation for a hearing, responding to discovery requests and meetings with complainant's representative.

#### 417.04 MSPB Appeals

Automatic Time: In matters brought before the MSPB, OIG supervisors should grant official time for any and all of the following or similar events:

1. Time spent in a mediation session or any other Alternative Dispute Resolution program;
2. Meeting with an agency official, such as an agency representative;
3. Attending the employee's own deposition (taken by the agency);
4. Attending a deposition as a witness, i.e., as an agency witness when you are not the appellant;
5. Pro se litigant deposing agency witnesses (pro se litigants may also require additional Discretionary Time for other discovery matters as well);
6. Meetings and other pre-hearing sessions with an MSPB Administrative Judge;
7. Attending an MSPB hearing;
8. Time spent in Administrative Judge and Judge initiated settlement conferences where all parties are present;
9. If a matter is appealed to Federal court, attending pre-trial sessions with Department of Justice attorneys;
10. If a matter is appealed to Federal court, attending the trial;
11. Appellant actual travel time to any of the above of not more than one hour each way, per event (travel time in excess of one hour must be accounted for as discretionary time or leave); and
12. Witness and agency representative travel and preparation time for any of the above.

OIG employees must make reasonable attempts to schedule meetings to minimize interference with workload and productivity (time sensitive projects, for example).

Automatic time is not capped. If a manager believes an employee's request for automatic time is unreasonable, he or she should consult with employee relations. Managers must consult with employee relations prior to denying a request for automatic time.

Discretionary Time: In addition to automatic time, OIG supervisors should grant up to four (4) hours of discretionary time for use during an MSPB matter. The OIG employee shall determine how to use his or her discretionary time. Discretionary time may be used for matters such as, but not limited to,

complainant's preparation for a hearing, responding to discovery requests and meetings with complainant's representative.

#### 417.05 Administrative Grievances

The OIG permits official time for grievances handled through the GSA Grievance Procedures in accordance with GSA OAD P 9771.1A GSA Grievance Procedures. Specifically, "in presenting a grievance or preparing a challenge to a disallowance decision, an employee has the right to a reasonable amount of official time if the employee is in active duty status. Supervisory approval for the use of official time must be obtained in advance. This allowance of time does not extend to the preparation of a grievance." Accordingly, time spent in presenting a grievance or preparing a challenge to a disallowance decision is considered automatic time under this policy. Official time is not permitted for grievance preparation.

#### 417.06 Other Proceedings

OIG employees required or authorized by law to be present at hearings or board proceedings, such as before the Office of Special Counsel, the Office of Personnel Management and similar bodies in matters related to their official capacity will be excused from normal duties for that purpose without charge to leave. Such time shall be considered automatic time. OIG employees must consult with management concerning the use of official time for other purposes.

#### 417.07 Response to Proposed Suspensions or Adverse Actions and Proposals based on Unacceptable Performance

Upon written request and approval from their immediate supervisor, an OIG employee in duty status who is given a notice of proposed disciplinary, adverse, or performance based action may have discretionary time, as set forth in 417.01, to review the material relied upon, consult with a representative, secure affidavits and prepare a written or oral reply.

An OIG employee that is not in a duty status who is given a notice of proposed disciplinary, adverse, or performance based action will not receive discretionary time, as set forth in 417.01, to review the material relied upon, consult with a representative, secure affidavits and prepare a written reply.

OIG employees shall be granted automatic time to present their oral reply, including actual travel time to, and return from, the presentation.

#### 417.08 Additional Discretionary Time-Extenuating Circumstances

Management may grant discretionary time beyond four (4) hours in extenuating circumstances. The employee must submit a written request for additional discretionary time, explaining the extenuating circumstances that the employee believes justifies the need for the additional time. Management must consult with employee relations before granting or denying a request for additional discretionary time due to extenuating circumstances.

#### 417.09 Coordination with JP

Upon notification, whether formal or informal, of the existence of an OIG employee's allegation of discrimination, or any other significant employee-relation matters, OIG managers and supervisors must immediately contact employee relations.

Effective Date 7/11/2016

## 418.00 POLICY GOVERNING EXPENSES FOR PROFESSIONAL CREDENTIALS

### 418.01 Introduction

Heads of Components may approve payment for employees to obtain professional credentials. Such approval is discretionary and not an entitlement. Any decision to authorize payment will be based on factors such as availability of funds and whether credentials are necessary for employment. Where funds are limited, payments will first be made for credentials that are required as a condition of employment.

This authority may be re-delegated in writing. Credentials covered include professional accreditations, licenses, or certifications that are either directly related to employees' positions or that would further OIG interests (e.g., credentials that are needed for the development of knowledge, skills, and abilities in response to mission/function changes or for recruitment, retention, career development or worker transition objectives). Payment for expenses necessary to obtain credentials, and their subsequent renewals, may include, at the Component's discretion, such additional expenses as membership fees, examinations, registration fees, and travel costs, where necessary to obtain the credential.

The Credentials Policy does not permit reimbursement for membership fees if the OIG employee is (1) a member of an organization that does not provide credentials/certifications or (2) a member of an organization which provides certifications and credentials but the OIG employee is not seeking to obtain the certification/credential (i.e. is not a member for the purpose of obtaining the credential).

Authority governing payment of professional credentials is found in 5 U.S.C. 5757. That section permits agencies to use appropriated funds or funds otherwise available to pay for "(1) expenses for employees [in any federal pay system] to obtain professional credentials, including expenses for professional accreditation, State-imposed and professional licenses, and professional certification; and (2) examinations to obtain such credentials." This authority may not be exercised on behalf of any employee "occupying or seeking to qualify for appointment to any position that is excepted from the competitive service because of the confidential, policy-determining, policy-making, or policy-advocating character of the position."

### 418.02 Definitions

"Accreditation" is a certification of competence in a specified area issued by a duly recognized and respected accrediting organization.

"Certification" is recognition given to individuals who have met predetermined qualifications set by an agency of government, industry, or a profession.

"Credentials" include professional accreditations, licenses, or certifications that are either directly related to an employee's position or that would further the OIG's statutory mission.

"Directly related" refers to skills and abilities that would enhance an employee's performance of the duties of the currently occupied position.

“License” is the formal permission granted by an agency of the federal, state, or local government to an individual to engage in a given occupation upon finding that the applicant has attained the minimal degree of competency required to engage in that occupation.

“Professional” is broadly interpreted to mean any occupation.

Hence, any OIG employee in a career field that has a job-related license, registration or certification is eligible. Priority for payment of expenses associated with licenses and certification and related expenses will be given when the credential is required by appropriate local, state, or Federal government authority to perform the work required by an employee’s position.

#### 418.03 Eligibility

This policy applies to all OIG employees. However, payments may not be made on behalf of any employee “occupying or seeking to qualify for appointment to any position that is excepted from the competitive service because of the confidential, policy-determining, policy-making, or policy-advocating character of the position.” 5 U.S.C. 5757(b).

#### 418.04 Provisions Governing Reimbursement of Expenses for Professional Credentials

1. Payment of expenses under this authority is totally discretionary with OIG management. Continued payment of expenses associated with credentials is not guaranteed and nothing in this policy creates a right or benefit.
2. Payment for credentials (including subsequent renewals) will be by reimbursement. Reimbursement for all requests is subject to funding availability. Under no circumstance will the amount of reimbursement exceed \$500 for the combined total expense of all credentials and related expenses such as examinations for a single employee in any given fiscal year.
3. The employee should discuss eligibility for reimbursement with their supervisor before incurring any expense for professional credentials.
4. In preparing for or maintaining a professional credential, employees must comply with the OIG's policies on personal use of government resources.
5. Supervisors must ensure that the employee has successfully obtained the credential or taken the examination prior to approving reimbursement of costs incurred by the employee.
6. Payments may include, at the approving official's discretion, reimbursement for such additional expenses as membership fees, reporting fees, exam fees, registration, and travel costs, so long as payment of the fees is a condition precedent to obtaining a credential. If an OIG employee joins a professional organization for a purpose other than obtaining the credential and does not obtain/maintain the credential, the membership fees will not be reimbursable under the OIG's Credentials Policy. For example, the OIG will not reimburse employees for social membership or to attend events/educational seminars hosted by an organization that does not issue any professional credentials.

7. Training expenses (e.g., exam preparation courses and materials, events and educational seminars, etc.) normally will be reimbursed under the policies governing training and not under this policy. This includes the OIG's training and development policy (OIG Manual, Section 413.00), the conference policy (OIG Manual, Section 423) and the purchase card policy (OIG Manual, Section 718). When an expense associated with training is required to obtain a professional credential and is not covered under another policy, payment may be authorized under this policy.

8. Components shall ensure that criteria for payment of expenses to obtain professional credentials are applied consistent with merit system and equal opportunity principles as set forth in 5 U.S.C. § 2301 and 2302.

#### 418.05 Administration Procedures

Each OIG component has designated a contact person to receive all requests for reimbursement and supporting documentation (e.g., receipts, organization information, certification requirements) under this policy:

- JP: Executive Staff Assistant
- JA: Director, Administration and Data Systems Staff
- JI: Executive Staff Assistant
- JE: Deputy Director for Inspections
- JC: Counsel to the Inspector General

That person will, as directed by the component head, determine what expenses are eligible for reimbursement and whether there are sufficient funds to do so. Once that determination is made, the contact person will notify the individual seeking reimbursement as to what expenses will be approved. Approved expenses must then be submitted for reimbursement through the Agency's E-Gov Travel Service (currently CONCUR/CGE). JP will provide further instructions to each component on how to implement this practice.

Effective Date 6/17/2016

## 419.00 TELEWORK POLICY

### 419.01 Introduction

Purpose: This policy establishes the circumstances and terms under which eligible OIG employees may telework to the maximum extent possible without diminishing employee performance or OIG operations.

Authority: Public Law 106-346, Section 359, and The Telework Enhancement Act of 2010 (Public Law 111-292) require each executive agency to establish a policy under which eligible employees may telework to the maximum extent possible without diminishing employee performance or agency operations. There is no right or entitlement to telework.

### 419.02 OIG Telework Policy

As set forth below, the OIG telework policy provides for Regular Telework and Situational Telework. These terms are defined in subparagraphs (a) and (b) below.

An employee's ability to participate in regular or situational telework is determined according to job position and individual capacity (i.e. position eligibility and individual eligibility). See Section 419.06.

#### (a) Regular Telework:

Regular telework occurs on a recurring and ongoing basis. Regular telework is limited to two days per pay period.

#### (b) Situational Telework:

Situational telework normally occurs on an infrequent basis and must be approved by the employee's supervisor in advance.

Situational telework addresses specific or temporarily defined organizational or employee needs, such as the need to work away from the employer's official worksite, occasioned by structural renovations affecting the worksite; short-term localized traffic such as those occasioned by weather conditions; security concerns; or an employee's infrequent, short-term personal situation, injury or illness that precludes commuting to the worksite but does not diminish the employee's ability to work.

### 419.03 Employee Participation in Telework is Voluntary

An employee who signs a completed Telework Agreement in which they request to telework may not be required to engage in telework.

#### 419.04 The Nature of Telework

Telework is the mechanism by which an OIG employee performs his/her duties at an alternate location. Telework encompasses more than merely answering phones/responding to emails when received. Telework includes what is generally referred to as remote work but does not include any part of work done while on official travel or field work, as defined in Section 419.11. While teleworking an OIG employee occupies the same duty status as his/her colleagues working in their government offices. Telework may not be employed as a substitute for leave, dependent care, or to attend to other personal responsibilities. A teleworking employee must ensure that dependent care and other non-official activities do not interfere with the employee's official responsibilities and ability to telework.

##### A. Reporting to the official worksite on telework days:

(i) A teleworking employee must be available, upon request, to report to the employee's worksite or other required location on a planned/scheduled telework day for a variety of reasons including, but not limited to, meetings, briefings, special assignments, emergencies/exigent circumstances, or duties that must be performed at the office or within a limited timeframe(s). The decision to require a teleworking employee to report to the employee's worksite or other required location rests within the discretion of the respective Component Head or Responsible Management Official.

(ii) The requirement for a teleworking employee to report to the employee's worksite or other location on a scheduled telework day will neither: (1) serve to terminate the telework arrangement nor (2) entitle the employee to a replacement telework day for the day that the employee was required to report to the employee's worksite or other location.

(iii) If possible advanced notice will be provided to the teleworking employee if there is a need for the employee to report to the worksite.

##### B. Administrative leave, dismissals, and emergency closings:

(i) For Employees Who Are Scheduled to Telework (Regular or Situational).

A teleworking employee may not cease working when the federal government (or regional office) is closed for all or part of the employee's scheduled telework day. You must telework the entire day unless you take leave or your manager grants you an excused absence. For example, an employee whose telework hours are 8 a.m. to 5 p.m. must work those scheduled hours, even if OPM or GSA/OIG announces a delayed arrival or an early dismissal.

(ii) For Employees Who Want to Perform Unscheduled Situational Telework.

On days when OPM has listed the Federal government as "open" but allowing use of unscheduled telework, employees must notify their supervisor of their desire to perform unscheduled telework. Supervisor approval is required prior to telework; supervisors will generally grant the employee's request for unscheduled situational telework on these days if the employee is eligible and has the necessary equipment and materials to telework and sufficient work to perform at the telework site unless his/her presence is requested at the worksite due to a critical work circumstance. If the employee does not have the necessary equipment or enough work, the employee must take unscheduled leave or a combination of unscheduled leave and unscheduled telework.

(iii) For Employees Who Are "Telework Ready" (i.e. Telework Eligible and Have Signed Completed Telework Agreements).

On any workday that the Federal government (or regional office) is closed:

a. The Deputy Inspector General or component heads may, as appropriate and in accordance with the employee's Telework Agreement, for mission-related purposes, direct telework-ready employees to telework in lieu of being granted administrative leave.

A telework-ready employee who is required to telework when the Federal Government (or Regional Office) is closed is not entitled to receive overtime pay or compensatory time off for performing work during the employee's regularly scheduled hours. Moreover, the telework-ready employee must work his/her full tour of duty for the entirety of the period directed by management.

(iv) A teleworking employee may be granted an excused absence (i.e. administrative leave) for the amount of time Federal offices are closed when it is not possible to telework due to:

a. The emergency situation adversely affecting the telework site (e.g., disruption of electricity or internet connection, loss of heat, lack of alternative dependent care, etc.); and/or

b. The teleworking employee's duties are such that the employee cannot telework or continue to telework without contact with the employee's regular worksite (e.g. to accomplish the assigned tasks the employee needs to be in contact with someone who is not teleworking).

(C) Continuity of Operations (COOP):

The telework policy is intended to be used to support the OIG's COOP plan. When a COOP emergency is declared, the COOP plan controls.

#### 419.05 Responsibilities

A. Requirements for OIG Component Heads:

OIG component heads are required to determine, in the first instance, which positions within their respective components are ineligible to participate in telework. See Sections 419.02 and 419.06. The component head will determine whether a position, based on OIG mission and organizational needs and position duties and responsibilities, is eligible for regular or situational telework. Determinations that a position is ineligible for regular or situational telework must be made in writing and provided to the Telework Management Official.

B. Requirements for Responsible Management Officials (RMOs), Regional Inspectors General for Auditing (RIGAs), Special Agents in Charge (SACs), Division Directors, and other supervisors:

(i) Determine and notify each employee under their supervision whether or not they are eligible to telework. This determination should be made within 10 days of receipt of the employee's signed Telework Agreement form. RMOs may, in accordance with the eligibility criteria set forth in Section

419.06, Eligibility, and Appendix 1:

- deny a telework request;
- modify an existing Telework Agreement; or
- terminate an existing Telework Agreement.

(ii) Decide whether to require an employee to come to the office on a regular telework day in accordance with Section 419.04(a) of this policy.

(iii) Decide whether to grant or deny a request for situational telework. In evaluating any request, consideration should be given to productivity, operational needs and mission, the basis for the request, consistency with OIG policy, and other factors such as those described in Section 419.06(b) and Appendix 1. A request may be denied for any legitimate, business reason.

(iv) Revoke a Telework Agreement based on the factors in Section 419.06(b)(ii) or Appendix 1 and promptly terminate an existing Telework Agreement if any of the factors in Section 419.06(b)(iii) occur.

(v) Advise their component head when their office must be closed due to an emergency so the component head can decide whether, for mission-related purposes, to require telework-ready employees to telework. For tracking purposes, the Deputy Assistant IG for Administration (JP) must be notified when an office is closed.

(vi) Ensure (in conjunction with the employee) that the responsible timekeeper is informed of the teleworking hours and basis for telework (i.e. regular or situational and, if situational, whether due to an emergency closure), so the information can be accurately entered into the OIG's time and attendance records system.

C. Requirements for OIG Employees:

(i) Sign a Telework Agreement, as specified in Section 419.08. In summary, any employee who declines to telework should so indicate on the Telework Agreement. All OIG employees who may want to telework, even if only in an emergency situation, are required to complete the Telework Agreement and must comply with the requirements in this policy.

(ii) Use their government issued OIG laptop when teleworking and that includes the use of virtual private network (VPN).

(iii) Cooperate with their supervisors to ensure the responsible timekeeper makes the appropriate entries in the OIG's time and attendance records system.

D. Requirements for Telework Managing Official (only the last requirement can be delegated):

(i) Develop and implement policy related to the OIG's telework program.

(ii) Advise OIG leadership, including the Inspector General, the Deputy Inspector General, the Associate Inspector General, supervisors and employees about telework requirements.

(iii) Be a primal point of contact for the Office of Personnel Management on telework matters.

## 419.06 Eligibility

Management approval of telework requires separate determination of position eligibility.

(a) Position eligibility: Not all positions are eligible for regular telework, or telework of any kind. Some positions require, on a daily basis, on site activity that cannot be handled effectively remotely or at an alternate worksite. A position that requires an employee to be on site daily may include, but is not limited to, customer service interface positions with the general public and/or agency staff, face to face contact jobs, or jobs that require employees to have hands on contact with, for example, facilities, to successfully fulfill the requirements of the position. Even if a position is determined to be eligible for telework, the number of permitted telework days may be limited due to work requirements. Telework for such positions would diminish employee performance or agency operations.

The component head will consider OIG mission and organizational needs and position duties and responsibilities when making eligibility determinations. See Section 419.05 for review responsibilities.

(b) Determining eligibility: The RMO or his/her designee shall determine the eligibility of each employee who requests to telework on a case-by-case basis. In arriving at this determination, the RMO or his/her designee must apply, as appropriate, the factors set forth in subsection (b)(ii) and Appendix 1 to the facts of each case so as to reach a conclusion as to the employee's eligibility to telework. If the RMO or his/her designee determines that the employee is eligible to telework, then the employee is eligible to do so after the Telework Agreement is signed by the required parties. See Appendix 2. The RMO may revoke an eligibility determination at any time based on the factors below or in Appendix 1.

Employees who are new to the OIG must wait a minimum of six (6) months before being eligible to participate in the OIG Telework Program, unless the component head determines otherwise.

(c) Ineligibility:

(i) An OIG employee is ineligible to participate in the OIG Telework Program if any of the conditions in the list below exist with respect to the employee. The RMO or his/her designee may, but is not required to, grant a waiver and permit an otherwise ineligible employee to telework when he/she determines that doing so is in the best interest of the RMO's component; the component head must concur in any waiver which allows teleworking for employees with conduct or performance issues (i.e. the final disqualifying factor listed in Section 419.06(b)(ii)). An employee determined to be ineligible under (ii) or (iii) below may not be required to telework in an emergency situation.

(ii) Disqualifying factors:

- Unavailability of necessary materials at the alternate worksite.
- Degradation of workplace efficiency that would be created by the employee's teleworking, e.g., an adverse impact upon the productivity or morale of OIG employees, or the supervisor's ability to manage operations.
- Instances of performance that raise objectively reasonable concerns about the employee's ability to perform his/her duties at an alternate work site, such as not timely responding to phone calls, emails, or instant messages from managers and/or co-workers.
- History of unexcused absences or other attendance and availability issues inconsistent with telework.
- Deficiency in the employee's ability to work independently (especially in developmental or trainee positions).

- Failing to timely report back to the official worksite when required to do so without good reason.
- Failing to comply with management's need to change the employee's telework schedule.
- The employee's most recent performance rating of record is below the "meets expectations" level or the employee otherwise requires close supervision.

(iii) As stated in the Telework Enhancement Act, an employee may not telework if the employee has been officially disciplined for conduct as follows:

- For being absent without permission for more than 5 days in any calendar year; or
- For violations of subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch for viewing, downloading, or exchanging pornography, including child pornography, on a Federal Government computer or while performing official Federal Government duties.

The RMO or his/her designee cannot grant a waiver of ineligibility for these conduct-related disqualifying factors.

#### 419.07 Pay, Leave, Etc.

- a. While teleworking an employee is bound by all of the laws, rules, regulations, and policies that govern the conduct of a GSA/OIG employee on duty at the employee's regular government worksite.
- b. The rules for overtime apply to teleworking employees. Under those rules, for example, a teleworking employee exempt from the Fair Labor Standards Act may not be reimbursed for overtime work unless previously approved and ordered by management.
- c. A teleworking employee is eligible to participate in OIG programs that are available to employees generally (e.g., Alternative Work Schedule). However, the approval of the teleworking employee's daily work schedule remains within the purview of the employee's individual Component head, RIGA, SAC, or Division Director.

#### 419.08 Telework Agreements

All OIG employees must sign a Telework Agreement, as follows. All OIG employees who do not want to telework must complete Sections A (identifying information), B (election not to telework) and F (certification/signature). All OIG employees who wish to telework, including regular, situational and emergency teleworkers, must sign and complete the entire Telework Agreement and obtain approval from their RMO prior to teleworking. The terms of the agreement must be acceptable to the RMO and the employee. See Appendix 2.

##### A. Work Schedule and Work Status:

If not otherwise specified, an employee's telework hours will be the same as the employee's official worksite duty hours.

##### B. Work Assignments:

Supervisors must ensure an equitable distribution of work assignments among employees regardless of worksite.

### C. Performance Management:

A teleworking employee is required to perform in accordance with the employee's performance standards and adhere to the terms and conditions of his/her Telework Agreement. Supervisors must use the same performance standards to evaluate the productivity of teleworkers as are used in evaluating a traditional office worker. Periodic status reports may be used within offices to access work products and productivity.

### D. Alternate Worksite:

(i) An employee who is approved to Telework will certify the safety of his/her alternate worksite as required in the Telework Agreement (Appendix 2).

(ii) High speed internet access utilizing cable, digital subscriber line (DSL) or fiber optic service is required at the alternate worksite, and it is a necessary precondition to a regular Telework Agreement (and may be required for situational telework). The choice of an internet service provider and the actual procurement of the employee's internet service is the responsibility of the employee, as are all charges for installation, maintenance and repair of related equipment. JPM (i.e. the OIG IT Service Desk) will not support the configuration, operations or installation of any of the equipment specified above.

(iii) OIG telecommunications devices (such as Aircards, USB Cellular Modems, MiFi/Jetpacks and Tethered iPhones) are not a substitute for high speed internet access and shall not be used for regular or situational teleworking. Supervisors, however, may approve the use of these devices for situational telework in limited circumstances.

(iv) The teleworking employee is responsible for the set-up and maintenance of his/her alternate worksite and associated personal equipment including telecommunications devices, office automation equipment and related supplies. It is the employee's responsibility to ensure that the alternate worksite provides the work environment, connectivity, and security consistent with the work effort in which the employee is engaged.

### 419.09 Training

A teleworking employee must take the following training prior to teleworking. This training is available through the <http://www.telework.gov> website.

Telework.Gov Training ([http://www.telework.gov/tools\\_and\\_resources/training/employees/index.aspx](http://www.telework.gov/tools_and_resources/training/employees/index.aspx))

### 419.10 Information Technology (IT) - Generally

Only OIG-furnished laptops may be used to gain access to the OIG network. OIG-furnished laptops are specifically designed and configured to meet OIG IT requirements and satisfy security mandates. Teleworkers must observe all Agency and OIG IT security requirements. These requirements are available on the OIG Intranet and GSA's InSite, and include IT Rules of Behavior; security of wireless networks; and encryption of laptops and portable media.

The following guidelines are applicable to all OIG teleworkers.

A. Obtaining Computer Hardware for Telework - Issuance of Computers:

For purposes of this policy, the OIG (JPM) will provide and support one laptop computer per teleworking employee for use at the employee's official and alternate worksites.

B. IT Support for Employees Teleworking:

JPM will not provide support at alternate worksites. Support will be provided remotely from the JPM IT help desk or at the nearest OIG location to which replacement parts may be dispatched.

C. Printers and Printing:

Employees are not authorized to print documents when teleworking from an alternate worksite that is not in GSA OIG government workspace.

D. OIG VPN Usage:

Only OIG furnished laptops will be able to access the OIG network through the OIG Virtual Private Network (VPN) connection. All OIG furnished laptops are configured to meet the security regulations required including security scans, encryption, and two factor authentications. The OIG VPN system is designated to verify the basic security of OIG furnished laptops prior to finalizing connection to the OIG network. Any system which fails these security tests will be prevented from accessing the OIG network as a security precaution to protect the OIG network.

E. Loss of Equipment:

Any employee who has a telework related IT device that is lost or stolen must immediately report that loss to the JPM Help Desk in accordance with GSA IT Security Policy (GSA Order CIO P2100.1I) and Rules of Behavior (GSA Order CIO 2104.1A). (JPM contact information can be found on the OIG internal website <http://go.gsaig.gov>.) The JPM Help desk will notify the appropriate Information System Security Officer who will begin the incident response process. Other notifications by the employee may also be required. For example, equipment lost or stolen outside of Federal facilities must first be reported to the local police that has jurisdiction and then to the OIG upon returning to the office. All OIG teleworkers should review the GSA IT policies frequently.

F. Authorized Users:

OIG employees must ensure that no one else is permitted to use their OIG-furnished laptops or the OIGVPN connection while they are teleworking.

G. Dual Homing:

Teleworking employees may not connect their OIG-provided laptops to a network other than the OIG Virtual Private Network in a Dual Homing Configuration, except at the direction of JPM to provide remote service. Examples of impermissible dual homing include, but are not limited to, "goto my pc" and "bomgar".

## H. Phone coverage

Teleworking employees must have adequate phone coverage to ensure others can readily communicate with them on work-related matters. For regions that have the OIG's Voice-Over-Internet-Phones, the JPM IT Help Desk can assist with configuration for the OIG laptop.

### 419.11 Definitions

**Alternate Worksite** - A worksite other than an OIG worksite. Presently, the only alternate worksite authorized under this policy is a space located in the employee's residence. However, a supervisor may authorize telework from a different location on a case-by-case basis if circumstances warrant.

**Component Head** - The Assistant Inspectors General; the Counsel to the Inspector General; the Associate Inspector General.

**Emergency Situation** - Includes national security situations; extended (man-made or natural) emergencies; or other unique situations upon which the Agency/OIG is closed or access to the official facilities is compromised.

**Field Work** - Routine and regular travel to conduct work in customer or other worksites as opposed to a single authorized alternative worksite (e.g., site audits, site inspections, investigations, property management, traveling between worksites, or on Temporary Duty (TDY)).

**Official Worksite** - Pursuant to 5 CFR §531.605, an employee's official worksite generally is the location where the employee regularly performs his or her duties when he/she is not teleworking.

**Responsible Management Official (RMO)** - The supervisor with whom an employee agrees to the terms of the employee's Telework Agreement.

**Telework** – An approved work arrangement at a site other than an employee's official worksite. Telework does not include any part of work done while on official travel or field work.

**Telework Agreement** - A written agreement completed and signed by an employee and appropriate official(s) that outlines the terms and conditions of the telework arrangement.

**Telework Management Official** – An established position within the OIG (JP) responsible for: (a) policy development and implementation related to the OIG's telework program; (b) advising OIG officials; (c) being a primary point of contact for the Office of Personnel Management on telework matters; and (d) performing other duties as assigned. The OIG TMO is the HR Director.

**Telework-ready** – all OIG employees who are eligible to telework because they have a completed, signed and approved Telework Agreement wherein the employee has chosen to participate in telework.

**Teleworker** - An OIG employee who is approved for telework and performing OIG work at an alternate worksite.

Effective Date 6/30/2016

## 420.00 OIG POLICY ON COLLABORATIVE RESOURCES AND SOCIAL MEDIA

The OIG follows GSA's Information Technology (IT) security policies, which include 2100.1J CHGE 1 CIO GSA Information Technology (IT) Security Policy, 2104.1A CIO CHGE 1 GSA Information Technology (IT) General Rules of Behavior, 2160.2B CIO CHGE 1 GSA Electronic Messaging and Related Services, and CIO 2106.1 (Social Media Policy) to the extent they do not conflict with the OIG mission. The OIG also may expand on those policies through separate OIG policies. This policy sets out additional rules governing OIG employee access to GSA collaborative resources, social media and similar IT systems that provide individuals an opportunity to create and share content. Examples of such systems include Chatter, Facebook, Twitter, Salesforce, LinkedIn, Gmail, Gcal[endar], Google Chat, Google Talk, Google Docs, Google Groups, Google Sites and Google Drive.

Please note that the GSA Google cloud accounts created by JPM for OIG employees, also known as GSA alias accounts, automatically grant access to many of these collaboration tools and require employees to follow the rules and responsibilities identified in section 420.02. OIG personnel may only obtain access to alias accounts for official purposes.

### 420.01 Applicability

This policy applies to all OIG authorized users, which include employees, contractors or other third parties who: (1) process or handle any OIG-owned information, data or IT equipment; or (2) access OIG IT systems to conduct business on behalf of, or with, the OIG.

### 420.02 Rules and Responsibilities

The following rules and responsibilities apply to all OIG authorized users, in addition to those set forth in GSA policy.

- OIG authorized users generally will have read-only access to collaborative resources, social media and similar systems maintained by/for GSA or the OIG (i.e. OIG authorized users may not create, add, delete, or otherwise modify data). Supervisors may authorize more than read-only access as appropriate.
- All OIG-generated or sourced information placed by an OIG authorized user on a GSA or OIG collaborative resource, social media or similar system without prior authorization from an OIG supervisor will be deleted upon discovery.
- OIG authorized users should assume that any information posted on a GSA or OIG collaborative resource, social media or similar system will be further disseminated.
- OIG authorized users acting in their official capacities generally should not, without prior supervisory authorization, create or share content (e.g., post comments) that can be attributed to the OIG on GSA collaborative resources, social media or similar systems.
- OIG authorized users may submit requests to administrators of GSA collaborative resources, social media or similar systems for additional access/permission rights in situations where upgraded access is required to read content (e.g., Google Group moderator grants OIG authorized user with system access

in order to view group posts, articles, documents, etc.). Users that gain upgraded access in this manner are not authorized to create or share content without supervisory approval.

#### 420.03 Penalties for Non-Compliance

Users who do not comply with this policy may have their access to specific GSA and/or OIG collaborative resources, social media or similar systems revoked and may incur disciplinary action – up to and including termination – as well as civil liability.

Effective Date 1/5/2018

## 421.00 INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) FOR INDIVIDUALS WITH DISABILITIES - SECTION 508 OF THE REHABILITATION ACT OF 1973

### 421.01 Purpose

Section 508 of the Rehabilitation Act of 1973 ensures that employees with disabilities have access to electronic data and information technology through the use of assistive technology. OIG exceptions to this GSA Order are noted under 421.03 Policy, below.

### 421.02 Scope and Applicability

OIG staff must comply with Section 508 of the Rehabilitation Act of 1973.

The Office of Inspector General (OIG) follows GSA Order 2105.1C CHGE1, CIO GSA Section 508: Managing Information and Communications Technology (ICT) for Individuals with Disabilities. For general references also see on GSA InSite:

- Section 508 Procedures Handbook
- Section 508 Accessibility Program
- GSA 508 Agency Roles and Responsibilities

### 421.03 Policy

- The website master will ensure compliance by captioning of all audio and video multimedia developed or procured and posted on the GSA OIG Intranet website.
- As the designated POC, the GSA OIG Service Desk Manager fields general Section 508 compliance questions related to OIG IT content and accessibility. An IT-specific Section 508 question is initiated with an IT Service Desk ticket. The ticket is then routed to the appropriate group, website manager, or support specialist, who is then responsible for providing the appropriate response to the ticket initiator.
- The GSA OIG Director of Information Technology is the agency official responsible for establishing guidance on Information and Communications Technology (ICT) accessibility management for the OIG.

### 421.04 Contracting Personnel

The OIG contracting office (JPC) is responsible for complying with all contracting requirements in GSA policy 2105.1C CHGE1.

### 421.05 508 Exceptions

The GSA OIG Assistant Inspector General for Administration is responsible for reviewing general exception requests from OIG managers using form GSA 508: Request for Exception to the Section 508 Requirement, which can be found under Exhibit A: Request for Exception to the Section 508 Requirement on the OIG website.

Effective Date 12/12/2013

#### 422.00 PURCHASE AND USE OF KITCHEN APPLIANCES

On June 25, 2004, the Government Accountability Office (GAO) issued a decision (#B-302993) that concluded agencies may use appropriated funds to purchase certain kitchen appliances when the primary benefit of their use accrues to the agency, notwithstanding a collateral benefit to the individual.

Pursuant to GAO's recommendation, the OIG is adopting this policy to ensure uniformity in the use of appropriations to acquire kitchen appliances and in the determination of the usefulness of appliances in light of operational benefits and the responsibility to provide a safe work environment.

This policy applies to kitchen appliances such as refrigerators and microwave ovens located in areas accessible to multiple employees.

##### 422.01 Policy

The use of appropriated funds to purchase kitchen appliances is proper when the primary benefit stemming from the use of such appliances accrues to the agency and not to individual employees. All requests for the purchase of kitchen appliances shall be forwarded to JPF for initial review to ensure that appropriate space and conditions exist for the type of kitchen appliance(s) proposed for purchase.

If space and other requirements are met, JPF will forward the request to JP for appropriate internal coordination and final approval. Once a final decision is made, the request will be returned to the requestor. If approved, the requesting component's operational funds will be used to fund the kitchen appliance. Funding must be available in the component's operational budget. In any given year, no component may spend more than a minimal amount of its operational budget on such purchases, and the cost of each appliance must be kept to a reasonable amount. The requesting component should be mindful of the current budget climate before requesting the appliance.

Upon purchase, kitchen appliances will become attached or installed equipment, and removal from the facility at any time and for any purpose except as is necessary for approved repairs and general maintenance is prohibited. Notwithstanding the above provision, appliances may be moved if OIG operations at a particular location are moved to other facilities.

Note: OIG funds may not be used to pay for goods consumed in the use of the appliances (for example, microwavable frozen foods), which are the responsibility of employees using those appliances.

##### 422.02 Procedures

1) Upon identifying the need for kitchen appliance(s), in accordance with the business need justification criteria in this policy, the OIG component head or designee shall submit a request to JPF. That request should contain, at a minimum, the following information:

- a) Building Name/Number
- b) Room Number(s)
- c) List and quantity of kitchen appliance(s) that have been identified along with power requirements and approximate dimensions

2) If JP authorizes the purchase, the requesting OIG Component may then purchase the kitchen appliance(s) using existing procurement mechanisms including the SmartPay/IMPAC Card or a properly executed purchase request (PR).

#### 422.03 Business Need Justification: Criteria

The justification of business need submitted by the requesting OIG Component to JPF for the purchase of kitchen appliance(s) must demonstrate that the worksite to receive the kitchen appliance(s) meets the following criteria.

- 1) The area in which the appliance(s) is to be placed is centrally located and accessible to multiple employees.
- 2) The employee population that will be receiving and utilizing the appliance justifies the size and type of item needed.
- 3) The purchase of the kitchen appliance will be a benefit to the agency, and not just to individual employees.

Effective Date 9/28/2017

## 423.00 CONFERENCE PROCEDURES

### 423.01 Purpose and Scope

Pursuant to Office of Management and Budget (OMB) Memoranda M-12-12 (Promoting Efficient Spending to Support Agency Operations), M-11-35 (Eliminating Excess Conference Spending and Promoting Efficiency in Government), M-17-08 (Amending OMB Memorandum M-12-12, Promoting Efficient Spending to Support Agency Operations) and Executive Order 13589 (Promoting Efficient Spending) the Office of Inspector General (OIG) for the General Services Administration (GSA) will limit its conference attendees to the minimum number and time required, and adopts the following procedures and internal controls for OIG conference expenditures. The OIG also adopts Appendix C to GSA Order OAS 5785.1A, (Conference and Event Management) but no other portion of that order.

These procedures and controls provide accountability and transparency regarding OIG conference expenditures, ensure that all conference expenses and activities comply with both the Federal Travel Regulation (FTR) and the Federal Acquisition Regulation (FAR), and are justified by the mission needs of the OIG.

These procedures and controls apply to conference sponsorship, conference hosting, or attendance of OIG employees at conferences sponsored or hosted by other Federal or non-Federal entities. These controls do not specifically address what items may be provided at a conference, or compliance with appropriate requirements in selecting a site; any questions in these areas should be addressed to JP.

### 423.02 Definitions

Conference – As defined in OMB Memorandum M-12-12 and the Federal Travel Regulations, a conference is "[a] meeting, retreat, seminar, symposium or event that involves attendee travel. The term 'conference' also applies to training activities that are considered to be conferences under 5 C.F.R. 51-0.404."<sup>[1]</sup>

[1] "Agencies may sponsor an employee's attendance at a conference as a developmental assignment under section 4110 of Title 5, United States Code, when—

- (a) The announced purpose of the conference is educational or instructional;
- (b) More than half of the time is scheduled for a planned, organized exchange of information between presenters and audience which meets the definition of training in section 4101 of Title 5, United States Code;
- (c) The content of the conference is germane to improving individual and/or organizational performance, and
- (d) Development benefits will be derived through the employee's attendance."

5 C.F.R. § 410.404.

The term "conference" for the purpose of this policy shall mean an organized and formal meeting, whether conducted face-to-face or through the use of information technology, where individuals assemble (or meet virtually) to exchange information and views or explore or clarify a defined subject, problem, or area of knowledge, whether or not a published report results from such meeting, where at least one OIG employee will incur reimbursable official travel expenses— i.e. non local travel expenses. However, to the extent a meeting or event requiring only local travel also includes expenses for registration, exhibitor, conference or other key indicia of a conference, such event shall be deemed a conference.

The term "conference" for the purpose of this policy does not include training (e.g., a lecture where the primary focus is to listen to or learn from the presenter) that is held as a separate matter and not part of a conference, meetings related to operational functions such as technical and administrative site visits, normal mission-related travel by any OIG employee to conduct OIG business in connection with a specific review, investigation, inspection, evaluation, or audit (e.g., travel to meet with an auditee, or witness in an investigation or review), whether conducted face-to-face and/or through the use of information technology. Nevertheless, in arranging these business meetings, managers should keep in mind M-12-12's and M-17-08's instruction to reduce travel costs as much as possible without impairing the effective accomplishment of the agency's mission. Any question about whether a meeting is a conference under this policy should be discussed with JP.

Conference Expenses - all costs paid by the Government for a conference, whether paid directly by agencies or reimbursed by agencies to travelers or others associated with the conference (e.g., speakers, persons contracted to plan the conference or assist with the conduct or logistics of the conference, etc.). Such costs include, but are not limited to, the cost of pre-conference planning activities, travel to and from the conference, ground transportation, lodging, meals and incidental costs, meeting room rental, audiovisual costs, registration fees, speaker fees, honoraria, other conference-related administrative fees, and the cost of employees time spent on en route travel and at the conference. Conference expenses, as defined in M-12-12 and M-17-08, do not include Federal employee time (i.e. salary expense) for conference preparation, and conference fees should be net of any fees or revenues received by the agency through the conference and should not include costs to ensure the safety of attending government officials.

Site Selection Factors - include commuting distance of attendees, convenience to the organization, removal from workplace distractions, administrative fees, availability of facilities (space, equipment, and supplies), speaker fees, employees' time spent at the conference, and travel to and from the conference.

Training - "the process of providing for and making available to an employee, and placing or enrolling the employee in a planned, prepared, and coordinated program, course, curriculum, subject, system, or routine of instruction or education, in scientific, professional, technical, mechanical, trade, clerical, fiscal, administrative, or other fields, which will improve individual and organizational performance and assist in achieving the agency's mission and performance goals" (5 U.S.C. § 4101).

Official Travel - please see GSA Order 1ADM 4290.1, GSA Order OAS 5770.1, and OIG Policy 406.

### 423.03 Designation

Executive Order 13589 states each agency, agency component, and office of inspector general should designate a senior level official to be responsible for developing and implementing policies and controls to ensure efficient spending on travel and conference related activities. That person for the OIG shall be the Assistant Inspector General for Administration (AIG for Administration).

### 423.04 Conferences Hosted or Sponsored by the OIG

#### 423.04A Planning

Each office within the OIG that plans to host or sponsor a conference – including the Office of Audits (JA), Office of Counsel (JC), Office of Inspections (JE), Office of Investigations (JI) and Office of Administration (JP) -- should prepare a plan, including Site Selection Factors, as a means for the OIG to ensure the proper use of funds for all conferences, including conferences that are considered training activities under 5 CFR 410.404.

Each OIG office should explore the use of videoconferencing as a viable option for conferences within the OIG. Funding should always be a consideration in creating the plan. OIG office conference plans must be approved by the head of the office, or his or her designee.

Each office shall submit its conference plan to the AIG for Administration at least three months before any planned conference if the anticipated expense exceeds \$3,500. Six weeks for all other conference plans. The AIG for Administration will then submit them to the Deputy Inspector General (DIG) for preliminary approval. No funds should be obligated unless and until approved.

#### 423.04B Approval Requirements

Pursuant to OMB M-17-08:

A. Any planned conference hosted or sponsored by the OIG, or by other Federal or non-Federal entities, for which the net expenditures by the OIG would exceed \$500,000 must be pre-approved by the Deputy Inspector General (DIG). In order for the conference to be approved, the DIG must make a determination, in writing, that a single conference is the most cost-effective option to achieve a compelling purpose.

In addition, the DIG must approve ALL other conferences hosted or sponsored by the OIG.

#### 423.04C Process for Requesting Approval

OIG offices planning to host or sponsor a conference -- for training or non-specific operational purposes -- shall submit the "GSA OIG Request for Approval of Meeting/Training" sheet (OIG Conference Sheet) (Appendix 1) to the AIG for Administration. This approval form needs to be completed for all conference requests regardless of cost. The AIG for Administration will forward all OIG Conference Sheets to the DIG for approval. The OIG Conference Sheet also will function as a Purchase Request (PR) as needed.

More specifically, the procedures for seeking approval for an OIG hosted or sponsored conference are as follows:

Step 1: The OIG office completes the OIG Conference Sheet (Appendix 1) and (as necessary) prepares a Statement of Work/Need (SOW).

The OIG Conference Sheet ensures that the DIG has the information needed in order to determine whether or not the request should be approved. Consequently, all parts of the form should be completed as accurately as possible and contain:

- Basic Information: the name, type of conference, dates and location, name(s) of training class(es) and any suggested vendors (not required), and agenda;
- Statement of the Mission Purpose: the justification for the conference, including the results expected to be obtained;
- Estimated Expenses: pre-conference planning travel and hotel costs (if any), travel and per diem, hotel, meeting space, audiovisual use, light refreshments, ground transportation, instructors, and any other costs;
- Statement of Work or Need (SOW): SOW with exact requirements and justification, including very specific information such as number of attendees, agenda and times, room set-up (i.e., U-shaped), audiovisual needs, refreshment needs and schedule, type of trainer(s) and hotel arrival and check-out date.

Step 2: The OIG office submits the OIG Conference Sheet and SOW to the AIG for Administration for review.

- JP will conduct an initial review of requirements.
  - Once JP determines all requirements are met, the JP signatory (usually the AIG for Administration) will forward the package to the DIG for approval.
  - When applicable, if approved by the DIG, the package is submitted to the Budget and Financial Management Office (JPB) for funding approval.
  - Once all the approvals have been received, the package is forwarded to the Contracting Office (JPC) for procurement action, if needed.
- Step 3: Procurement (if needed).

Procurement will proceed according to the requirements on the OIG Conference Sheet and SOW.

- Before an award is made, JPC will work with the OIG office requesting the conference to select a vendor(s) at a fair and reasonable price and in compliance with applicable laws and regulations.

JPC will make the award and notify the OIG office.

- JPC notifies the OIG office of any scheduling particulars, such as how to register and any cut-off dates.
- While attending the conference, if difficulties or additional needs arise, JPC should be contacted immediately.

#### 423.04D Required Submittals After the Conference

After a conference, the OIG office that hosted or sponsored the conference must submit an updated OIG Conference Sheet to the AIG for Administration that shows the actual expenses incurred. JP will compile and track all expenses spent on conferences. If the actual cost was 120% or greater than the estimated cost, the AIG for Administration will inform the DIG.

#### 423.05 Attendance at Conferences Not Sponsored or Hosted by OIG

OIG offices must notify, before any funds are committed on a nonrefundable basis, the AIG for Administration if they anticipate sending more than 10 employees to one conference or spending more than \$1,000 per attendee for any one conference. The \$1,000 does not include travel; it includes only the conference fee. That notice must include the conference date, when a decision is needed, who is planning on attending, the justification, and the approximate total estimated cost, including travel. Notices should be sent via email.

The AIG for Administration will review the request and then forward to the DIG for approval. The AIG for Administration will make every attempt to inform OIG offices of the DIG's decision regarding conference attendance as quickly as possible.

OIG offices should consult with the AIG for Administration if they need to register and commit funding before they receive a decision from the DIG.

#### 423.06 Website Reporting

JP is responsible for ensuring proper website reporting of conference expenses, as follows. Net OIG conference expenses where the particular conference expenses were in excess of \$100,000 shall be reported on the OIG internet site annually, no later than January 31 of each year, starting in 2013. Reporting shall be on a dedicated place on the OIG website and include a general report about conference expenses and activities throughout the year.

For any OIG conference where the net expenses for the OIG exceeded \$100,000, the report shall include:

- the total conference expenses incurred by the OIG for the conference;
- the location of the conference;
- the date of the conference;
- a brief explanation of how the conference advanced the mission of the agency; and
- the total number of individuals whose travel expenses or other conference expenses were paid by the OIG.

For any OIG conference where the net expenses for an agency sponsored conference exceeded \$500,000, the website also shall include the IG's determination that the conference was the most cost-effective option.

Finally, the website shall include information about the net conference expenses for the fiscal year incurred as well as a general report about conference activities throughout the year. In order to ensure proper reporting, each OIG component shall provide to the AIG for Administration, via email, a listing of the information referenced above for all conferences attended by employees within their components by December 31 of each calendar year.

Effective Date 6/30/2016

## 424.00 IT EQUIPMENT REQUEST POLICY

### 424.01 Purpose

With IT devices and equipment becoming more commonplace, the OIG must ensure requests for these assets meet the operational and fiscal needs of our organization while also maintaining the appropriate level of security for the OIG. The successful effort required to meet these needs relies on the cooperation of the various OIG components, the budget, contracting, and financial management offices, and the IT division.

This policy covers all OIG IT equipment that requires a connection to the OIG network and/or requires support from JPM to operate or manage, in order to ensure equipment is compatible with OIG IT systems and that proper security policies are followed. This policy replaces the OIG Individual Equipment Policy and the Personal Printer Policy.

### 424.02 GSA Policy References

- IT Security Procedural Guide: Securing Mobile Devices and Applications, CIO-IT Security-12-67.
- 2100.1J CHGE 1 CIO GSA Information Technology (IT) Security Policy

### 424.03 Policy

- As stated in OIG Policy 718.05 Prohibited Purchases, the procurement card cannot be used to buy Information Technology equipment, except for consumable supplies. Requests for IT equipment should originate from the component head or their delegated approver(s). This will ensure that managers are aware of requests being made by their employees and that the request meets the mission needs of the business line.
- The request may be in the form of an email or procurement request (PR) for any item costing \$3,000 or less, but must be in a PR for items costing more than \$3,000. In accordance with section 204.06, the request should be made to the OIG Contracting Office, which shall ensure appropriate approvals are obtained.
- Requests will be reviewed by JPM to ensure all security procedures and policies are followed. This includes, but is not limited to, ensuring the equipment is compatible with the OIG IT infrastructure, hardening the equipment against vulnerabilities, and having the ability to maintain and support the equipment.
- Personal desktop printers will be approved for all GS-15 and GS-14 employees as well as anyone who supervises employees.
- The Office of Investigations may purchase IT equipment in support of an investigation(s) and/or mission using the purchase card as necessary in exigent circumstances; however, such equipment is not to be connected to the OIG network or JPM issued/supported IT equipment without formal review and approval by JPM to determine whether there are potential security, support, technology conflicts.

#### 424.04 Exceptions

Exceptions to the requirements of this policy may be requested by component heads, but shall be granted solely at the discretion of the IG, who may decide to consult with the IT Steering Committee before making a decision.

Effective Date 7/8/2016

## 425.00 OIG WAIVER OF CLAIMS FOR OVERPAYMENT OF PAY AND ALLOWANCES AND OF TRAVEL, TRANSPORTATION, AND RELOCATION EXPENSES AND ALLOWANCES

### 425.01 Introduction

This policy establishes the procedure to process a waiver of claims arising from erroneous payments of pay and allowances, travel, transportation, and relocation expenses and allowances made to or on behalf of OIG employees, where repayment would not be in the public's best interest.

### 425.02 Authority and Responsibilities

5 U.S.C. § 5584 authorizes the waiver of claims by the United States, in whole or in part, against employees arising out of erroneous payments of pay and allowances, travel, transportation, and relocation expenses and allowances. Congress transferred the authority to waive claims for erroneous payment from the Comptroller General to the Office of Management and Budget (OMB). P.L. 104-316 (1996). OMB subsequently redelegated this waiver authority to the executive agency that made the erroneous payment.

The Administrator of General Services Administration has delegated to the Inspector General (IG) the authority to review requests for waivers for pay and allowances and for travel, transportation, and relocation expenses and allowances submitted by OIG employees. GSA Order ADM 5450.39D. The IG has redelegated to the Deputy IG the authority to waive or deny claims in any amount; the Deputy IG may delegate that authority further, and as stated in this policy has delegated the initial determination of whether waiver is proper to the Associate Inspector General.

### 425.03 Definitions

"Pay" means basic pay, special pay, incentive pay, retainer pay, or in the case of an individual not entitled to basic pay, other authorized pay.

"Allowances" refer to payments made for subsistence, quarters, uniforms, family separate maintenance allowances, and overseas station allowances. Pay or allowance does not include travel expenses or expenses to transport household goods.

"Debt" is an amount of money, funds or property that has been determined by an agency official to be due the United States from any person, organization, or entity, except another Federal agency. For the purposes of this policy, the terms "debt" and "claim" are synonymous and interchangeable.

"Waiver" means the cancellation, remission, forgiveness, or non-recovery of a debt allegedly owed by an employee to an agency.

"Fault" exists if, in light of all the circumstances, it is determined that the employee knew, or should have known, that an error existed, but failed to take action to have it corrected. Fault can be derived from an act or a failure to act. Unlike fraud, fault does not require a deliberate intent to deceive. Whether an employee should have known about an error in earnings is determined from the perspective of a reasonable person.

#### 425.04 Applicability

This policy addresses erroneous payment of pay and allowances and of travel, transportation, or relocation expenses and allowances made to or on behalf of OIG employees. The policy does not affect authority to litigate, settle, compromise, or waive any claim of the United States under any other statute. As stated in the GSA Accounts Receivable and Debt Collection Manual, 4253.1A CFO P, ordinarily, a legal and proper payment may not be considered for waiver, although owing to later circumstances, the individual may have to repay all or part of the overpayment. Examples of legal and proper payments, not subject to waiver consideration, include:

- a. Advanced annual or sick leave unearned at the time of separation.
- b. Advanced uniform allowances not earned at the time of separation or upon transfer from the work unit that required the uniforms.
- c. Voluntary Separation Incentive Program (VSIP) repayment if the employee returns to Federal Government service.
- d. Federal Employee Health Benefits (FEHB) insurance premium payments made on behalf of the employee while in an extended period of Leave without Pay (LWOP) and when an employee has elected to continue FEHB coverage while on LWOP.
- e. Lump sum leave payments that must be refunded if the person is re-employed in Federal service prior to expiration of the period of annual leave related to the lump sum leave period.

A request for a waiver of a claim shall not affect an employee's opportunity under 5 U.S.C. § 5514(a)(2)(D) for a hearing on the determination of the agency concerning the existence or the amount of the debt, or the terms of the repayment schedule. A request by an employee for a hearing shall not affect an employee's right to request a waiver of the claim. The determination whether to waive a claim may be made at the discretion of the deciding official either before or after a final decision is rendered on the claim.

#### 425.05 Waiver Requirements

For a waiver to be considered, the OIG must receive the proper documents for waiver within three years from the date of discovery of the overpayment. A waiver may be considered when collection of the claim would be against equity and good conscience and not in the best interest of the United States provided that there does not exist, in connection with the claim, an indication of fraud, misrepresentation, fault, or lack of good faith on the part of the employee or any other person having an interest in obtaining a waiver of the claim.

#### 425.06 Waiver Processing

##### 425.06A Requests

The employee must submit a request for waiver of the erroneous payment. The request must be in the form of a memorandum that provides a description of the overpayment, the amount, all documentation relating to the overpayment, and a statement by the employee that he/she was unaware of the error. Any subsequent payments received by the employee after the administrative error has been discovered

and the employee is notified are not subject to waiver and must be repaid or collected. The employee's request for waiver shall be sent to the Office of Administration (JP), 1800 F Street N.W., Room 5022, Washington, DC 20405.

#### 425.06B Report of Investigation

A waiver of overpayment may not be considered without a report of investigation. Both the Office of Administration (JP) and the "responsible debt area" (i.e. the OIG component who approved the payment) are responsible for preparing the investigative report for all OIG employees, although they may request another OIG component to conduct the investigation. The report of investigation (prepared using GSA Form 2578) must include the employee's name, the employee's OIG office address, the date of discovery of the error, the amount of the overpayment, a description of the overpayment, a statement of finding (re: fault on part of employee) and a recommendation to waive or deny the request for waiver.

The report of investigation (GSA Form 2578) will address the following five factors:

1. Was the overpayment a result of an administrative error? An administrative error occurs when the agency fails to carry out written administrative policy or fails to comply with mandatory regulations. This includes, but is not limited to misinterpreting policies or regulations causing an incorrect payment to occur.
2. Has action been initiated to preclude this type of error in the future? The answer to this question should describe what positive action has been taken to avoid a similar error.
3. Is there any evidence of fraud, misrepresentation, fault, or lack of good faith on the part of the employee or other person having an interest in this claim?
4. Could the employee have been reasonably expected to suspect an error? A judgment will be made whether a reasonable person could be expected to detect an error on the official forms (travel authorizations or other documents provided to the employee). If the answer to this question is yes and the employee fails to advise the appropriate GSA offices of a suspected error, the overpayment will be repaid. Good faith is required of the employee. Every case will be examined in light of its particular facts. For example, if an employee's job requires knowledge of travel regulations, the conclusion as to fault may be different than an employee who has no knowledge of travel regulations.
5. Would collection of the overpayment be against equity, good conscience and the best interest of the United States? Generally, there is sufficient evidence to waive repayment if an erroneous payment occurs through administrative error and there is no indication of fraud, misrepresentation, fault, or lack of good faith. Waiver of travel, transportation, and relocation allowances must depend upon the facts existing in the particular case. The facts upon which a waiver is based should be recorded in detail and made a part of the written record.

The final investigative report will be provided to the Associate Inspector General who, based on an evaluation of the facts, will decide whether to waive or deny the claim. A copy of the final waiver decision will be provided to the employee and to GSA's Financial and Payroll Services Office in Kansas City so that Financial and Payroll Services can take appropriate action, such as collecting any overpayment from the employee pursuant to the GSA Accounts Receivable and Debt Collection Manual,

4253.1A CFO P, or, if the claim is granted, making any required notification to the IRS. If the employee has repaid all or part of a waived claim, the employee must contact Financial and Payroll Services to apply for a refund.

#### 425.06C Appeals

If an employee wishes to have a claim reconsidered, a request and any new information relevant to the appeal should be submitted to the Assistant IG for Administration, 1800 F Street, NW, Room 5022, Washington, DC 20405. The request for an appeal must:

- a. be made in writing;
- b. specify the basis for appeal;
- c. include a statement regarding any mitigating factors;
- d. be submitted to the Assistant IG for Administration no later than 60 days from receipt by the employee of written notice of the denial of the waiver; and
- e. attach the original request for a waiver and the denial of the waiver.

The Assistant IG for Administration will provide the request to the Associate Inspector General, who will make a recommendation to the Deputy IG, who will then make the final decision on the request for reconsideration.

#### 425.06D Repayment

While the GSA OIG policy permits reimbursement of professional credential expenses (including membership fees, examinations, registration fees and travel costs) certain ineligible reimbursements are not necessary to obtain or renew the credential (i.e. a condition precedent to the credential). See 5 U.S.C. § 5757 and GSA OIG Manual Sections 418.01 and 418.04. Because there is no statutory authority for the reimbursements listed above, the GSA OIG must recoup the overpayment.

In an effort to recoup the overpayment, GSA OIG will notify the current or former employee via certified mail. Upon receiving the Notice of Overpayment of GSA OIG Funds, the employee must take one of the following actions within 30 days from the date of the notice:

- Repay the debt. Employees must remit the full amount, in a check or money order payable to General Services Administration (GSA) with a brief explanation for his/her payment on the memo line, to the OIG Budget Office (JPB), located at 1800 F Street N.W., Room 5032, Washington, D.C. 20405. In addition, the employee must provide an approximate time frame(s) and ConcurGov document, claim or other number(s) associated with the initial transaction(s), if available.
- Agree to a repayment plan. If the employee is unable to pay the amount in full, s/he must contact the undersigned to discuss a mutually acceptable repayment plan. The employee should refer to the enclosed Notice of Rights for further information on alternative payment arrangements.

#### 425.07 Recordkeeping

JP will maintain a register that shows the disposition of each claim or overpayment. The register and supporting files will be available for review as requested and appropriate.

Effective Date 9/23/2015

## 426.00 OPERATIONS IN THE ABSENCE OF APPROPRIATIONS

### 426.01 Purpose

This policy sets forth the standards and procedures governing OIG operations in the absence of appropriations. GSA policy on operations in the absence of appropriations is contained in GSA Order ADM 4220.1K, Operations in the Absence of Appropriations. With the exception of the provisions discussed below, the OIG adheres to the plan outlined in GSA Order ADM 4220.1K.

### 426.02 Implementing Action

All OIG employees will follow the implementation plan set forth in Section 2 of the Attachment to GSA Order ADM 4220.1K. The implementation plan goes into effect only when authorized by the Inspector General (IG) upon direction from the Office of Management and Budget (OMB).

### 426.03 No Year Funding

In the event the OIG has no year funding available, the IG will decide as appropriate when they will be utilized for mission critical needs.

### 426.04 Exempt and Excepted Personnel and Activities

The Inspector General is exempt from furlough due to a lapse in appropriations.

Excepted personnel are the Deputy Inspector General and the minimum number of other personnel, as designated by the Inspector General or Deputy Inspector General, needed to conduct excepted activities to protect life and property, including pursuing or directly supporting law enforcement and criminal investigations or other legal proceedings that cannot be deferred.

Excepted personnel may include investigators, auditors, management analysts and attorneys as needed. Excepted personnel may also include contracting officers, budget employees, personnel employees, information technology employees and facilities employees. Designated employees may be able to telework with supervisory approval, in accordance with the OIG policy on telework, depending on the specific requirement for assistance. Excepted OIG management will call non-excepted employees on their personal numbers if they become excepted.

### 426.05 Prohibition on the Use of Mobile Devices and Remote Access to OIG Systems

The prohibitions of the Antideficiency Act extend to work conducted outside of the office environment. Accordingly, non-excepted employees of the OIG are prohibited from using OIG-supplied wireless devices, such as iPhones, iPads, and/or any other means with which to remotely access OIG systems for purposes of conducting regularly assigned work.

#### 426.06 Recall System

Non-accepted OIG employees should monitor local media to determine when the lapse is over, and when they should return to work.

Effective Date 3/27/2017

#### 427.00 SELECTION AND ASSIGNMENT OF OIG EMPLOYEES FOR TEMPORARY ASSIGNMENT OR DETAIL TO THE LEGISLATIVE BRANCH

##### 427.01 Purpose

This order sets forth a process for the selection, assignment, and management of an OIG employee to be detailed on temporary assignment to committees of the United States Congress (detailee).

##### 427.02 Authority

The OIG follows GSA Order HRM 9334.2, dated July 8, 2016. 3 USC 112 authorizes the heads of Federal agencies to detail personnel to the White House; there is no statute that deals specifically with the detail of executive branch personnel to the legislative or judicial branches. Comptroller General Decisions (21 Comp. Gen. 954 and 1055) set forth guidance for details to Congress.

##### 427.03 Delegation

The management of a Congressional detailee is delegated to the Deputy Inspector General (DIG); final authority for selection of a detailee is retained by the Inspector General (IG).

##### 427.04 Implementing Actions

Effective immediately, the following actions will be implemented:

427.04A All requests for a Congressional detailee, or the extension of an existing detail must be in writing (email or letter) from the Congressional committee or sponsoring organization. All requests for a detailee will be accepted by the Congressional Affairs Liaison (CAL) or shall be forwarded to the CAL when received by another office.

427.04B Once a request for a detailee is received, the CAL shall send a call for nominations to the appropriate components with a brief description of the duties and the time commitment. Nominations in the form of a resume and a one page written request letter shall be returned to the CAL within two weeks.

427.04C Only full time OIG employees at the GS-13 grade level or above are eligible for nomination as a detailee. The IG may waive this requirement under special circumstances (e.g., special technical knowledge requested by Congress). Except under special circumstances, a detailee must be based in metropolitan Washington, DC.

427.04D The CAL will review the nominations and make a recommendation to the IG through the DIG.

427.04E The cost of the detailee shall be borne by the originating organization of the employee for the duration of the Congressional assignment.

427.04F In the absence of specific statutory authority for the detailee, the OIG shall assign the detailee to the legislative branch only if the legislative work to be performed by the detailee relates to matters ordinarily handled by the OIG and will, therefore, further the purposes for which the OIG's appropriations are made, and where the absence of the OIG employee assigned will not be detrimental to the work of the OIG or necessitate the hiring of an additional employee.

427.04G The CAL shall as appropriate establish guidelines for communication with and by the OIG detailee. OIG Counsel (JC) shall be responsible for ensuring the detailee is briefed on their responsibilities under the Hatch Act and all other ethics rules and regulations; briefings will be documented by JC.

427.04H No permanent replacement of the detailee shall be made unless the detailee is separated from the OIG or accepts a new position within the OIG. The Deputy Assistant Inspector General for Administration shall be responsible for ensuring that the temporary assignment of the detailee and the reservation of their vacated position is undertaken in conformance with this order.

427.04I OIG will maintain and approve a detailee's time and attendance, in coordination with the Congressional committee. OIG also will obtain input from the Congressional committee regarding a detailee's performance.

Effective Date 11/23/2016

## 428.00 REASONABLE ACCOMMODATION POLICY

### 428.01 Purpose

To transmit the GSA OIG policy and procedures for providing reasonable accommodation to qualified employees or applicants with disabilities.

Section 6 of the Inspector General Act of 1978 (5 U.S.C. App 3), as amended, grants the OIG independent authority to formulate policies and make determinations concerning human capital issues within the OIG. Pursuant to that authority, the OIG has determined to follow GSA's policy on reasonable accommodation as stated in GSA Instructional Letter CPO IL-13-03 ("GSA policy") except as noted below.

### 428.02 Applicability

The policy applies to all OIG employees.

### 428.03 Definition

The OIG defines "transitory and minor" as meaning a minor impairment that is expected to last six or less months and not the definition GSA uses in Attachment 1, Paragraph 2(l).

### 428.04 Legal Authority

In addition to the legal authority cited in CPO IL-13-03, Extended, the Inspector General Act of 1978 as amended provides the OIG independent personnel authority.

### 428.05 Responsibilities

1. The GSA policy limits who can be the decision-maker (DM). The OIG is not bound by that limitation, but recognizes that there may be other circumstances that warrant a different DM.
2. GSA policy frequently refers to the Office of Chief People Officer; in the OIG, those references are to the Office of Administration (JP).
3. GSA policy also refers to the Office of General Counsel; in the OIG, those references will be to the OIG Office of Counsel (JC).
4. In the OIG, the Local Reasonable Accommodation Coordinator (LRAC) will be the Employee Relations Officer. The LRAC is responsible for coordinating OIG Reasonable Accommodation requests between the employee, and the DM and to assist with implementation and record keeping of such reasonable accommodations. The LRAC is not required to consult with the GSA National Reasonable Accommodation Coordinator (NRAC) before taking any action. The LRAC is responsible for obtaining all medical documentation to support reasonable accommodation requests in consultation with OIG JC.

5. The DM shall continue the interactive process, as appropriate, even if a reasonable accommodation is granted. If questions arise about a person's disability over time, the DM shall consult with the LRAC and OIG JC.

#### 428.06 Consultation and Review of Medical Documentation

1. GSA policy refers to the LRAC coordinating with other staff offices, such as GSA Office of Civil Rights (OCR), OGC, GSA Center for Technology Access (CITA) office, or other resources to identify effective reasonable accommodation options. The OIG LRAC only consults with the GSA CITA office and/or OIG JC.

2. The OIG LRAC consults with the HR Director and OIG JC for applicants and employees, in cases where the disability is obvious and typically no medical documentation is required beyond understanding specific limitations and barriers, or if the medical documentation is insufficient to approve a request, or the request may cause an undue hardship or interferes with the department's mission.

3. Any medical information that is obtained must be kept strictly confidential in a file separate from the employee's personnel records. Supervisors and managers may be given access to the extent needed in making decisions regarding reasonable accommodation, including necessary restrictions on the duties of the employee or accommodations.

Effective Date 7/5/2016

#### 429.00 POLICY AND PROCEDURES RELATED TO MERIT PROMOTION OR PLACEMENT

Section 6 of the Inspector General Act of 1978 (5 U.S.C. App 3), as amended, grants the Inspector General independent authority to “select, appoint and employ such officers and employees” as are necessary to carry out the functions of the Office of Inspector General (OIG), and to take such actions as are necessary to carry out the duties and responsibilities of the Act. Such actions include formulating policies and making determinations concerning human capital issues within the OIG. Pursuant to that authority, the OIG has determined to follow GSA’s Order on merit promotion as stated in GSA Order 9335.1A CPO GSA Merit Promotion Plan except as noted below.

##### 429.01 Noncompetitive Candidates

The OIG hires noncompetitive candidates using the maximum flexibility permitted by law. Accordingly, the OIG may use noncompetitive candidates to fill both posted and non-posted vacancies. Noncompetitive candidates must meet minimum eligibility requirements and qualification standards by the time of appointment, as opposed to within 30 calendar days of the closing of the vacancy, if a vacancy is posted.

##### 429.02 Release for Placement

Upon receiving a written notification of a selection decision and proceed to hire notification, JPH will take appropriate action to arrange a release date with the losing office or agency.

For all Office of Inspector General employees selected for promotion under this program, the release date will be at the end of the first full pay period following the date the release is requested. For actions other than promotions, a longer period may be allowed i.e., two full pay periods; however, the release date should be no longer than two full pay periods following an official request to the losing office for a release date, unless the gaining office agrees.

Effective Date 5/3/2017

## 430.00 SUPERVISOR TRAINING

### 430.01 Purpose

This chapter establishes OIG requirements for Supervisor Training.

### 430.02 Applicability

The policy applies to all OIG employees who are appointed to supervisory positions.

### 430.03 Legal Authority

The requirement for Federal Supervisory Training is found in 5 CFR 412.202. Guidance is also provided by the Office of Personnel Management (OPM). See, e.g., <http://www.opm.gov/wiki/training/Supervisory-Leadership-Development/Print.aspx>. For SES requirements please see the AIG for Administration or the Deputy AIG for Administration.

### 430.04 Mandatory Training Requirements

All agencies are required to provide training within one year of an employee's initial appointment to a supervisory position as well as refresher training to all supervisors and managers at least every three years.

OIG Human Resources will provide the required training for new supervisors within their first year as a supervisor and refresher training every three years. This training will cover the required topics - to (1) mentor employees; (2) improve employee performance and productivity; (3) conduct employee performance appraisals in accordance with agency appraisal systems; and (4) identify and assist employees with unacceptable performance.

### 430.05 Additional Training

If the Component Head or supervisor determine that additional training may be necessary, a combination of off-the-shelf courses (e.g. Graduate School USA), on-line through GSA On-line University, seminars, and conferences can be utilized. As another option, supervisors may wish to review the GSA Leadership Competency courses identified at the GSA On-Line University.

### 430.06 Completion and Reporting of Training

JP will keep a master list of supervisors and record all required training provided by JPH. If additional supervisory training is warranted, each component is responsible for providing the training officer in JP with the training records showing completion of the additional training.

Effective Date 10/27/2017

## 431.00 OIG POLICY AND PROCEDURES FOR MEMORANDA OF UNDERSTANDING (MOU)

### 431.01 Purpose

The OIG may perform reimbursable work for or receive reimbursable work from any other Federal unit in the executive branch, including another GSA component, if it is in the position to do so and if applicable legal requirements are met. This chapter establishes OIG policy and procedures for processing Memoranda of Understanding with other federal agencies.

The OIG generally will follow GSA Order CFO P 4251.4A, Chapter 3, Part 9 and other applicable documents, such as the OMB Memo titled, "Improving the Management and Use of Interagency Acquisitions" (June 6, 2008), to the extent they address Memoranda of Understanding and they do not conflict with OIG policy.

### 431.02 Applicability

The policy applies to all Agreements between the OIG and any other government entity in the executive branch. Agreements concerning reimbursable work performed by the OIG for the legislative branch are covered in Section 427 of the OIG Manual.

### 431.03 Legal Authority

Basic authority for Federal agencies to enter into reimbursable agreements, and the way that they are handled, is contained in 31 U.S.C. 1535, commonly known as the Economy Act. Implementing regulations for interagency acquisitions are found at 48 CFR subpart 17.5. In addition, the OIG generally enters MOUs under the authority of the Inspector General Act of 1978 as amended. Components should consult with JC for other legal authorities applicable to specific MOUs.

### 431.04 Approvals

All MOUs must be authorized by the Inspector General and approved by the other agency before any services are rendered. This requirement also applies to no-cost MOUs.

For service contract MOU's, the Inspector General may delegate this authority.

For MOU's that involve employee detail assignments, the Inspector General's approval must be included on the Procurement Request (PR) Form as well as the MOU itself.

### 431.05 MOU Requirements

At a minimum, all MOUs must include the following information:

- Purpose of the MOU
- Authority for the MOU
- Scope of work to be completed
- Term of the MOU (should be within the fiscal year, October 1 through September 30)

- Costs to be incurred or reimbursed, if any
- Points of Contacts for both entities (including financial POC)
- Payment and Collection system information for both parties
- Signatures of both parties, including signature of Component Head and Budget Office Representative

#### 431.06 MOU Procedures

The following procedures must be completed for all MOUs, regardless of whether they are at cost or no-cost. MOUs drafted by the other participating agency may be accepted.

1. The component requesting/accepting the services should complete the MOU including all requirements listed in Section 431.05. The document should be signed by the head of the component and approved by JC for legal sufficiency and by the IG.
2. Once the IG has approved the MOU, the document will be forwarded to JPB for funding approval. The Budget Office Representative will provide funding approval and return the original signed copy to the component for distribution to the requesting/accepting government agency for their approval.
3. Before any services are performed, the OIG component requesting/accepting services should receive a signed copy of the MOU from the other government agency.
4. A copy of the final signed agreement should be forwarded to JPB. JPB will keep electronic and hard copies of all signed agreements.
5. Once the signed MOU is in place, services may commence. It is prohibited to accept or provide services without an agreement in place that has been executed by all required parties. The OIG component should track the services rendered/received in order to ensure funds are not overspent and the term of the MOU is not exceeded. The OIG component should report to JPB on a quarterly basis regarding the status of the MOU, and upon completion of the MOU.

Effective Date 12/12/2017

## 432.00 MISCELLANEOUS REIMBURSEMENTS

### 432.01 Purpose

The ConcurGov miscellaneous reimbursement voucher provides an efficient and cost-effective way to reimburse employees for eligible low dollar expense items. ConcurGov miscellaneous reimbursements are made in accordance with GSA and OIG policies and procedures.

The OIG generally follows GSA Memorandum, "Policy Guidance for the GSA Purchase Card and E2 System Miscellaneous Reimbursements" (January 3, 2013) and GSA Order PFM P 4290.1 Extended, Chapter 7, insofar as they address miscellaneous reimbursements and except where doing so would be inconsistent with an OIG policy. This policy can be found at:  
[https://insite.gsa.gov/portal/mediaId/556906/fileName/Policy\\_Guidance\\_GSA\\_Purchase\\_Card\\_and\\_E2\\_System\\_Miscellaneous\\_Reimbursements\\_Memo\\_v2.action](https://insite.gsa.gov/portal/mediaId/556906/fileName/Policy_Guidance_GSA_Purchase_Card_and_E2_System_Miscellaneous_Reimbursements_Memo_v2.action).

### 432.02 Applicability

This policy applies to all OIG employees.

### 432.03 Authorized Miscellaneous Claims

The ConcurGov (CGE) travel system must be used to process all miscellaneous reimbursements. Miscellaneous expenses are generally a one-time occurrence for which the government receives a benefit. Employees incur these expenses in one of two ways. Employees perform local travel for which they are reimbursed and they purchase items for which they can be reimbursed. Employees are reimbursed if the underlying expense was authorized and if the claim is legally payable. Acceptable miscellaneous expenses may include:

1. Local mission travel (in excess of an employee's normal, daily round trip commuting costs)
2. Local training travel (in excess of an employee's normal, daily round trip commuting costs)
3. Professional liability insurance
4. Continuing legal education training
5. Elective training (see Chapter 413 of this Manual)
6. Professional credentials (see Chapter 418 of this Manual)
7. Purchases made by JI in exigent circumstances to support an investigation or mission when a purchase cardholder is not immediately available to purchase through usual authorized means.

### 432.04 Unauthorized Miscellaneous Claims

Miscellaneous reimbursements will not be authorized for routine supply purchases that can and should be made using the official government purchase card. Reimbursements will also not be approved for personal preference items that the employee chooses to purchase instead of using government furnished items.

Effective Date 12/1/2014

#### 433.00 POLICY REGARDING INTERN ACCESS TO OIG INFORMATION TECHNOLOGY (IT)

##### 433.01 Purpose

Given that most interns work for short terms of employment and the federal government does not conduct comprehensive background investigations of those interns, they potentially pose a security risk. Accordingly, this policy is intended to ensure that OIG IT resources, data, and applications are kept secure and protected.

##### 433.02 Policy

Interns will not be given access to OIG IT resources, data, or applications without supervisory approval. Supervisors are responsible for approving, coordinating, and monitoring all necessary or required access to OIG data by their interns. Supervisors must provide a written notice (e-mail will suffice) to JPM stating what OIG IT resources, data, or applications each intern is to be given access to; by doing so, the supervisor accepts responsibility for the intern's actions regarding that access. Supervisors also are responsible for the interns' use and return of government furnished equipment. JPM will track access requests, grant access and later remove access when the intern departs. Additionally, JPM will provide reports of access as requested.

Effective Date 11/22/2017

## 434.00 OIG INFORMATION TECHNOLOGY (IT) SECURITY POLICY

### 434.01 Purpose

The OIG follows the latest version(s) of GSA Orders on IT Security except where doing so would be inconsistent with an OIG policy. These policies include:

- CIO 2100.1K GSA Information Technology Security Policy
- 2181.1 CIO P Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing
- 2182.2 CIO Mandatory Use of Personal Identity Verification (PIV) Credentials,
- 7640.4 2ADM (Revalidated) GSA Smart Card
- 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
- 9297.2C CIO GSA Information Breach Notification Policy.

Specific IT security policies for the OIG are as follows.

### 434.02 Incident Response Reporting Procedures

Personally Identifiable Information (PII), as defined in OMB Memorandum M-07-16, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Examples include, but are not limited to social security number, date and place of birth, mother's maiden name, and medical history.

All OIG employees must report suspected PII loss, security violations, security incidents, and incidents involving the loss or theft of OIG hardware or software to their supervisor and the OIG IT Service Desk as soon as the incident is identified. The OIG IT Service Desk notifies the OIG Information System Security Manager (ISSM) who is responsible for reporting security incidents to the GSA Chief Information Security Officer (CISO). The ISSM will include the Office of Investigations in any security reports submitted to the GSA CISO. PII incidents that are identified outside of the OIG IT Service Desk core business hours (Monday through Friday 8:00 – 4:30 Eastern Time) are to be reported using the "Report an IT Incident" icon on the OIG Intranet homepage. This will direct the user to enter a ticket to the OIG IT Service Desk. Contact information for the Director of JPM and the ISSM are also located with the icon for emergencies. The OIG IT Service Desk will notify the Director of JPM and the ISSM of all incidents involving PII or hardware/software loss. The Director of JPM, or the ISSM in his absence, will alert the Deputy Inspector General (DIG), the Assistant Inspector General (AIG) for Administration and the Deputy Assistant Inspector General for Administration (Deputy AIG for Administration) of the incident. Documented incident reports will follow this same reporting process and will be sent within twenty four (24) hours.

All incidents involving the theft of GSA OIG hardware, software, and/or information in physical form, occurring in GSA Federal facilities, must be reported by the employee to their supervisor and the Special Agent in Charge for their respective regional Office of Investigations. Headquarters personnel should report the theft to the Special Agent in Charge of the Operations Division. The Office of Investigations, as appropriate, will coordinate reporting to the Federal Protective Service, the local police, or other law

enforcement authority with jurisdiction. Similar incidents occurring outside of Federal facilities must first be reported to the local police that has jurisdiction and to JI and their supervisor upon returning to the office. In addition, the incident must be reported to the OIG IT Service Desk. The Director of JPM, or the ISSM in his absence, will alert the DIG, the AIG for Administration and the Deputy AIG for Administration of the incident.

#### 434.03 OIG Rules of Behavior for Accessing Personally Identifiable Information (PII)

OIG staff do not have to obtain any GSA required approvals prior to removal of devices containing PII from GSA facilities (not including hard copy files), nor do they have to obtain any GSA required approvals prior to remotely accessing PII.

OIG staff may remotely access PII only via an OIG approved secure Virtual Private Network (VPN) while using OIG approved electronic media.

OIG employees are reminded to always abide by 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII), when accessing PII remotely or at the workplace.

#### 434.04 Personally Owned Mobile Devices

Personally Owned Mobile Devices (POMD) are not allowed on the OIG network but may access approved Government guest networks (e.g., OIG-Guest and GSA Guest Wi-Fi).

#### 434.05 OIG Password

Passwords for specific accounts used to access OIG-issued applications must contain a minimum of eight (8) characters which include a combination of letters, numbers, and special characters.

OIG user name and password are required for accessing specific OIG applications.

Exceptions to the OIG Password policy are to be submitted to the Director of JPM. The Director will discuss whether to accept or deny the risk for the exception and the duration of the exception with the Deputy AIG for Administration.

#### 434.06 OIG Electronic Messaging and Collaboration Services (EMCS)

The official OIG email system is identified as Electronic Messaging and Collaboration Services (EMCS).

OIG employees use OIG Active Directory accounts to access their EMCS accounts.

All email messages and their attachments older than 60 days are moved and stored in a separate archive repository contained within the EMCS system.

Messages larger than 250 megabytes sent outside the OIG network or 2 gigabytes sent inside the OIG network will be blocked. These messages can be sent using the Large File Transfer (LFT) procedures located in the OIG IT reference manual. The OIG IT reference manual can be found within the IBM Notes Email tab along the left hand side just above the inbox.

An OIG supervisor's request to review a subordinate employee's emails must be routed through the employee's component head, routed through JP and JC for consultation, and can only be approved by the Inspector General (IG) or Deputy Inspector General (DIG). JPM will provide the supervisor access to an OIG employee's emails only after written and/or email approval has been provided.

Employees shall protect email messages sent outside the OIG network using the encryption feature in Lotus Notes per OIG policy 719.00, Transmittal of Sensitive Information via Email.

#### 434.07 International Travel

OIG mobile devices can be configured for International Travel with the exception that JPM issued devices are not authorized to store or process any Secret (S) or Sensitive Compartmented Information (SCI) classified information. OIG employees are to contact the OIG IT Service Desk at least 2 business days prior to travel and then again upon return to work so that the Service Desk may configure the device before departure and then reconfigure the device when back in the United States.

#### 434.08 HSPD-12 Personal Identity Verification (PIV) Cards

GSA OIG personnel are required to use their Personal Identity Verification (PIV) cards to login to all OIG issued personal laptops or desktops, regardless of whether they are in the office or remote.

Handling cases when a PIV card is not available, such as:

- a) A Federal employee on detail to GSA OIG, issued a PIV from the employees assigned Agency
- b) Any employee or contractor expected to be employed for less than 180 days and not issued a PIV
- c) Any person with a disability that does not allow the individual to utilize a PIV card and laptop.
- d) Any user with a PIV that is lost, forgotten at home, or damaged in any way, may contact the OIG IT Service Desk to request a temporary exception to the above requirement, not to exceed forty-five (45) days.

JPM handles the above cases using authenticated, encrypted, temporary tokens. Tokens are configured to meet the forty-five (45) day threshold and are disabled after that time. Once a user has a new or replacement PIV card, or their temporary duty has completed, the token must be returned to JPM. JPM monitors token use throughout the duration that it has been issued.

New Users (includes new contractors, temporary duty, and Federal employee on detail) - when JPM sends the laptop for a new user to pick up on their first day, JPM sends a temporary token separately for that user. JPM notifies the supervisor of the password for the supervisor to distribute to the new user.

Existing Users (includes lost or damaged PIV) – contact the OIG IT Service Desk. JPM configures a temporary token and sends it overnight for the next day. A password is sent to the user's supervisor for initial access.

Because temporary tokens expire in 45 days, a new token must be issued prior to the 45 day window if a PIV card has not been issued by that time. Otherwise, the laptop will be inaccessible. JPM will notify the

user that their token is set to expire in 10 days and for them to contact the IT Service Desk for a new token.

Effective Date 10/1/2015

## 436.00 OIG TELECOMMUNICATIONS POLICY

### 436.01 Purpose

The Office of Inspector General (OIG) follows the latest versions of GSA Guidance, unless specified otherwise in sections 436.02 through 436.07 below. The latest GSA guidance related to the use of telecommunications resources can be found at <https://insite.gsa.gov/portal/directives>. Among the most relevant are:

- CIO G 10000 GSA Telecommunications Guide
- CIO P 2165.2 GSA Telecommunications Policy
- CIO 2104.1A GSA Information Technology (IT) Rules of Behavior.

### 436.02 Telecommunications Support

The OIG IT Division (JPM) is responsible for providing user support for all OIG-provided telecommunications equipment, systems and services used by OIG employees.

Telecommunications equipment includes but is not limited to employee desktop computers and laptops connected to the network, Voice over Internet Protocol (VoIP) desk phones, and cellular phones, smartphones and air cards.

Telecommunications systems include GSA OIG voice and data networks, and private branch exchanges (PBXs) and Unified Communications voice systems (IP PBXs).

Telecommunications services include local and long-distance wireline voice services and telephone calling cards, the data wide-area network (WAN) connecting GSA OIG offices, wireless voice and data services contracted by GSA OIG.

Support for IT equipment, systems and services are provided by the OIG Service Desk.

The OIG IT Service Desk is available by:

- Calling 202-273-7399
- Sending an email to [OIGITServiceDesk@gsaig.gov](mailto:OIGITServiceDesk@gsaig.gov)
- Creating a ticket at <https://oigitservicedesk.gsaig.gov>.

### 436.03 Wireless Device Services

The OIG has contracted for its own wireless services. Mobile devices are issued by JPM at the direction of the organization component head. Requests for mobile devices should be directed to the supervisor.

### 436.04 Waste, Fraud and Abuse

Computer Viruses and Destructive Programs: Employees who receive emails that they suspect contain malicious content should select the "Report SPAM" button on the menu in Lotus Notes which will safely

notify the OIG IT Security team of the suspected email. For computer viruses or program incidents other than email, employees should report it to their supervisor and also to the OIG IT Service Desk.

Annoying and Offensive Communications: Employees who witness abuse of this guideline should report it to their supervisor and also to OIG Service Desk.

#### 436.05 Remote Networks and Printing

When connected to the OIG network using the Virtual Private Network (VPN), split tunneling (connecting to a Local Area Network (LAN) while at the same time connecting to the Internet) and/or multi-homing (simultaneously connecting a device to more than one network) is not allowed and all internet traffic must be routed through the VPN.

Printing from an OIG provided device to a non-OIG managed network is not allowed.

#### 436.06 Personal Devices

Personal devices, such as mobile phones, laptops, home computers, tablets or other devices are not to be used on the OIG private network. This practice of using personally owned mobile devices in the workplace to access government owned systems or applications is referred to as Bring Your Own Device (BYOD). The GSA/OIG does not participate in the GSA BYOD program.

#### 436.07 Lost or Stolen Mobile Devices

For any lost or stolen device, employees are to report these incidents to the OIG Service Desk per OIG policy 434.02 Incident Response Reporting Procedures.

Effective Date 2/21/2017

## 441.00 PROPERTY MANAGEMENT PROGRAM POLICY

### 441.01 Purpose and Scope

This policy sets forth the standards and procedures governing Office of Inspector General's (OIG) requirements for the Property Management Program and the duties and responsibilities of Property Management Officers (PMO), Inventory Administrators (IA), Custodial Officers (CO), and employees.

The OIG follows GSA Order ADM 7800.12, "Management of the U.S. General Services Administration's (GSA) Internal Personal Property," except where the provisions in that Order conflict with OIG policy.

Assets inventoried by the Office of Investigations (OI) are not subject to this policy. OI is responsible for inventorying agent equipment and gear.

### 441.02 Definitions

The following definitions are pertinent to OIG operations:

1. **Accountable Property:** Accountable property includes property owned, leased, or otherwise under Government control costing more than \$1,000, or property deemed sensitive (see definitions of End Item and Sensitive Property below). All accountable property must be recorded in the OIG Property Management System (PMS). Exhibit A displays the types of sensitive property that must be recorded in OIG's PMS. Furniture, appliances, and real property are not considered accountable property under this policy.
2. **Custodial Area:** The physical location of an office or division that is assigned to a Custodial Officer.
3. **Custodial Assigned:** Any equipment not currently assigned to personnel, shared (i.e., copier, shredder, color printer), or assigned to a non-OIG employee.
4. **Physical Inventory:** A physical identification and count of accountable or sensitive property for reconciliation to the PMS.
5. **Sensitive Property:** Sensitive property is accountable property, regardless of cost, that requires control because of sensitivity to loss or theft. Within OIG, most "end item" information technology (IT) is deemed sensitive and therefore accountable property.

### 441.03 Responsibilities

#### 1. Property Management Officer (PMO)

The Assistant Inspector General (AIG) for the Office of Administration shall designate an employee(s) to serve as the PMO for accountable assets assigned to all OIG components. PMO responsibilities shall include:

- Providing leadership and guidance to OIG staff on the proper use, care, and disposal of property.

- Ensuring that inventory records are maintained for each assigned custodial area.
- Approving and archiving items from the system (i.e., excessing, donation, destruction).
- Ensuring that the PMS remains current and accurate.
- Overseeing yearly physical inventory.

## 2.Inventory Administrators (IA)

Generally, inventory administrators shall act as the primary staff responsible for controlling accountable and sensitive property. IA responsibilities include:

- Adding, updating, and maintaining the PMS for accountable and sensitive property. All common, shared, or temporarily unassigned IT equipment in a physical location should be assigned to the Custodial Officer at that location in the PMS.
- Ensuring all assignments, reassignments, disposals and/or retirements of accountable property are recorded in the PMS, with identification to assignee, within 10 business days of assignment, reassignment, disposal, and or retirement. When shipments of new IT equipment are received, these items should be entered into the PMS within 10 business days of receipt, and assigned to the Custodial Officer as Custodial Unassigned while waiting for installation.
- Working closely with the Custodial Officer who will authorize/approve updates as required.

## 3.Custodial Officers

There must be one Custodial Officer per designated physical location, appointed by the Special Agent-in Charge (SAC), Regional Inspector General of Auditing (RIGA), Division Director, or Assistant Inspector General (AIG). Custodial Officer responsibilities include:

- Accounting for all property (assets) assigned to a designated physical location.
- Identifying and properly disposing of items that are no longer necessary within the custodial area.
- Designating secure storage areas for accountable property not issued to prevent theft of OIG property.
- Notifying the PMO of disposal of property and loss of Custodial Assigned property.
- Conducting yearly physical inventory.

## 4.Employees

Upon receipt of accountable or sensitive property, employees shall assume the responsibility for its protection and safekeeping. Employees will have read-only access to their own record. Specific employee responsibilities shall include:

- Confirming/rejecting changes to their inventory. If employees are aware of a change to their assigned property and do not receive a verification request from the PMS within 10 business days of this change, they should contact their Custodial Officer.
- Exercising reasonable and responsible care of all accountable and sensitive property.
- Reviewing and electronically confirming their personal inventory record during the annual inventory and after receiving or surrendering any personal property.
- Informing their Custodial Officer of any changes to assigned property and properly reporting lost, stolen, or damaged property.
- Surrendering all items of issued property to their supervisor prior to their transfer to another OIG location or on their last day of employment.

#### 441.04 Inventory Management

It is OIG's policy that control of all accountable property shall be appropriately documented and maintained in a traceable and orderly manner. To that end, all accountable property must be recorded in OIG's PMS. Designated IAs and Custodial Officers are responsible for ensuring the integrity of the PMS by ensuring that all property received (including new shipments waiting to be configured and deployed), assigned, reassigned, or disposed of is recorded in PMS within 10 business days of the occurrence with appropriate identification of assignee.

A physical inventory of all accountable or sensitive property will be conducted yearly.

#### 441.05 Lost or Stolen Personal Property

Employees may be held liable for lost, stolen, or damaged property if there is evidence of negligence or misconduct. Employees are charged with safeguarding all equipment and sensitive information necessary to perform their duties. However, when a loss, theft, or damage occurs there are reporting requirements that must be strictly followed.

Employees shall report any property loss to his or her supervisor and police if applicable. The employee must immediately report any lost or stolen IT assets, to the OIG IT Service Desk per 434.02 Incident Response Reporting Procedures.

The AIG shall determine whether to institute a Financial Liability Proceeding. See 508.00 Financial Liability for Stolen, Damaged, Lost or Destroyed Government Property for policy and procedures.

#### 441.06 Disposal of Property

Federal Management Regulation §102-36.30 deems property to be excess when it is no longer needed to carry out the functions of official programs within an agency. The CO must request approval for the disposal of all property through the PMO. The process for disposing of property differs depending on the location and the sensitivity of the property.

Effective Date 1/17/2017

## 442.00 RECRUITMENT, RELOCATION AND RETENTION INCENTIVES

### 442.01 Purpose

Recruitment, Relocation and Retention Incentives are a critical component of the OIG's overall mission to attract qualified applicants and/or retain employees with outstanding qualifications for positions in designated employment categories. Incentives may also include creditable service for annual leave accrual for non-Federal work experience and experience in the Uniformed Service.

With the exception of the provisions discussed below, the OIG adopts GSA Order HRM 9575.1, "Recruitment, Relocation and Retention Incentives."

### 442.02 Applicability

The following types of employees are eligible to receive a recruitment, relocation, or retention incentives:

1. General Schedule (GS);
2. Senior Level (SL) or Scientific and Professional (ST);
3. Senior Executive Schedule (SES);
4. Employees in prevailing rate positions (WG, WL, WS); and
5. Any other position in a category for which payment of an incentive has been approved by OPM.

The following types of employees are excluded from receiving recruitment, relocation, or retention incentives:

1. Presidential appointees;
2. Non-career SES; and
3. Those in positions excepted from the competitive service due to its confidential, policy-determining, policy-making, or policy-advocating character.

### 442.03 Legal Authority

The authorities cited for this policy are 5 U.S.C. 5753; 5 U.S.C. 5754; 5 U.S.C. 5514; 5 U.S.C. 5584; 5 CFR Part 575, Subparts A, B, and C; and 5 CFR Part 550, Subpart K.

The Inspector General Act of 1978 as amended ensures that the OIG can provide policies and procedures separate from those of GSA to ensure independence.

#### 442.04 Definitions

##### a. Recommending Official.

The supervisor or manager making the selection is the recommending official.

##### b. Reviewing Official.

The Human Resources Director has managerial responsibility to ensure the OIG's use of recruitment, relocation and retention incentives conform to legal authorities and HRM 9575.1.

##### c. Approving Official.

The Deputy Inspector General is the approving official for all recruitment, relocation and retention incentives.

#### 442.05 Designated Employment Categories

All positions within the OIG are deemed mission critical for purposes of incentives.

#### 442.06 Responsibilities

##### a. Recommending Official

Preparing the written recommendation with appropriate supporting documentation justifying the request for a recruitment, relocation or retention incentive.

##### b. Office of Human Resources

1. Reviews package to ensure the justification and documentation support use of the incentive and the request is in compliance. Consults with requesting organization, as necessary, to request additional information or documentation.
2. Submits package for final approval or disapproval to the Deputy Inspector General.

##### c. Assistant Inspector General for Administration

Coordinates with the Human Resources Director for review and final action to forward to the Deputy Inspector General for approval or disapproval.

#### 442.07 Procedures for Requesting Approval for a Recruitment, Relocation and Retention Incentive

a. The recommending official will prepare the request for a recruitment, relocation or retention incentive and forward it in accordance with the OIG paragraph on "Responsibilities" for concurrences and approval. Applicants or Employees should be advised not to decline other offers of employment or notify current employers of their intent to leave before the request is approved.

Any requests for an incentive that exceeds 25% of an individual's rate of basic pay must be approved by the DIG and referred to OPM for further approval.

b. Notification of approval or disapproval will be sent to the recommending official and to the reviewing official.

c. JPH will:

1. Forward any DIG approved incentive in excess of 25% to the Office of Personnel Management (OPM) for final approval.

2. If the incentive is approved, notify the applicant or employee and ensure that the applicant or employee signs a service agreement before entry on duty, assignments to or retention in the position.

3. Process the Request for Personnel Action (SF-52) for the appointment, and maintain all supporting documents.

#### 442.08 Documentation and Recordkeeping

The records and documentation will be maintained for a minimum of 2 years by JPH.

Effective Date 12/13/2017

## 443.00 IT SOFTWARE LICENSE MANAGEMENT POLICY

### 443.01 Purpose

The purpose of software license management is to manage, control, and protect software assets. Proper management of license policy minimizes noncompliance, ensures controlled expenses, and reduces the possibility of duplicate licenses.

### 443.02 Scope and Applicability

CIO 2108 GSA Software License Management applies to all OIG employees and contractors except when in conflict with OIG policy. An exception to the below policy requirements is granted to JI personnel responsible for administering Digital Crime Forensic Unit and Technical program assets, which are not administered or serviced by JPM.

### 443.03 Policy

Specific IT software management policies for the OIG IT are as follows:

- Only OIG IT personnel have administrative rights to install software on OIG IT assets.
- Requests for any and all software for use on OIG IT assets (workstations, laptops, or mobile devices) are to be made via the OIG IT Service Desk.
- Software that has been approved for use can be found in the Configuration Items List in the Appendix.
- For requests of software not listed in the Configuration Items (CI) List, the user is required to submit a Procurement Request (PR) with justification specifying how the software is to be used.
- Software license information is to be entered by JPM into the OIG Software License Management Repository, which is integrated into OIG's IT Service Management (ITSM) system.

### 443.04 References

For the process on how to initiate a software license request, see OIG Information Technology (IT) Service Desk Standard Operating Procedures 435.02

Appendix: Configuration Items (CI) List

Effective Date 2/6/2017

## 444.00 OIG INFORMATION TECHNOLOGY (IT) INTEGRATION POLICY

### 444.01 Purpose

To set forth policy for integrating key IT principles when planning and managing IT solutions developed for, or operated by, GSA OIG. This policy has been developed to assure that solutions are compliant with GSA OIG IT standards. These standards are addressed as early as possible during project and acquisition planning activities. GSA OIG IT is engaged throughout the project lifecycle.

### 444.02 Applicability

The GSA CIO 2102.1 Information Technology (IT) Integration Policy applies to all internal GSA IT projects.

This policy applies to the Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act and that it does not conflict with other OIG policies or the OIG mission.

GSA OIG does not use the GSA IT Vendor Management Office (VMO), GSA IT Service Portfolios or the GSA Business Capability Portfolios for the acquisition or management of GSA OIG IT services.

The GSA OIG Information Technology Division (JPM) provides either directly or indirectly, all hardware, software, network and telecommunications services to the OIG. As such, at JPM's recommendation, the OIG may utilize some GSA-hosted applications or network services (e.g. Pegasys) but is not required to use all GSA IT services (e.g. GSA OIG does not use GSA's Customer Relationship Management (CRM) technology). JPM is responsible for all GSA OIG Enterprise Document Management, Enterprise Solutions, Enterprise Information and Data Management, Digital Services, and Records Management.

### 444.03 Scope

This policy applies to acquisition, planning, development, maintenance, enhancement, operation and disposal of IT systems and solutions of any size, complexity, or significance that should be considered part of GSA OIG's IT portfolio. This policy applies to all GSA OIG IT project managers, system owners, and other staff responsible for defining, delivering, operating, supporting, and retiring IT systems and solutions. This policy does not apply to IT assets acquired and maintained by personnel administering JI's Digital Crimes and Forensics Unit.

### 444.04 Policy

#### a. General Guidelines

1. The policy applies to any new, internal GSA OIG IT solution, in all of its life cycle phases.
2. This policy applies to any major enhancement effort related to an existing project that meets any of the following criteria:
  - All IT efforts, excluding license renewals, production support activities, and basic operational activities.

- Any cloud acquisition, regardless of dollar value.
- Any proposed Blanket Purchase Agreement for IT products or services, regardless of dollar value.
- Requests for Information (RFI) and other market research initiatives related to IT initiatives regardless of dollar value.
- Strategic or high-priority IT acquisitions

3. All solution development, modernization, and enhancement efforts are to ensure compliance with the Key IT Principles. Failure to follow this policy may result in unacceptable deviations from planned cost, schedule, and performance expectations, and could ultimately result in project termination.

4. The policy requires integration of compliance-based processes and controls specific to the Key IT Principles identified above, appropriately scoped to ensure effective management control and authority over IT projects.

b. Key IT Principles. The following information identifies the five Key IT Principles that must be addressed for all new and existing IT projects.

1. Single Sign-On. JPM will manage the Single Sign-On strategy and associated solution options available within GSA OIG.

2. Cloud First. The Cloud First policy mandates that agencies consider cloud options first before making any systems or network changes in order to take full advantage of cloud computing benefits to maximize capacity utilization, improve IT flexibility and responsiveness, and to minimize cost. This does not require cloud solutions but does require cloud considerations.

3. Open Source Software (OSS). OMB M-16-21 strongly encourages the development and procurement of open source software. GSA OIG will make its source code publicly available, under licenses that allow use, copying, modification, and redistribution, when not in conflict with the GSA OIG mission.

4. Records Management. Federal law requires all Federal agencies to create and preserve records that adequately and properly document "the organization, functions, policies, decisions, procedures, and essential transactions of the agency" (44 U.S.C. 3101). Create and preserve records documenting the organization, functions, policies, decisions, procedures, and transactions of GSA OIG; also, records necessary to protect the legal and financial rights of the Government and of persons affected by GSA OIG's activities (44 U.S.C. 3101). By December 31, 2019, all permanent electronic records in Federal agencies will be managed electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format. Agencies should also consider the benefits of digitizing permanent records created in hard-copy format or other analog formats (e.g., microfiche, microfilm, analog video, analog audio).

5. IT Security Engagement. The GSA OIG IT Security team is the authority responsible for ensuring OIG IT solutions are compliant with federal, GSA and OIG security standards.

Effective Date 3/21/2017

## 445.00 IT CONFIGURATION MANAGEMENT

### 445.01 Purpose

The Federal Information Security Act of 2002 (FISMA), the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-128, Guidelines for Security Configuration Management of Information Systems, and NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations, provide guidelines for IT Configuration Management.

This Procedures document establishes the conditions for Configuration Items (CI's) and information system baselines. The primary purpose of Configuration Management (CM) is to ensure that CI's and information systems perform as intended. Proper CM adherence also documents a level of detail sufficient to repeatedly produce the CI and information system to meet the needs for operation, quality management, maintenance, repair, replacement, and disposal. CM is an important component for providing reliable and secure network services. CM requires complete and accurate documentation of the enterprise network infrastructure. Any change or addition made to CI's or to the information system is considered to be a risk to its continued successful operation.

### 445.02 Scope

These procedures apply to any alteration to the operational environment of the OIG General Support System (GSS) managed by the GSA OIG Information Technology Division (JPM). These procedures also apply to all CIs and Information Systems that are a part of the GSS as defined by the OIG Configuration Management Plan (CMP). This includes network communications, applications, hardware, software, firmware, and configuration settings key to operating, supporting and maintaining the OIG GSS and other services.

### 445.03 Objectives

The main CM objectives:

- 1) Identify and document CI baseline;
- 2) Minimize the adverse impact of necessary changes on system confidentiality, availability, integrity, and service level;
- 3) Allow the control and identification of CI's and information systems in order to provide a stable production environment; and
- 4) Maximize the productivity of the people involved in the planning, coordination and implementation of configuration management database.

#### 445.04 Roles and Responsibilities

- a. Authorizing Official (AO). The AO or designee is responsible for operating the information system at an acceptable level of risk to organizational operations including mission, functions, image, reputation, and organizational assets. The IG has designated the Director, Information Technology as the AO.
- b. Configuration Manager. Develops and maintains plan, policies, CI list, and procedures; conducts configuration audits to ensure the CM activities are properly performed; administers Request for Change (RFC) notifications; and closes change request tickets. The Configuration Manager is a member of the OIG IT Division (JPM).
- c. Information System Security Officer (ISSO). Ensures implementation of system-level security controls and maintains system documentation. The ISSO will participate in the configuration management process to provide security impact analyses for the technical staff. The ISSO is a member of the OIG IT Division (JPM).
- d. System Manager. Identifies and implements approved baseline configurations, and assists with configuration monitoring activities. In addition, technical staff will be included in the process for determining the appropriate baseline for each CI. The System Manager is also responsible for ensuring that CI's and information system baselines comply with the CM process and provide complete and accurate information to the CM in a timely manner. The System Manager is a member of the OIG IT Division (JPM).
- e. Change Control Board (CCB). The Change Control Board will monitor approved changes and conduct implementation to ensure that the actions performed result in successful and continued operation of the OIG GSS. Change Control Board members are defined in OIG 439.00 Change Control Board (CCB) Guide.

#### 445.05 Configuration Management Process

The first step of the CMP requires system managers to establish the CI and Information System baselines – a snapshot of the current design settings and functionality of the CI's – and to provide details regarding all hardware and software. The baseline includes identification of servers, workstations, and software applications currently being used in the production environment and the specific configuration settings for each. This table outlines the process.

##### Configuration Management Process

##### Identify CI's

Configuration items include:

- Devices
- Software
- Operating Systems
- Applications

Identify System Manager A System Manager can be the administrator of major application, database, SharePoint, and Domain servers in addition to overseeing Government off-the-shelf (GOTS) or Commercial off-the-shelf (COTS) application developers.

Identify CI Baseline System Managers will identify and document CI baseline.  
Security Team Evaluates the baseline and provides issue or risk potential to the System Managers.  
System Managers Remediate, mitigate, or prepare a risk acceptance for the AO.  
AO Reviews the risk acceptance then approves or denies.  
CI Baseline New system baseline, which is a snapshot of the current design settings.  
CI Change Deviation of the established baseline is processed through the Change Control process.

#### 445.06 Request a Change

Any change to the CI baseline will adhere to OIG 439.00 Change Control Board (CCB) Guide. The purpose of a request is to provide complete documentation of the change, which includes:

- Justification for approval
- Impact risk assessment and mitigation strategy
- The implementation plan
- Results of the change

#### 445.07 Configuration Audits

Configuration verification and regular audits verify the proper application of the established baseline. Audits will be conducted by the Security Team to ensure continued compliance. Any non-compliance of an established baseline will be forwarded to the Authorizing Official and System manager for remediation.

Effective Date 11/16/2017

## 446.00 OIG SHAREPOINT GOVERNANCE POLICY

### 446.01 Purpose

This policy identifies the acceptable use for Microsoft SharePoint on the GSA OIG SharePoint platform. This policy in its entirety achieves the following:

- Ensures compliance of individuals and organizations with the rules and responsibilities regarding the use of SharePoint.
- Establishes acceptable uses of SharePoint.

### 446.02 Applicability

This policy applies to all GSA OIG authorized users, which include employees, contractors or other third parties who: (1) process or handle any OIG-owned information, data or Information Technology (IT) equipment; or (2) access OIG IT systems to conduct business on behalf of, or with, the OIG.

There are three different levels of SharePoint expertise:

1. Casual User with limited IT expertise. The casual user views information or inputs and removes information from SharePoint, but generally does not change what a site looks like.
2. Standard Developer uses the existing "out-of-the-box" features that SharePoint has available for everyone.
3. Custom Developer uses advanced workflow development features. This level of SharePoint access requires training, certification and the additional installation of SharePoint Designer 2013 software.

This policy applies to all three levels of experience but is comprehensive enough to define the requirements for the highest level of user expertise.

### 446.03 Scope

This policy applies to any technologies or resources that are attached to the OIG SharePoint platform.

### 446.04 Definitions

- Intranet – the enterprise-wide, organizational home page for all employees of the OIG. Information, data, and documents shared on the intranet are generally viewable by all OIG employees.
- SharePoint – a Microsoft web-based platform that integrates with Microsoft Office products. The OIG's Intranet is architected using SharePoint. This empowers individuals, teams, and component organizations to collaborate and share content throughout the OIG.
- Site – a single page, list, library, or form.
- Site collection – a collection of sites and subsites that group and organize information, data, and content.
- Team site – a SharePoint site collection established for OIG components and sub-components with user access controls for increased security. Team sites for OIG components enable secured document collaboration within that organization.

- Personally Identifiable Information (PII) data - as defined in OMB Memorandum M-07-16, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Examples include, but are not limited to social security number, date and place of birth, mother's maiden name, and medical history.
- Classified data – Information that requires protection of confidentiality, integrity, or availability. Access is restricted by law or regulation to particular groups of people, and mishandling can incur criminal penalties.
- Browser – a program with a graphical user interface for viewing websites on the Internet (e.g. MS Internet Explorer, Firefox, Google Chrome, Safari).

#### 446.05 Roles

- Users – all OIG employees, contractors, and anyone with access to the OIG SharePoint are users. SharePoint users have read-only access to the resources and content on the SharePoint Intranet. Users do not have access to Team sites unless access is explicitly granted.
- Site Owners – SharePoint users with ownership of one or more SharePoint site or site collection.
- Approvers – SharePoint users with content approval duties and responsibilities on SharePoint site or site collections with content approval workflows enabled.
- Contributors and Designers – SharePoint users with the ability to create, edit, and upload content to SharePoint.
- The OIG IT Division (JPM) administers, maintains, develops and provides consultation services for SharePoint best practices and use.

#### 446.06 Content

- Images – Images are best stored as PNG or GIF formats and in the images folder at the site level.
- Documents – Microsoft Office documents, PDFs, files, and other content can be organized and storage in SharePoint Document Libraries.
- Lists – Structured data can be stored in SharePoint lists, allowing item creation, editing, and removal. In a list, data is gathered in rows, and each row is known as a list item.
- Web pages – SharePoint supports the creation of web pages within sites and site collections. Web pages can host static text, images, and other document types using SharePoint web apps.

#### 446.07 Policy

- The SharePoint Intranet and Team sites are government resources and shall be used for official use only.
- SharePoint users are prohibited from creating, uploading, and sharing imagery, text, documents, or any other inappropriate content that may be offensive, indecent or obscene or which may be used to harass, threaten, or abuse others.
- Users shall not attempt to access any files, documents, or content for which they do not have the authorization to access.
- Personally Identifiable Information (PII) and Classified Data

- The SharePoint Intranet is prohibited from use as a platform to share, store, or distribute content containing classified data.
- Personally Identifiable Information (PII) is permissible on SharePoint but the following security requirements apply to the protection of PII:
  - ☑OIG 434.03 OIG Rules of Behavior for Accessing Personally Identifiable Information (PII) must be followed.
  - ☑If it is a business requirement to store PII on SharePoint, PII must be encrypted using a FIPS 140-2 certified encryption module. (SecureZip is provided on all JPM issued laptops).
  - ☑PII shall be stored on SharePoint with proper access controls and shall be made available only to those individuals with a valid need to know. The SharePoint site owner will control access to the site containing PII.
- SharePoint site owners, and contributors, (which include users with access to create, upload, edit and approve content) have a duty to review content within their SharePoint sites for the existence of PII or classified data.
- SharePoint users shall report incidents of PII or classified data stored on SharePoint per the procedures defined in OIG 434.02 Incident Response Reporting Procedures.

- Customization

- All web pages in top site collections, sites, and subsites shall inherit the standardized template and theme applied throughout OIG Intranet. Content areas within web pages that do not interfere with the standardized template can be customized as needed.

- Moderation

- SharePoint site owners, approvers, designers, and contributors are expected to self-moderate the content uploaded and shared on SharePoint for which they have editorial control.
- JPM will restrict or modify access rights in those instances where SharePoint and/or IT security policies are not enforced through self-moderation.

- Workflow Development

- Standardized workflow development using existing (out-of-the-box) features is available to everyone in SharePoint without requiring any additional software.
- Custom workflow development requires the installation of the SharePoint Designer 2013 software. Requests for SharePoint Designer 2013 are made to the OIG IT Service Desk. When making the request, the SharePoint contributor will need to have:

- ☑Approval from their immediate supervisor to be attached to the request ticket.
- ☑SharePoint Designer Certification. First-time requestors of SharePoint Designer 2013 must attach the certifications for completing the following courses found in GSA On Line University (GSA OLU):
  - ☑Microsoft SharePoint Server 2013 - Developing Core Solutions: Business Processes
  - ☑Navigating, Lists, Libraries, Alerts, and Document Sets in SharePoint 2013

- Lifecycle and retirement

◦JPM will conduct reviews of the SharePoint site and subsites to identify seldom used sites for removal to restore valuable storage space. JPM will notify site owners when their site is slated for removal and granted 30 calendar days to respond to the removal intent.

- Technical Restrictions

- File Size Limit - Due to resource limitations and general performance requirements, each file, document, or other content uploaded to SharePoint is limited to 50Mb in size. There are no exceptions to this policy.

- Browser – SharePoint use is restricted to the Microsoft Internet Explorer and Microsoft Edge browsers. Use of third party Web Browsers is not supported.

- Scripting – JavaScript and other web-based scripting libraries are prohibited.

- JPM Responsibilities for SharePoint

- Administration – JPM is responsible for high-level administration of site ownership, and SharePoint system performance and upkeep. JPM can smoothly transition ownership of a site from one person to another.

- Maintenance – JPM manages the SharePoint servers and resources. JPM will perform periodic maintenance of the SharePoint servers which may result in short, (and in some rare circumstances, extended) downtime of the SharePoint Intranet and Team sites. When possible, JPM will perform maintenance outside of core business hours of operation.

- Development

- ▣JPM will provide complex development services that are beyond standardized SharePoint features.

- ▣Requests for JPM Development support are made via the JPM Software Development Request Form found on the Information Technology (JPM) Intranet site page, with the icon under the JPM System Resources section.

- ▣All project requests require the approval of a Special Agent-in Charge (SAC), Regional Inspector General of Auditing (RIGA), Division Director, or Assistant Inspector General (AIG) to initiate a project. This approval can be attached to the JPM Software Development Request Form.

- ▣Development projects are prioritized based on agency needs. Requests for development should allow for reasonable project planning and project development time necessary to support the request.

- Consultation Services – JPM offers recommendations and provides advice to site owners on a variety of SharePoint topics such as site governance, change management, workflows, and approval structures. This is performed on an ad-hoc basis while working with site owners in the course of supporting and maintaining the SharePoint environment.

- Backup – JPM performs daily and weekly backups of SharePoint. Backups are maintained in accordance with the OIG 407.00 Records Management Policy.

#### 446.08 References

Applicable policies include:

- 434.00 OIG INFORMATION TECHNOLOGY (IT) SECURITY POLICY
- 420.00 OIG POLICY ON COLLABORATIVE RESOURCES AND SOCIAL MEDIA
- 407.00 OIG RECORDS MANAGEMENT, INCLUDING HANDLING ELECTRONIC RECORDS
- 2104.1A CIO CHGE 1 GSA Information Technology (IT) General Rules of Behavior
- 2180.1 CIO P GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
- 2100.1K CIO GSA Information Technology (IT) Security Policy



## CHAPTER 500 - ETHICAL CONDUCT AND RESPONSIBILITIES

This Chapter sets forth the responsibilities and standards of ethical conduct expected of OIG employees. By virtue of the unique position and charter of the OIG, and the need for credibility and discretion in handling sensitive issues and information, OIG employees are expected to conduct themselves in accordance with the standards and guidelines that govern the ethical behavior of GSA employees.

### 501.00 STANDARDS OF ETHICAL CONDUCT

501.01 Role of the Office of Counsel in Implementing Ethics Standards

501.02 Ethics Training

501.03 Ethics Notices to New Employees and New Supervisors

### 502.00 USE OF AGENCY OFFICE EQUIPMENT

### 503.00 OUTSIDE EMPLOYMENT

### 504.00 REPORTING FINANCIAL INTERESTS

### 505.00 MANAGING PRIVILEGED AND SENSITIVE INFORMATION

### 506.00 OBLIGATIONS OF PERSONNEL APPOINTED AS AGENTS OF A GRAND JURY

### 507.00 ATTENDANCE AT MEETINGS AND CONFERENCES OUTSIDE GSA

### 508.00 FINANCIAL LIABILITY FOR STOLEN, DAMAGED, LOST OR DESTROYED GOVERNMENT PROPERTY

508.01 Assistant Inspector General (AIG) or Component Head Determination to Proceed

508.02 Financial Liability Proceeding

Effective Date 5/3/2017

## 501.00 STANDARDS OF ETHICAL CONDUCT

Two sets of ethics standards apply to GSA employees. The first set, the Standards of Ethical Conduct for Employees of the Executive Branch, can be found at 5 C.F.R. Part 2635 (also available at <https://insite.gsa.gov/portal/content/502440>). The standards apply to all employees of the Executive Branch of the Federal Government. The standards discuss gifts from outside sources, gifts between employees, conflicting financial interests, impartiality in performing official duties, seeking other employment, misuse of position and outside activities.

The second set of standards, the Supplemental Standards of Ethical Conduct for Employees of the General Services Administration, is a supplement to the government-wide standards which are described above. These standards apply only to GSA employees to include OIG personnel and are codified at 5 C.F.R. Part 6701.).

The GSA supplemental regulations generally prohibit (1) solicited sales to subordinates by GSA employees; (2) the purchase of real and personal property sold by GSA; (3) the purchase of real estate by certain GSA employees; and (4) the taking and disposal of government property. The supplemental regulations also requires employees to obtain approval before engaging in certain outside employment, and identifies appropriate officials to whom waste, fraud, abuse and corruption are to be reported.

### 501.01 Role of the Office of Counsel in Implementing Ethics Standards

The Office of Counsel to the IG is responsible for providing advice and assistance to OIG employees on all questions regarding the application and intent of the GSA and government-wide standards of conduct. The advice may be provided either in writing or orally. In addition, the office is responsible for providing annual ethics training, reviewing financial disclosure reports and as necessary reviewing outside employment requests. However, the OIG Office of Counsel cannot independently provide controlling ethics advice pursuant to 5 CFR § 2635.107(b), make determinations concerning whether an event attended by an employee constitutes a widely attended gathering for purposes of an exception to the gift rules under 5 CFR § 2635.204(g), or handle SES ethics matters.

### 501.02 Ethics Training

The Office of Counsel to the IG implements the Office of Government Ethics (OGE) training regulation at 5 C.F.R. Part 2638, Subpart G, which requires agencies to provide a minimum of one hour of ethics training annually to all covered employees. Because of the particularly sensitive role played by each OIG employee, the Inspector General has determined that all employees will receive annual training. The training program provides for one-hour of on-line training. The training presents a summary of the ethics standards along with the conflict of interest statutes and any recent ethics regulations, and discussion of examples of ethics questions from employees. Except for on-line training, a form which indicates that employees received the annual training must be executed by each employee and kept on file.

### 501.03 Ethics Notices to New Employees and New Supervisors

Pursuant to the Office of Government Ethics (OGE) final rule amending the regulations at 5 C.F.R. Part 2638, JPH will ensure that all written offers of employment include notices of the ethical obligations associated with the position and that required ethics notices are provided to all new supervisors.

Effective Date 5/3/2017

#### 502.00 USE OF AGENCY OFFICE EQUIPMENT

Pursuant to a GSA Order, ADM 7800.11, (link made) GSA employees are authorized to use agency office equipment for personal use under certain conditions. Specifically, an employee can use office equipment on an occasional basis if the use involves minimal additional expense to the Government (for example, small amounts of paper) and does not interfere with official business. The personal use of agency equipment should occur during personal time and not during official time. An employee who exceeds the limits for personal use of agency equipment as set out in the Order may violate the government-wide standard of conduct relating to misuse of position. Employees should also understand that, notwithstanding the policy allowing some personal use of office equipment, there is no expectation of privacy with regard to any electronic message sent through Government-provided messaging services.

Effective Date 5/3/2017

#### 503.00 OUTSIDE EMPLOYMENT

The guidelines for outside employment are set out in 5 C.F.R. § 6701.106 of the GSA supplemental standards. Generally, that standard requires a GSA employee to obtain written approval from his immediate supervisor prior to engaging in outside employment, with or without compensation, with a prohibited source.

Effective Date 5/3/2017

#### 504.00 REPORTING FINANCIAL INTERESTS

The Office of Counsel to the IG is responsible for disseminating and reviewing OGE Form 450, Executive Branch Confidential Financial Disclosure Report. The report requires filers to disclose particular assets and income, liabilities, outside positions, agreements and arrangements, and gifts and travel reimbursements. The purpose of the report is to assist employees and their agencies in avoiding conflicts between duties and private financial interests or affiliations. The OIG has designated as filers all OIG auditors, investigators, attorneys, and contracting warrant officers, as well as all other OIG employees in grades 13 through 15. The report is reviewed by an employee's supervisor and a Deputy Standards of Conduct Counselor.

Effective Date 5/3/2017

## 505.00 MANAGING PRIVILEGED AND SENSITIVE INFORMATION

OIG employees have access to privileged or sensitive information not generally available to other GSA employees or the public. OIG employees must therefore exercise extreme care in the use and handling of information to prevent its unauthorized disclosure.

Government-wide requirements in this area include the following:

- Employees are not permitted to disclose confidential, privileged, or sensitive information to unauthorized persons, or make copies of any part of an official file for other than official purposes.
- Information obtained during the course of business because of the employee's position, is official information and is not a possession of the employee.

Specialized requirements relating to the OIG's handling of privileged and sensitive information include the following:

- Much of the information processed within the OIG is maintained in a Privacy Act system of records; contains proprietary information; or requires protection or special handling in accordance with:

- the Right to Financial Privacy Act;
- the Federal Rules of Criminal Procedure;
- the Federal Acquisition Regulation; or
- the Trade Secrets Act (18 U.S.C. § 1905).

- The Comptroller General's standards contained in the "Government Auditing Standards," address the issue of privileged and confidential information and the auditor's responsibility to disclose "certain operating information on a need-to-know basis only to persons authorized by law or regulation to receive it."

- The protection and professional handling of information by investigators -- including the concept of "need-to-know" in all aspects of operations -- is generally addressed in: (1) the position classification standards for GS-1811 investigators; (2) the Freedom of Information Act, which exempts certain investigation matters from disclosure; and (3) the Privacy Act, which ensure the protection of information relating to certain individuals.

OIG employees are expected to exercise due professional care and apply the following guidelines to prevent the compromise of OIG/Agency information:

- Discussions involving ongoing jobs or information obtained as the result of the employee's position with the OIG are limited to management officials and OIG employees who have a need to know.
- Existing procedures for the dissemination and release of information are followed. For example: (1) RIGAs/SACs and AIGs are, within certain limits, authorized to issue reports and generate correspondence; (2) Privacy Act and Freedom of Information Act requests must be processed through JC

and in accordance with applicable laws and regulations; and (3) budget and other information furnished to the Congress often requires coordination and special handling.

- Certain sensitive information may be best disclosed by OIG supervisory personnel.
- The utmost tact and discretion must be exercised in dealing with Agency employees and the public.
- If in doubt, guidance is obtained from the OIG supervisor before disclosure or dissemination of information received as a result of an employee's position with the OIG, or through the conduct of OIG business.

Effective Date 5/3/2017

506.00 OBLIGATIONS OF PERSONNEL APPOINTED AS AGENTS OF A GRAND JURY

The policies and procedures for grand jury information are contained in Section 910 of this manual.

Effective Date 5/3/2017

#### 507.00 ATTENDANCE AT MEETINGS AND CONFERENCES OUTSIDE GSA

Approval by the responsible office head is required for a member of the OIG to represent GSA or the OIG as a speaker or participant in activities outside GSA. Also, such participation in outside events by OIG personnel acting as representatives of GSA or the OIG is reported to the IG, through channels, as a matter of information.

Numerous laws, regulations, and executive orders apply to the participation of Federal employees in outside activities and events. Generally, Federal employees are prohibited from receiving, accepting, or obtaining any honorarium, fee, supplemental salary, compensation, or item of value from private sources for speeches given, articles written, and participation provided as a result of their OIG employment. OIG employees participating in or attending meetings and conferences outside of GSA should consult with JC regarding any activity that may result in the employee receiving any remuneration or item of value, or participating in an activity that may result in any real or apparent conflict of interest.

Effective Date 5/3/2017

## 508.00 FINANCIAL LIABILITY FOR STOLEN, DAMAGED, LOST OR DESTROYED GOVERNMENT PROPERTY

This policy applies to all government property issued to OIG employees. This policy supplements GSA's policy on managing internal government property, ADM 7800.12 and personal use of agency office equipment, ADM 7800.11A. Government property includes but is not limited to government issued laptops, phones, iPhones, tablets, firearms, body armor, vehicles and radios. The following sets forth procedures the OIG will follow to determine whether an employee should be held financially responsible for government property that is stolen, damaged, lost or destroyed as a result of the employee's negligence, improper use, or willful actions.

### 508.01 Assistant Inspector General (AIG) or Component Head Determination to Proceed

Before an OIG employee is held financially liable for stolen, damaged, lost or destroyed GSA property, the employee shall be afforded due process through a proceeding that permits facts to be gathered and provides the employee an opportunity to reply. Accordingly, the relevant AIG or component head shall first consider whether to institute a proceeding to determine if an employee should be held financially liable for stolen, damaged, lost or destroyed property. Factors that may be considered include but are not limited to:

1. The current financial value of the property, if it is possible to determine, and the replacement value of the property;
2. The intrinsic value of the equipment, if any (e.g. if the equipment contained sensitive or confidential information); and
3. The apparent cause of the damage or loss.

### 508.02 Financial Liability Proceeding

Where the AIG or component head believes a proceeding should be initiated, he or she shall consult with the Deputy Inspector General. If it is determined that a proceeding should occur, the AIG or component head shall appoint an "investigating authority" to conduct an investigation into the matter. The investigating authority may be anyone. The AIG or component head may also appoint a "deciding official," the person responsible for making the final determination on whether the employee should be held financially liable for the government property, or choose to serve in that role themselves.

The following procedures must be followed:

- a. The investigating authority will gather relevant evidence regarding the government property that is stolen, lost, damaged, or destroyed and will record, in writing, the information gathered during the investigation, including summaries of any interviews. As part of the investigation, the investigating authority will provide the employee an opportunity to make a statement or present any relevant evidence.
- b. The investigating authority will provide a written report of the results of his or her investigation to the AIG or the component head who requested the investigation and the deciding official, if applicable.
- c. The deciding official shall review the information compiled by the investigating authority to determine whether the government property was stolen, lost, damaged or destroyed as a result of the employee's

negligence, improper use, or willful actions; the extent of the loss to the government; and, as appropriate, the amount for which the employee should be held financially liable.

d. The base amount of liability is the replacement value of the property. The deciding official should consider the following in determining if the employee's financial liability should be modified. This list is not exclusive. The deciding official may consider other factors as well, including the following.

i. Any evidence presented by the employee that demonstrates that the employee is unable to pay the replacement value of the property.

ii. Any evidence that demonstrates that the replacement value of the property is not an appropriate measure of liability.

iii. If the government property was stolen, lost, damaged, or destroyed as the result of multiple employees' negligence, improper use, or willful actions, the deciding official shall determine what percentage of the total liability each employee is responsible for and apportion the damages accordingly.

e. If the deciding official concludes the employee should be held financially liable, the deciding official will provide the employee with an initial decision and 15 business days to provide written comments on that decision. All information or evidence considered by the deciding official must be disclosed and/or provided to the employee at the time the initial decision is issued to allow the employee a reasonable time to respond to that evidence.

f. Upon the expiration of the 15 days or the receipt of the employee's written comments, the deciding official will review the evidence, including any additional statement or evidence presented by the employee, and issue a written final decision to the employee.

g. The deciding official shall provide a copy of the entire written record (i.e. the investigating authority's report, initial decision, employee comments, final decision and all other documents considered) to JPH for retention purposes.

h. If the deciding official determines that the employee should be held financially liable for the stolen, damaged, lost or destroyed government property, they shall also forward a copy of the final decision to JP so that management can initiate the process to recover the funds from the employee.

CHAPTER 600 - RELATIONSHIPS WITH EXTERNAL ORGANIZATIONS

601.00 SEEKING REPRESENTATION FROM THE DEPARTMENT OF JUSTICE

602.00 RESERVED

603.00 OIG LIAISON WITH THE OFFICE OF THE SPECIAL COUNSEL

603.01 Responsibilities of the Office of the Special Counsel

603.02 OIG Liaison with the Office of the Special Counsel

604.00 CONGRESSIONAL CONTACTS, MEDIA CONTACTS AND PRESS RELEASES

604.01 Congressional Contacts

604.02 Media Contacts, Web Postings, and Press Releases

605.00 OIG LIAISON WITH THE CIVILIAN BOARD OF CONTRACT APPEALS (CBCA)

605.01 Responsibilities of the Civilian Board of Contract Appeals (CBCA)

605.02 OIG Liaison with the Civilian Board of Contract Appeals (CBCA)

606.00 OIG LIAISON WITH THE OFFICE OF CONGRESSIONAL AND INTERGOVERNMENTAL AFFAIRS

607.00 OIG RELATIONSHIPS WITH GSA OFFICIALS

608.00 OIG RECOGNITION PROGRAM FOR GSA EMPLOYEES

608.01 Eligibility

608.02 Recognition Process

608.03 Recognition

Effective Date 11/22/2016

601.00 SEEKING REPRESENTATION FROM THE DEPARTMENT OF JUSTICE (DOJ)

Federal employees, including former federal officials and employees, may receive representation in civil, criminal and Congressional proceedings in which they are sued, subpoenaed, or charged in their individual capacity pursuant to regulations established by the Attorney General. 28 CFR §50.15.

When an OIG employee believes he is entitled to representation by the Department of Justice in a proceeding covered by 28 CFR §50.15, he must submit forthwith a written request for the representation, including all process and pleadings served upon him, to the Counsel to the Inspector General and the employee's immediate supervisor. The procedures for requesting such representation are found at 28 CFR §50.15. The Counsel will assign the request to an appropriate JC attorney, who along with any other OIG attorney designated as reviewer shall undertake a full and traditional attorney-client relationship with the employee with respect to application of the attorney-client privilege. With DIG concurrence, the Counsel in accordance with 28 CFR §50.15 shall submit in a timely manner to DOJ a statement containing the findings as to whether the employee was acting with the scope of his employment and a recommendation for or against providing representation. Where there is any conflict, the provisions of 28 CFR Part 50 control.

Effective Date 11/22/2016

## 603.00 OIG LIAISON WITH THE OFFICE OF THE SPECIAL COUNSEL

### 603.01 Responsibilities of the Office of the Special Counsel

The Office of Special Counsel is an independent Federal investigative and prosecutorial agency. Its primary mission involves safeguarding the merit system by protecting Federal employees and applicants from prohibited personnel practices, especially reprisal for whistleblowing. In addition, the Office of Special Counsel enforces and provides advisory opinions regarding the Hatch Act, and the Office of Special Counsel protects the rights of Federal employee military veterans and reservists under the Uniformed Services Employment and Reemployment Rights Act of 1994.

The Office of Special Counsel, in addition to the Office of Inspector General, serves as a safe and secure channel for Federal workers who wish to disclose wrongdoing. The Office of Special Counsel reviews five types of disclosures: 1) a violation of law, rule, or regulation; 2) gross mismanagement; 3) a gross waste of funds; 4) an abuse of authority; or 5) a substantial and specific danger to public health or safety. The Office of Special Counsel will, under most circumstances, guarantee the whistleblower's confidentiality. Information about the Office of Special Counsel and the whistleblower complaint process can be obtained at the public GSA OIG webpage, under Whistleblower Protection.

### 603.02 OIG Liaison with the Office of the Special Counsel

The AIGI acts as the OIG liaison with the Office of Special Counsel concerning allegations of prohibited personnel practices, unless the allegation involves alleged wrongdoing by an OIG employee, in which case the Counsel to the Inspector General acts as the OIG liaison with the Office of Special Counsel.

Except as noted above, the AIGI coordinates matters reported to the Office of Special Counsel concerning allegations of prohibited personnel practices. The AIGI ensures that the IG receives prior notification of all such matters referred to the Office of Special Counsel. After such notification, the AIGI contacts the Office of Special Counsel as circumstances dictate.

Effective Date 11/22/2016

## 604.00 CONGRESSIONAL CONTACTS, MEDIA CONTACTS AND PRESS RELEASES

The policies and procedures to be followed in responding to congressional and media inquiries and in processing press releases are designed to ensure timely notification to the IG and maximum coordination with Agency public information specialists on media issues.

### 604.01 Congressional Contacts

The policies and procedures governing OIG responses to congressional inquiries are set forth in Subchapter 713 of this Manual. Procedures for handling requests for information from the GSA Office of Congressional and Intergovernmental Affairs are set forth in Section 606.00.

### 604.02 Media Contacts, Web Postings, and Press Releases

The Inspector General as the office head has authority over all media contacts, web postings, and press releases. While the policy below is applicable to OIG employees, the Inspector General may depart from it, or delegate to others the authority to depart from it, whenever in his/her judgment such action is appropriate. The Inspector General also may take any other action he/she deems appropriate, consistent with applicable laws, in connection with OIG public communications.

#### 1. Media Contacts

The communications and public affairs liaison ("communications liaison") is the focal point for all media communications, and any contact with the media by any OIG employee must be reported to the communications liaison.

The general authorizations for OIG individuals to answer media inquiries are as follows.

- Inquiries involving sensitive or highly publicized investigations or other reviews, and investigations being conducted jointly between an OIG field office and headquarters, between two or more OIG field offices, with another OIG, or with State or local law enforcement organizations, should be referred to the communications liaison, who will coordinate responses to media inquiries with the appropriate office prior to release.
- For routine operations or non-sensitive matters, the AIGs, DAIGs, ADAIGAS/RIGAs, SACs, and other OIG staff/division directors are authorized to answer general media inquiries when in their judgment it is appropriate to do so. If other employees are contacted, they should refer the caller to the appropriate OIG manager. The AIGs are responsible for ensuring the SACs and ADAIGAS/RIGAs receive appropriate training before talking to the media.
- Special agents who are approached by the media during an enforcement action (search warrant or arrest) are authorized to speak with the press generally about the OIG and that they are participating in a search warrant/arrest, but they are not to disclose any information about the case or identify any subject. They can tell the press to contact the respective Assistant United States Attorney or the

communications liaison, and they can hand out their business card and a brochure. The SAC is responsible for ensuring special agents receive appropriate training before talking to the media.

2. Web Postings. The OIG will post to its website reports, congressional testimony and statements of the Inspector General and OIG staff, news releases, and other items that pertain to the OIG. The OIG generally will post any Department of Justice press release that pertains to OIG work when available. All postings must be consistent with applicable laws, including the Privacy Act, the Freedom of Information Act, and the Trade Secrets Act.

a. Procedures for OIG web postings.

The OIG will designate individuals with authority to post content to the OIG web page. The communications liaison is responsible for ensuring those individuals receive training before they begin posting content to the OIG web page. Those designated individuals are authorized to post routine operational matters, organizational information, and press releases from other agencies, such as the Department of Justice, without further review. Copies of such posting should be forwarded to the communications liaison when posted.

Any final audit or other report must be reviewed by JC before posting to ensure any required redactions are made. Any non-routine matter, including information about specific audits, inspections, or investigations, must be coordinated with the communications liaison and receive legal review from JC before being posted. The designated individuals will post the material once the communications liaison and JC have concurred.

b. General guidance for OIG web postings.

The following general guidance is applicable to all OIG web postings. However, this guidance does not alter any existing legal requirements.

- All investigative material posted to the OIG webpage will comply with the Privacy Act and Department of Justice policy. More specifically, information from an OIG investigative file cannot be publicly disclosed absent an authorization under the provisions of the Privacy Act. In addition, the OIG must comply with Department of Justice regulations at 28 CFR 50.2, which can be found at the following link:

[http://edocket.access.gpo.gov/cfr\\_2001/julqtr/pdf/28cfr50.2.pdf](http://edocket.access.gpo.gov/cfr_2001/julqtr/pdf/28cfr50.2.pdf)

- As a general rule, the OIG will make information from an investigative file public only if it is already a matter of public record, e.g., information that has been offered in open court or made part of a guilty plea.

- Information about the subject generally will not be made public in administrative investigations or in cases where DOJ has declined.

- The Inspector General, or Deputy Inspector General, can decide to disclose non-public information when he/she determines there exists a legitimate public interest to do so, and release of that information would not constitute an unwarranted invasion of personal privacy.

3. Press Releases. To the extent possible, the OIG relies upon web postings and the local U.S. Attorney or other prosecutive authority, such as a representative of the Department of Justice (hereinafter

collectively referred to as the U.S. Attorney), to issue press releases on significant activities resulting from OIG investigations. OIG field offices should encourage the local U.S. Attorney to seek concurrent issuance by DOJ.

The OIG may draft a press release on its activities when a U.S. Attorney or DOJ does not intend to do so, or whenever the Inspector General or Deputy Inspector General decides it would be appropriate to do so. OIG press releases in general:

- ° address only completed work efforts, i.e., fully executed legal actions;
- ° adhere to the pre-trial publicity guidelines of DOJ (28.C.F.R. § 50.2, Release of information by personnel of the Department of Justice relating to criminal and civil proceedings);
- ° include only information that is a matter of public record (material designated as "For Official Use Only" or personal information protected by the Privacy Act of 1974 is not used); and
- ° receive the concurrence of the IG, DIG, Counsel to the IG, the communications liaison, and, as appropriate, the AIGI and/or AIGA.

a. Procedures for Issuance of Press Releases.

When the cognizant OIG official (e.g., RIGA, SAC, or staff/division director) believes a press release is appropriate, and the U.S. Attorney or DOJ representative is not going to issue a press release, the cognizant OIG official will draft a press release, in coordination with the U.S. Attorney as appropriate. The OIG official immediately forwards it to the communications liaison through the cognizant AIG or Counsel.

b. Information to be Included in OIG Press Release.

Submissions. Submissions for OIG press releases should generally include the following:

- ° the name, office address, and telephone number of the person who developed the submission or who is most familiar with the action;
- ° suggested release time, including the date and a designation of the release time as a.m., p.m., or immediate. In those situations where the appropriate time is not known, the material should be marked with the caption "Do Not Release Until Notified."

As general guidance, press releases may include the following types of information:

- ° a profile of the individual or firm involved, including complete name, city/state location, and nature of relationship to the GSA; for individuals, age, DOB, title, name of employer, and length of employment, if known; for firms, the type of service or product they provide, and the term of the contract;
- ° time frame of activity, i.e., the period of operations covered by the audit or inspection, or time period during which the wrongdoing occurred;
- ° all relevant dates, e.g., the date of the report, indictment/information, guilty plea, trial, sentencing, settlement, and judgment;

° synopsis of the matter reported and issues involved, including detailed information such as types of violations committed, dollars involved, number of counts; and potential outcomes such as maximum sentencing or fines that can be imposed;

° identification of any other agency that worked on this audit, inspection, or case;

° the name of the Assistant U.S. Attorney handling the case, as appropriate; and

° identification of other remedies pursued as a result of this audit or investigation.

Effective Date 11/22/2016

#### 605.00 OIG LIAISON WITH THE CIVILIAN BOARD OF CONTRACT APPEALS (CBCA)

##### 605.01 Responsibilities of the Civilian Board of Contract Appeals (CBCA)

The Civilian Board of Contract Appeals (CBCA) was established to hear and decide contract disputes between government contractors and civilian executive agencies under the provisions of the Contract Disputes Act. The CBCA's authority under this statute extends to all agencies of the federal government except the Department of Defense and its constituent agencies, the National Aeronautics and Space Administration, the United States Postal Service, the Postal Regulatory Commission, and the Tennessee Valley Authority. The cases heard by the CBCA often result from the audit and investigative activities of the OIG.

##### 605.02 OIG Liaison with the Civilian Board of Contract Appeals (CBCA)

The Counsel to the IG acts as the OIG liaison with the CBCA. While the AIGA, AIGI, and AIG for Inspections retain full authority over their respective areas of responsibility, all OIG offices notify JC prior to initiating any inquiry, audit, or investigation involving the CBCA. This notification requirement specifically includes, but is not limited to, matters relating to hotline complaints, inspections, investigations, and audits. In addition, the appropriate office head promptly advises JC of OIG audit or investigative matters that have been docketed for trial or other proceedings before the CBCA.

In order to ensure that JC receives prior notification, each headquarters and field OIG employee is responsible for advising the head of his/her office prior to initiating any inquiry, audit, or investigation involving the CBCA. It is then the responsibility of that office head to notify JC. Such notification is written, unless time constraints indicate otherwise. In that case, oral notice is confirmed in writing at the earliest possible time. With regard to OIG matters docketed before the CBCA, the appropriate office provides immediate notification to JC. Notification in such cases may be verbal.

Effective Date 11/22/2016

#### 606.00 OIG LIAISON WITH THE OFFICE OF CONGRESSIONAL AND INTERGOVERNMENTAL AFFAIRS

The OIG Congressional Affairs Liaison is responsible for coordinating contacts between the OIG and the GSA Office of Congressional and Intergovernmental Affairs. In support of this policy, all correspondence from or to the Office of Congressional and Intergovernmental Affairs is routed through the Congressional Affairs Liaison.

Special practices and procedures govern the coordination of the congressional and legislative activities of the Office of Congressional and Intergovernmental Affairs and the OIG. The understanding covers GSA responses to OMB requests for comments, congressional hearings and testimony, contact with members and congressional committees, congressional inquiries and requests for IG information, and the agency legislative program.

Effective Date 11/22/2016

#### 607.00 OIG RELATIONSHIPS WITH GSA OFFICIALS

Ongoing OIG relationships with GSA officials are coordinated and OIG activities are conducted in accordance with guidance contained in this Manual. However, because this Manual is available only to OIG personnel, GSA management officials rely upon the GSA Administrative Manual (5410.1 OAD P), Chapter 9 and Maintaining Discipline (9751.1 CPO), as the primary source for information regarding OIG, audit and investigative activities.

Chapter 9, Audit and Investigative Services, outlines OIG access to records, types of audits and investigations, procedures for requesting audits and investigations, and follow-up actions.

Maintaining Discipline (9751.1 CPO) contains the GSA Penalty Guide. Table I of the Penalty Guide lists offenses that normally should be the subject of management inquiry and action. Table II lists suspected irregularities that must be reported to the OIG for review.

Effective Date 11/22/2016

## 608.00 OIG RECOGNITION PROGRAM FOR GSA EMPLOYEES

The OIG seeks to recognize individuals within GSA who (1) proactively present OIG with information that shows waste, fraud, or abuse involving GSA programs and operations; (2) are more than helpful to the OIG during the course of an OIG review; or (3) are found, during the course of an OIG review, to have met legal requirements in an exemplary manner. This policy provides for non-monetary recognition only. Any requests for monetary recognition should be made to the Deputy IG as a separate matter.

### 608.01 Eligibility

Recognition authorized under this program may be given to any GSA employee, except current OIG employees.

### 608.02 Recognition Process

OIG employees will forward all recommendations for recognition under this policy to the AIG for Administration. The transmittal will include the name and title of the individual, which of the above categories apply, a synopsis of the reason for the recommendation, the proposed written recognition, and a proposed method for delivery. The AIG for Administration will provide the recommendations to the Deputy Inspector General on at least a quarterly basis for a final decision.

### 608.03 Recognition

An individual may be recognized under this program through any written letter of appreciation or commendation, including in either of the following ways:

#### Certificate of Appreciation

The individual may be given a Certificate of Appreciation in person from the IG, Deputy IG, or other appropriate OIG official; normally the individual also will be given a photograph of the presentation.

#### Letter of Commendation

The individual may receive a letter of commendation from the IG that will be sent down through his or her chain of command in order to recognize their contribution. The letter will be tailored to the particular facts of each case.

## CHAPTER 700 - OPERATIONAL POLICIES AND PROCEDURES

### 701.00 RESERVED

### 702.00 OIG REVIEW OF LEGISLATION, REGULATIONS, AND DIRECTIVES

- 702.01 Requirements for OIG Review of Legislation, Regulations, and Directives
- 702.02 Responsibilities for Coordinating OIG Review of Legislation, Regulations, and Directives
- 702.03 RESERVED
- 702.04 OIG Review of Legislation and Non-GSA Regulations
  - 702.04A JC's Role in Coordinating OIG Review
  - 702.04B Procedures for Coordination of OIG Review
  - 702.04C Distribution of Comments Within the OIG
  - 702.04D Clearance Officer Role in Coordinating OIG Review

### 703.00 RESERVED

### 704.00 (b) (7)(E) INFORMATION

- 704.01 Obtaining (b) (7)(E) Information from (b) (7)(E) for Use in Criminal Investigations
- 704.02 Review of Requests of (b) (7)(E) Information
- 704.03 Records and Reporting Requirements to (b) (7)(E) Information

### 705.00 AUDIT REFERRALS OF POTENTIAL IRREGULARITIES TO JI

- 705.01 Definition of Suspicion of Irregularity Document
- 705.02 Policy on Referring SOIs
- 705.03 Procedures for Processing and Preparing SOIs
  - 705.03A Processing Irregularities Discovered during an Audit
  - 705.03B RESERVED
  - 705.03C Preparation and Processing of SOIs
  - 705.03D Headquarters Resolution of Disagreements
  - 705.03E Status Reporting on Investigations Related to Suspended or Curtailed Audits
- 705.04 Reporting Standards of Conduct Violations Disclosed by Audits
  - 705.04A OIG Policy on Reporting Standards of Conduct Violations Disclosed by Audits
  - 705.04B Procedures for Reporting Standards of Conduct Violations Disclosed by Audits

### 706.00 JI REFERRALS OF POSSIBLE MANAGEMENT DEFICIENCIES TO JA

- 706.01 Policy on JI Referrals to JA
- 706.02 JI Referral Memoranda
  - 706.02A Preparation of JI Referral Memoranda
  - 706.02B Review for Sensitive Information in JI Referral Memoranda
  - 706.02C Notifications to GSA Management
  - 706.02D Tracking of JI Referral Memoranda
  - 706.02E Disclosure of Management Deficiencies Affecting Investigative Cases
- 706.03 JI Referrals of Synopses of Investigation

### 707.00 SUBPOENAS

- 707.01 OIG Subpoena Authority
  - 707.01A Business Records
  - 707.01B Personal Records

- 707.01C Financial Institution Records
- 707.01D Government Records
- 707.02 Responsibility Within OIG for Processing Subpoenas
- 707.03 Policy on Use of Subpoenas
- 707.04 Procedures for Requesting Subpoenas
- 707.05 Approval and Processing of Subpoenas
- 707.06 Service of Subpoenas
- 707.07 Return of Service
- 707.07A Location of Return of Service and Nature of Production
- 707.07B Return Proceedings and Subsequent Questioning
- 707.07C Fifth Amendment Privilege
- 707.07D Handling of Documents
- 707.07E Failure to Comply
- 707.08 Subpoenas to Financial Institutions
- 707.08A Applicability of Right to Financial Privacy Act of 1978
- 707.08B OIG Policy on Advance Customer Authorization
- 707.08C Notice Requirements
- 707.08D Limitations on Transferring Financial Records
- 707.09 Reimbursement
- 707.10 Subpoena Enforcement Actions
- 707.10A Responsibility for OIG Subpoena Enforcement Actions
- 707.10B Elements of Subpoena Enforcement Actions

#### 708.00 CIVIL FRAUD AND OTHER CIVIL LITIGATION

- 708.01 OIG Policy on Civil Litigation
- 708.02 Responsibility for OIG Development and Referral of Civil Fraud and Other Civil Cases
- 708.03 Special Procedures for Defective Pricing/Price Reduction Cases
- 708.04 Special Procedures for Qui Tam Actions
- 708.05 Settlement of Civil Fraud Cases
- 708.06 Discovery Requests
- 708.07 Civil and Administrative Fraud Remedies

#### 709.00 PROCESSING OF CONTRACTOR SELF-DISCLOSURES

- 709.01 Status Reports Regarding Contractor Self-Disclosures
  - 709.01A Report of Receipt
  - 709.01B Interim Status Report
  - 709.01C Closeout Report
  - 709.01D Responsibilities
- 709.02 Involving Stakeholders and Accepting Settlements
  - 709.02A Initial Disclosure Meetings
  - 709.02B Participation of the Department of Justice
  
  - 709.02C Notification of Contracting Officers
  - 709.02D Resolution Through Litigation
  - 709.02E Administrative Resolution

#### 710.00 RESERVED

## 711.00 FREEDOM OF INFORMATION ACT REQUESTS

- 711.01 OIG Policy on FOIA Requests
- 711.01 A New Requirements Regarding Electronic Records
- 711.02 Responsibility for OIG Processing of FOIA Requests
- 711.03 OIG Procedures for Processing FOIA Requests
- 711.03A Referral of FOIA Requests to JC
- 711.03B Processing of FOIA Requests by OIG Components
- 711.03C FOIA Disclosure/Denial Decision and Transmittal of OIG Reply
- 711.03D Time Deadlines for Responding to FOIA Requests
- 711.03E Web Links to GSA/OIG FOIA/PA Procedures/Regulations

## 712.00 PRIVACY ACT REQUESTS AND NOTICES

- 712.01 Privacy Act of 1974
- 712.02 OIG Policy on Privacy Act Requests
- 712.03 Responsibility for OIG Processing of Privacy Act Requests
- 712.04 Procedures for OIG Processing of Privacy Act Requests
- 712.04A Referral to JC
- 712.04B Processing of Privacy Act Requests by OIG Components
- 712.04C Disclosure/Denial Decision and Transmittal of OIG Reply
- 712.05 Privacy Act Notice Provisions

## 713.00 CONGRESSIONAL REQUESTS FOR INFORMATION

- 713.01 OIG Policy on Congressional Requests for Information
- 713.02 OIG Control of Congressional Requests for Information
- 713.03 Responsibilities of OIG Components for Processing Congressional Requests for Information
- 713.04 Constituent-Based Requests for Information
- 713.05 Protective Marking of Proprietary Data and Other Sensitive Material

## 714.00 RESERVED

## 715.00 OBTAINING DUN AND BRADSTREET REPORTS

## 716.00 OIG ACTIONS WHEN COMPANIES OR INDIVIDUALS UNDER AUDIT OR INVESTIGATION FILE FOR BANKRUPTCY

- 716.01 Procedures for Situations When Companies or Individuals Under Audit or Investigation File for Bankruptcy

## 717.00 RESERVED

## 718.00 OIG GOVERNMENT PURCHASE CARD POLICY

- 718.01 Purpose
- 718.02 Designating OIG Card Holders
- 718.03 Requesting OIG Government Purchase Cards
- 718.04 Prohibited Purchases
- 718.05 Strategic Sourcing & Green Purchasing
- 718.06 Mandatory Logging of Transactions
- 718.07 Acceptance of Training Services
- 718.08 Convenience Checks

718.09 Approving Official (AO) Responsibilities

719.00 TRANSMITTAL OF SENSITIVE INFORMATION VIA EMAIL

719.01 Background

719.02 Applicability

719.03 Policy

720.00 CONTRACTOR ACCESS TO SENSITIVE DATA OR USE OF INFORMATION TECHNOLOGY RESOURCES

720.01 Purpose

720.02 Applicability

720.03 Policy

Procedures for File Encryption using SecureZip.pdfProcedures for File Encryption using SecureZip.pdf

Effective Date 10/3/2017

## 702.00 OIG REVIEW OF LEGISLATION, REGULATIONS, AND DIRECTIVES

### 702.01 Requirements for OIG Review of Legislation, Regulations, and Directives

Section 4(a)(2) of the Inspector General Act of 1978, as amended, requires that the OIG review existing and proposed legislation and regulations relating to agency programs and operations. As a result, all GSA regulations and internal directives concerning new or changed operating policies and procedures are forwarded to the OIG for review. Legislative items are forwarded to the OIG for review by the GSA Office of Congressional and Intergovernmental Affairs.

### 702.02 Responsibilities for Coordinating OIG Review of Legislation, Regulations, and Directives

In connection with the duties and responsibilities mentioned above, the IG has designated Counsel to the IG as the OIG's Clearance Officer. The Clearance Officer is responsible for coordinating review of all regulations and directives. These include GSA orders, Federal Property Management Regulations/Federal Acquisition Regulations amendments, GSA organizational changes, GSA training material, and the review of existing and proposed legislation and non-GSA agency regulations for the OIG.

### 702.03 RESERVED

### 702.04 OIG Review of Legislation and Non-GSA Regulations

JC reviews legislation and non-GSA regulations, including legislation provided by the GSA Office of Congressional and Intergovernmental Affairs and the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

#### 702.04A JC's Role in Coordinating OIG Review

JC is responsible for processing and coordinating comments on all proposed legislation. This includes: (1) receipt of proposed legislation; (2) maintenance of a control register; (3) routing legislation to cognizant offices for review; (4) and preparation of/drafting comments for the signature of the IG.

#### 702.04B Procedures for Coordination of OIG Review

JC solicits comments on legislative matters and non-GSA regulations from other OIG components as appropriate. Components must provide timely responses to enable JC to prepare final comments in accordance with the often short time frames established for legislative matters. Comments prepared for the signature of the IG should provide for review and concurrence by the division/staff originating the comments, concerned OIG offices, the Counsel to the IG, and the DIG. Copies of OIG comments on proposed legislation are maintained by JC.

#### 702.04C Distribution of Comments within the OIG

Distribution of comments on proposed legislation within the OIG is as follows:

- ☐ IG;
- ☐ Counsel to the IG; and
- ☐ Interested OIG components.

#### 702.04D Clearance Officer Role in Coordinating OIG Review

The Clearance Officer is responsible for processing and coordinating all OIG comments on regulations and directives. This includes: (1) receipt of issuances; (2) maintenance of a control register; (3) routing issuances to cognizant offices for review; and (4) consolidation of replies, when necessary.

Effective Date 3/27/2013

704.00 (b) (7)(E) INFORMATION

704.01 Obtaining (b) (7)(E) Information from (b) (7)(E) for Use in Criminal Investigations



704.02 Review of Requests of (b) (7)(E) Information

Special agents must submit requests for (b) (7)(E) information through channels to JC for review and concurrence. (b) (7)(E). Once JC determines that a request meets the legal sufficiency standards set forth in (b) (7)(E) JC will prepare for the IG's signature a letter to (b) (7)(E) requesting (b) (7)(E) information. In addition to including the information required by (b) (7)(E) the letter shall specify that (b) (7)(E) provide the information directly to the agent who generated the initiating request.

704.03 Records and Reporting Requirements Relative to (b) (7)(E) Information

(b) (7)(E) requires that agencies in receipt of (b) (7)(E) information track (b) (7)(E) For this purpose, the OIG Manual requires special agents to report in writing to JC all disclosures made to DOJ trial attorneys or Assistant United States Attorneys in the course of prosecution discussions. (b) (7)(E). (Because of strict (b) (7)(E), special agents should not provide copies of the (b) (7)(E) information itself to JC.)

To comply with this (b) (7)(E) requirement, JC should maintain a separate file associated with each request for (b) (7)(E) information. The file should include the following:

- ☐ the JI generated request for (b) (7)(E) information;
- ☐ a copy of the (b) (7)(E)
- ☐ a notation of any disclosures made by JI to DOJ trial attorneys or Assistant United States Attorneys in the course of prosecution discussions; and
- ☐ a copy of JI's letter to (b) (7)(E) sending back the (b) (7)(E) information.

Additionally, when the OIG has (b) (7)(E) information in its possession, JC must provide a report to (b) (7)(E) containing a description of any significant changes in OIG procedures for safeguarding (b) (7)(E) information and the results of any internal inspections relating to adherence to these security guidelines. JC must make this report as of (b) (7)(E).

Effective Date 6/7/2013

## 705.00 AUDIT REFERRALS OF POTENTIAL IRREGULARITIES TO JI

### 705.01 Definition of Suspicion of Irregularity Document

The Suspicion of Irregularity (SOI) document is the means used by JA to advise JI of suspected wrongdoing discovered as a direct result of an audit assignment. Discovery of a suspected wrongdoing not related directly to audit assignments is reported to JI in accordance with the GSA Supplemental Standards of Conduct.

### 705.02 Policy on Referring SOIs

In carrying out their audit responsibilities, JA staff must be alert to any information indicating potential wrongdoing (e.g., violation of law or regulation, or a matter that would lead to a contractor's suspension or debarment). Such information is promptly referred to JI for evaluation and appropriate action.

Once an SOI has been referred to JI, the related audit activity should continue to the extent that the audit work and/or the issuance of the report will not significantly impede the conduct of an investigation or the likelihood of a successful prosecution. It is the responsibility of the cognizant audit and investigative personnel to ensure that:

- ☐ a determination is made on the specific aspects of the audit activity that would significantly impede the conduct of an investigation or the likelihood of a successful prosecution; and
- ☐ work on other significant aspects of the audit activity, if any, continues.

These policies, and the procedures detailed below, apply to situations where auditors have developed some empirical evidence that wrongdoing has occurred, or could have occurred. They should not be construed as limiting the free flow of information and dialogue between auditors and investigators in cases where such evidence has not been developed. To the contrary, ongoing dialogue between auditors and investigators is a prerequisite for successful OIG operations.

### 705.03 Procedures for Processing and Preparing SOIs

#### 705.03A Processing Irregularities Discovered during an Audit

Upon discovery of a potential investigative matter, the Audit Manager and/or Auditor-in-Charge promptly notifies the RIGA in accordance with Section 705.03C. The RIGA advises JAO of the general nature of the suspected irregularity, and then discusses the matter with the RIGI. Discussions between the RIGA and the RIGI may result in: (1) agreement that a formal investigation is not required; (2) agreement that an SOI should be prepared and the audit continued; (3) agreement that an SOI should be prepared and the audit suspended or curtailed; (4) agreement that an SOI should be prepared, but disagreement on whether or to what extent the audit should be suspended; or (5) disagreement on the need for an investigation. All discussions between the RIGA and the RIGI involving potential investigative matters should be documented and included in the audit workpapers whether or not an SOI is issued or a formal referral is made to JI.

Each of these situations is discussed in the following paragraphs. In each instance when a decision is made to suspend or curtail an audit, the RIGA responsible for this decision notifies JAO. JAO will then be able to determine the impact of this decision on related audits in other locations. The RIGA is responsible for ensuring that entries are made in the appropriate information system for SOIs originating in his/her office.

1. Agreement That a Formal Investigation is Not Required. When the RIGA and RIGI conclude that there is insufficient evidence to warrant an investigation, documentation of the following is included in the audit workpapers: (1) the condition found, (2) the discussions held, and (3) the basis for concluding that an SOI is not required. The RIGI must obtain a zero file number for this information so that it can be indexed and retrieved if needed by JI.

2. Agreement That an SOI Should Be Prepared and the Audit Continued. When the RIGA and the RIGI agree that an SOI is warranted, but conclude that the nature of the irregularity is such that continuing the audit would not hinder the investigation, the SOI is prepared and submitted in accordance with Section 705.03C on preparation of SOIs. The RIGA, after consultation or in conjunction with the RIGI, is responsible for advising the auditor-in-charge of the types of information relevant to the investigation that may be found while the audit continues, and any issues that, if found, could affect the decision to continue the audit.

3. Agreement That an SOI Should Be Prepared and the Audit Suspended or Curtailed. When the RIGA and the RIGI agree that the planned scope of future audit work may compromise or impede the investigation, the audit is suspended or curtailed and the basis for such action is documented in the workpaper files. During the suspension or curtailment period, the RIGI must comply with the requirements of Section 705.03E.

4. Agreement That an SOI Should Be Prepared, but Disagreement on Whether or to What Extent the Audit Should Be Suspended. If the RIGA and the RIGI disagree on whether or to what extent the audit should be suspended, the RIGA prepares and distributes the SOI in accordance with the instructions in Section 705.03C. The audit is temporarily suspended during the period outlined in Section 705.03D for resolution of the disagreement at the necessary level by headquarters personnel.

5. Disagreement on the Need for an Investigation. If the RIGA and the RIGI disagree on the need for an investigation, the RIGA can have his/her request considered at a higher level. Under such circumstances, the RIGA prepares and distributes the SOI in accordance with Section 705.03C.

705.03B RESERVED

705.03C Preparation and Processing of SOIs

1. Preparation of SOIs. When it has been determined that an SOI is warranted, the auditor-in-charge prepares an SOI using the format and content guidance shown in Figure 705-01. This memorandum includes all available pertinent information on the matter, including monetary amounts if determinable. The SOI is issued by the RIGA within 5 working days of the discussion between the RIGI and the RIGA.

2. Distribution of SOIs. SOIs are distributed by transmittal letter. The RIGA provides the original and one copy of the SOI to the RIGI and two copies to JAO, with another copy to JC. JAO keeps one copy for

its file and forwards one copy to the AIGA. The RIGI provides one copy of the SOI to headquarters for inclusion in the case file.

#### 705.03D Headquarters Resolution of Disagreements

In instances where the RIGI and RIGA disagree on suspension of an audit or the need for an investigation, the matter is submitted to headquarters for resolution. The RIGA submits, to JAO and the RIGI, a memorandum containing an explanation of the areas of disagreement and summarizing the positions of the RIGI and RIGA. The number of copies of the SOI provided with the memorandum is the same as outlined in Section 705.03C.

The appropriate staff directors in JI and JA resolve any such disagreements. If it becomes necessary, the AIGA and AIGI render a decision on the matter, with the IG becoming involved only as a final resort. The referral of such disagreements to headquarters are acted on within 10 working days after receipt of the SOI package.

The results of headquarters resolution of disagreements between the RIGI and RIGA are provided to both parties in writing. Telephonic notification may be made, but must be followed by written confirmation.

#### 705.03E Status Reporting on Investigations Related to Suspended or Curtailed Audits

JI provides JA periodic summary status reports on SOI-initiated investigations that have resulted in audits being suspended or curtailed. These reports are not intended to reveal information on the status of investigations, but rather permit JA to plan for the resumption of the audit process. In March and September, JI provides status reports to JA so that audit status in the automated audit information system can be updated for semiannual reporting to the Congress.

If it appears that the issuance of the audit report is not possible in the foreseeable future, the RIGI may recommend that the audit be cancelled. Such recommendation, including the reasoning therefore, is made in writing to the RIGA. If a RIGA reviews such a recommendation and disagrees with the suggestion to cancel, he/she forwards his/her reasons to the AIGA, who resolves the matter with the AIGI. The matter is processed in the same manner as disagreements outlined in Section 705.03D. The RIGA need not repeat the position of the RIGI, but attaches a copy of the memorandum written by the RIGI.

JA and JI are responsible for tracking investigations initiated through the SOI mechanism. As part of the Interdisciplinary Meeting agenda in each region, JA and JI representatives discuss investigations resulting from SOIs that have: (1) been active for more than 6 months; or (2) resulted in an audit being suspended or curtailed. When possible, the RIGI verbally provides an estimate as to when audit activity can be resumed.

Upon completion of an investigation initiated through the SOI mechanism, the RIGI promptly notifies RIGA of the disposition of the case and actions that can/cannot be taken regarding the audit that had been suspended or curtailed.

## 705.04 Reporting Standards of Conduct Violations Disclosed By Audits

### 705.04A OIG Policy on Reporting Standards of Conduct Violations Disclosed by Audits

Violations of the GSA Standards of Conduct are never reported in OIG audit reports. Instead, audit findings of actual or apparent misconduct are always referred to the Office of Investigations for handling.

### 705.04B Procedures for Reporting Standards of Conduct Violations Disclosed by Audits

When an audit discloses an actual or apparent violation of the GSA Standards of Conduct, the following actions are taken:

☐ The RIGA consults with the RIGI (AIGI on Central Office matters) about the need for investigation, and provides the RIGI (AIGI), by separate memorandum, a description of the actual or apparent misconduct.

☐ The RIGI (AIGI) handles the misconduct referral in accordance with the provisions of Chapter 900 of the OIG Manual. If the decision is made to refer the matter to management instead of conducting an investigation, the RIGI (AIGI) is responsible for preparing the referral memo and transmitting it to the party(ies) with an official need to know under a "For Official Use Only" cover.

☐ The misconduct finding is not discussed in the audit report or related transmittal memorandum.

☐ The AIGI/RIGI notifies the RIGA on the disposition of the referral.

NOTE: Discovery of suspected wrongdoing not related directly to audit assignments is reported to the Office of Investigations in accordance with the GSA Standards of Conduct.

Effective Date 10/3/2017

## 706.00 JI REFERRALS OF POSSIBLE MANAGEMENT DEFICIENCIES TO JA

### 706.01 Policy on JI Referrals to JA

In conducting investigations, OIG special agents need to be alert to possible management deficiencies, especially weaknesses in accounting and/or administrative control, that allow fraud or abuse to occur. In order to maximize the use of information acquired during investigations, JI reports such information to JA for audit followup. The JA followup action involves transmitting the information to management, asking JC or JP to take some internal OIG action, and/or scheduling an audit.

When investigation discloses the possibility of specific management deficiencies, JI referrals to JA are in the form of referral memoranda prepared by the case agents. When investigation does not disclose specific management weaknesses, but the investigative findings might nonetheless be of operational interest to JA, the DAIGI forwards a copy of the Synopsis section of the Report of Investigation to JAO.

When the AIGA and/or a staff director request additional information about a referral memorandum or a synopsis, JI either allows them to review the case file or requests that the case agent provide the additional information.

### 706.02 JI Referral Memoranda

#### 706.02A Preparation of JI Referral Memoranda

JI reports the possibility of specific management deficiencies to JA through referral memoranda. Each referral memorandum:

(1) describes the possible management deficiency; (2) details the reasons for believing the deficiency exists; and (3) provides available supporting documentation. The referral memorandum to the AIGA is prepared by the special agent conducting the investigation. It is reviewed by the Special Agent in Charge (SAC), then forwarded to the AIGI for signature, with a copy provided to the RIGA. The AIGI makes the formal referral to the AIGA.

During post case file reviews, the DAIGI verifies that case agents have prepared referral memoranda on all investigative results that disclosed the possibility of specific management deficiencies.

#### 706.02B Review for Sensitive Information in JI Referral Memoranda

The SAC and AIGI carefully review the referral memorandum and supporting documents to ensure that sensitive, privileged, protected, and/or grand jury material is not inadvertently disclosed.

#### 706.02C Notifications to GSA Management

All notifications of potential management deficiencies are reported to the appropriate level of GSA management by JA, either through an audit report or memorandum, as appropriate.

#### 706.02D Tracking of JI Referral Memoranda

The SAC submits copies of all referral memoranda to headquarters for inclusion in the appropriate case files. JA is not required to keep JI formally apprised of the audit or review steps taken as a result of referrals; however, JA informally apprises JI of the results of its reviews. JI is not responsible for tracking or following up on JA actions resulting from JI referrals.

#### 706.02E Disclosure of Management Deficiencies Affecting Investigative Cases

If the SAC determines that the disclosure of a management deficiency could have an adverse impact on the investigation, he/she first discusses the seriousness of the deficiency with the RIGA. If the RIGA agrees that disclosure of the deficiency can await completion of the investigation, submission of the referral memorandum awaits such completion. The SAC notifies the AIGI of such instances by way of a memorandum, with a copy to the RIGA for the workpaper files.

If the SAC discovers a management deficiency that could result in significant and immediate dollar losses to the Government or have some imminent adverse impact on a GSA program or operation, but its disclosure could adversely affect the conduct of the investigation, the SAC consults with the RIGA prior to submitting the referral memorandum. The purpose of this consultation is to formulate actions and procedures to be followed to protect the integrity of the investigation and prevent losses or damage to the Government. These actions and procedures are then set forth in the referral memorandum.

Disagreements between the SAC and the RIGA are resolved by the AIGI and AIGA or, finally, by the IG.

#### 706.03 JI Referrals of Synopses of Investigation

When the DAIGI post investigation case file review does not disclose the possibility of specific management deficiencies, but JI determines that the investigative findings may still be of operational interest to JA, JI forwards to JA, via GSA routing slip, the Synopsis section of the Report of Investigation. In cases where individual identities should be protected from disclosure, JI deletes the names and any identifying references from the copy of the Synopsis.

Effective Date 11/22/2017

## 707.00 SUBPOENAS

### 707.01 OIG Subpoena Authority

Section 6(a)(4) of the IG Act empowers the OIG to require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary in the performance of the functions assigned the OIG by the IG Act.

Generally, this subpoena power applies to four basic categories of records.

#### 707.01A Business Records

The IG Act enables the OIG to require production of any business record, even those that are not normally made available under the audit clause of a contract. Furthermore, records may be obtained from businesses, subcontractors, and others who may not be subject to the audit clause provisions of a particular contract.

#### 707.01B Personal Records

An individual can be required to produce records within his/her personal possession, including tax returns, bank statements, and employment records. For example, personal records of a corporate officer can be obtained in addition to business records of the corporation.

#### 707.01C Financial Institution Records

Banks, savings institutions, credit unions, loan companies, and credit card companies can be required to produce their records and those of their customers. In many such situations, however, the Right to Financial Privacy Act of 1978 is applicable. Generally, the Act requires that specific advance notice of the subpoena be provided to an individual (non-corporate) customer. The statutory notice requirements of the Act must be strictly observed and fully complied with in subpoenaing an individual's records from financial institutions. Delayed notice provisions are available in emergency situations to prevent the destruction of evidence or flight from prosecution (Section 707.08B). The requirements of this Act make it especially important that such cases be closely coordinated with JC.

#### 707.01D Government Records

A State, municipal, or quasi-governmental body or agency can be required to produce relevant documents. The OIG subpoena power is not available to obtain records and information from other Federal agencies.

### 707.02 Responsibility Within OIG for Processing Subpoenas

JC serves as the focal point for all matters relating to the use and issuance of OIG subpoenas. All requests for subpoenas must be processed in accordance with the procedures set forth herein and must be reviewed and approved by JC prior to being forwarded to the IG.

### 707.03 Policy on Use of Subpoenas

Under normal circumstances, such as when a document or record is available under the audit clause of a contract, or when an individual has a contractual obligation to provide certain documents, attempts are first made to obtain the documents by reference to such authority. Also, if there is no evidence of wrongdoing by an individual or corporation, the auditor/investigator/inspector should attempt to obtain the records through voluntary means.

In routine cases, a subpoena normally is not requested until information obtainable by other means has been examined and analyzed. This enables the requesting auditor/investigator/inspector to define with particularity those documents needed to complement existing information. Furthermore, if the receiving party files a motion to quash the subpoena, the OIG will be able to demonstrate that the information cannot be obtained through normal procedures. However, a variety of circumstances could justify the issuance of a subpoena at an earlier stage of the audit/investigation. These circumstances may include the immediate need to obtain documents to prevent their loss, alteration, or destruction. In complex audits/investigations, numerous subpoenas may be issued, as needed, at various stages of the audit/investigation in order to fully develop the case.

JA, JI and JE should consult with JC as early as possible when considering use of a subpoena. Such early consultation can help significantly in determining the appropriateness of a subpoena, in considering alternative means of acquiring needed materials, and in framing and processing the subpoena request and subpoena itself.

### 707.04 Procedures for Requesting Subpoenas

Whenever documentary information or records needed in connection with official OIG activities and operations are not otherwise provided, a subpoena request may be considered. Requests contain the following information:

☐ Background of Subject Matter Under Audit/Investigation. This section sets forth a concise history of the audit/investigation to date. It includes the authority for the audit/investigation, an identification of the contracts and individuals involved, the ultimate goal of the audit/investigation, a summary of the audit/investigation completed to date, and identification of all known agencies that may be conducting a similar or joint audit/investigation.

☐ Justification for Subpoena Request. This section generally describes the items sought by subpoena and explains why these documents cannot be obtained by other means. Any lack of cooperation by the party under audit/investigation or the holder of records is discussed. The request specifies the particular audit/investigative goals that will be furthered by the subpoena. In requiring the production of documents and information by subpoena, the OIG is not required to determine that there is probable cause to believe that a violation of a criminal or civil statute or administrative regulation has been committed and/or that the materials sought constitute evidence of such violation. Instead, it need only be determined that the items sought are reasonably necessary to further proper OIG investigative, audit, or related activities.

☐ Description of Items. This section describes as precisely as possible those items that are to be obtained by the subpoena. While individual documents need not be identified, documents should be divided into certain categories, e.g., payroll records, payment invoices, bank statements, or income tax

returns, and are identified as completely as possible by date and party. In some cases, certain individual documents should be identified.

In consultation with JC, consideration should be given to the use of “including but not limited to . . .” language to assure that both specific known documents and other relevant materials that may not be individually known or identifiable are obtained. If applicable, the document categories are cross-referenced to a particular contract. The auditor or investigator should remember that a subpoena request need not be all inclusive. If subsequent audit/investigation determines that other documents are needed or that other parties are involved, additional subpoenas may be issued.

This section also identifies the recipient of the subpoena. If the documents are to be obtained from a corporation, a corporate officer, appropriate regional official, or custodian of records of the corporation, that person or entity is set forth as the named recipient. A subpoena of partnership records is directed to a partner. A subpoena for the records of a financial institution is directed to either the president or the appropriate branch manager. If records are sought from a State or municipal agency, the head of the agency is identified.

Subpoena requests of financial institutions and electronic communication custodians (see § 707.09) are considered recurring services. Therefore, each component that anticipates issuing subpoenas in a given fiscal year must complete a procurement request which provides an annual estimate for such services at the beginning of the fiscal year (see Contracting (JPC) Procedures at the end of Chapter 400). Once approved, a designated individual from each affected component shall maintain a copy for documentation purposes.

☐ Time and Place for Return of Service. The requestor should establish a location for the return of service. While the field audit or investigation office should normally be selected, the location should be within a reasonable distance from the location of the records. Where return of service at the field office is impractical, arrangements are made to allow return at an appropriate Federal facility. In unusual circumstances, e.g., involving voluminous documents, arrangements may be made to allow a return on the premises of the recipient of the subpoena.

#### 707.05 Approval and Processing of Subpoenas

Subpoena requests, upon approval of the appropriate RIGA or SAC, are sent through the AIGA/AIGI to JC. Requests from JE must be approved by the AIG for Inspections before forwarding to JC. JC reviews the subpoena request for completeness, legality, and validity. If necessary, a JC attorney identifies further areas of audit/investigation that should be undertaken before the subpoena can be justified, or may require the auditor/investigator/inspector to provide further elaboration or material in support of the request.

Upon determination by JC that issuance of a subpoena is appropriate, JC prepares necessary subpoena documentation; Privacy Act Notice; appropriate correspondence; and a memorandum to the IG recommending approval of the subpoena. Subpoenas are issued only upon approval and signature of the IG or DIG.

## 707.06 Service of Subpoenas

JC, in consultation with the requesting auditor/investigator, selects a date for compliance with the subpoena. In most instances, this date is at least 10 calendar days after the date of service. The attorney and the auditor/investigator/inspector determine the most appropriate method for service to be accomplished: personal service at the corporate location or private dwelling, or by registered or certified mail.

If service is effected by mail, JC mails the subpoena with attachments to the parties concerned. If personal service is chosen, the subpoena is sent to the requesting auditor/investigator/inspector to serve. The RIGA/SAC determines the appropriate staff member to serve the subpoena. (A copy of the subpoena is also sent to the requesting field office for inclusion in the audit/investigative file.) The auditor/investigator/inspector then delivers the subpoena, with attachments, to the addressee as expeditiously as possible.

Service upon a corporation is made during business hours and to the addressee. If the addressee is unavailable, a corporate officer or registered agent for service of process will suffice. If an individual other than the addressee receives the subpoena, the auditor/investigator/inspector obtains a receipt, setting forth the recipient's name and position. The auditor/investigator/inspector then executes the remaining portions of the Certificate of Return of Service and returns it to JC.

Any modifications of the subpoena sought by the subpoenaed party or any dealings where the party is represented by counsel are referred to JC. In all cases involving a subpoena, close coordination and consultation between the auditor/investigator/inspector and JC are maintained. Modifications in the scope and location of return of the subpoena may be accomplished by mutual agreement between the recipient and the OIG. Prior to the date of return, the auditor/investigator/inspector may be asked to examine the documents upon the premises of the recipient to verify the existence and volume of the documents sought.

## 707.07 Return of Service

### 707.07A Location of Return of Service and Nature of Production

No later than on the day and time appointed, the recipient of the subpoena is required to mail the documents to the OIG or make them available at the corporate office. In most cases, the location of the return is the field audit or investigation office.

The subpoenaed party may provide copies in the place of originals. However, the original records must be made available for verification if required. Any questions concerning this area are referred to JC.

The cover letter also directs the recipient to prepare an index of the documents provided. While this index is helpful to the auditor/investigator, the respondent cannot be compelled to prepare it.

### 707.07B Return Proceedings and Subsequent Questioning

In many instances, the production of the documents is a relatively simple matter. The subpoenaed party produces the documents, indicates his/her capacity to certify the documents, and a sworn statement is made indicating that the records are accurate, complete, and in full compliance with the subpoena. If

the auditor/investigator/inspector believes, however, that the documents are not complete or in full compliance with the subpoena, the respondent may be placed under oath and questioned. The subpoenaed party has the right to be represented by an attorney when s/he is questioned.

#### 707.07C Fifth Amendment Privilege

The limitations imposed upon questioning during an OIG subpoena return proceeding decrease the likelihood of improperly obtaining an incriminating statement from a respondent. In some instances, however, a question may arise as to the need to advise the respondent of his/her right against self-incrimination. A corporation does not have a Fifth Amendment privilege against self-incrimination. Therefore, only questions concerning the personal records or actions of the respondent could lead to an element of self-incrimination. If, at any time during the proceeding, the auditor/investigator/inspector believes that a question, properly within the scope of the subpoena return proceeding, could lead to an improperly compelled self-incrimination of the respondent, an appropriate warning must be given immediately.

#### 707.07D Handling of Documents

In using subpoenaed records, the auditor/investigator/inspector must be aware of the need to maintain control over the records. At the outset of any examination of the documents, it may be difficult to determine which, if any, of the documents will be used in subsequent civil, criminal, or administrative proceedings. Therefore, proper control is maintained over all documents and access to the documents is carefully controlled.

Upon the completion of the examination, the auditor/investigator/inspector determines which records are kept for later use, and which records may be returned to the respondent. Any record that is determined to be relevant to a criminal, civil, or administrative proceeding is retained until all proceedings have been exhausted. Documents referred to another agency, such as the DOJ, the Small Business Administration, or the Department of Labor, should be uploaded to the appropriate audit/investigative file.

#### 707.07E Failure to Comply

When a subpoenaed party refuses to comply, fails to appear, or fails to provide documents as required by the subpoena, the auditor/investigator/inspector consults with JC immediately. JC is responsible for resolving such cases and for initiating subpoena enforcement actions where necessary.

#### 707.08 Subpoenas to Financial Institutions

##### 707.08A Applicability of Right to Financial Privacy Act of 1978

Subpoenas directed to financial institutions calling for production of financial records of their customers may necessitate strict compliance with the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401-3422. This statute requires prior or contemporaneous written notice to the customer that his/her financial records have been subpoenaed, thereby affording him/her an opportunity to challenge the subpoena in court. The Act applies only when the customer is an individual or a partnership of five or fewer individuals. It has no application where the financial records sought are those of a corporation, business trust, or partnership comprised of six or more individuals. Because of the burdens imposed by this Act

and the sanctions that may be levied for violators, subpoena requests involving financial records from financial institutions must fully document the precise nature of the business entity involved. Appropriate public records, contracts, and other documents are examined to confirm a business entity's status as a corporation, limited liability company, proprietorship, general or limited partnership, or joint venture.

Section 3403 of the Act prohibits a financial institution from disclosing financial records of a "customer" (i.e., an individual or partnership of five or fewer individuals) except in accordance with the Act and upon receipt of a written certification by the Government authority that it has complied with all applicable provisions of the Act. However, Section 3402(1) of the Act allows a financial institution to disclose financial records when the customer authorizes it in writing. This written authorization must be limited to 3 months duration, must be revocable by the customer at any time prior to disclosure, must identify the financial records authorized to be disclosed, and must state the purpose for disclosure and the customer's rights under the Act. If such an authorization is submitted to the financial institution, no subpoena is required.

#### 707.08B OIG Policy on Advance Customer Authorization

In situations where the Act is applicable, written customer authorization is sought before subpoenas to financial institutions are requested. One exception to this policy is where secrecy or surprise is essential. As a practical matter, secrecy or surprise can be achieved only when the delayed notice provisions of Section 3409 of the Act are utilized. Under this section, if an appropriate court finds that prior notice to the customer will seriously jeopardize the audit/investigation, or that there is reason to believe that other specified events will occur, the court may issue an ex parte order delaying for up to 90 days the service of notice upon the customer, and prohibiting the financial institution from informing the customer that financial records have been subpoenaed.

#### 707.08C Notice Requirements

Full compliance with the Act requires that the customer be served, personally or by mail, on or before the date the subpoena is served upon the financial institution, with:

- ☐ a copy of the subpoena;
- ☐ a notice specifying the reasons why the financial records are being sought and setting forth the customer's rights under the Act (pursuant to 12 U.S.C. §3408(4)(A));
- ☐ a customer consent and authorization form for access to financial records;
- ☐ a motion paper that the customer may complete and file with the appropriate court in order to challenge the subpoena; and
- ☐ a sworn statement form, which the customer may complete and file in support of this motion.

To perfect his/her challenge, the customer must file the motion and sworn statement within 10 days from the date of service or 14 days from the date of mailing of the notice. The certificate of compliance is not provided to the financial institution until the time for customer challenge has expired.

## 707.08D Limitations on Transferring Financial Records

There are special limitations on transferring the financial information that is obtained through an RFPA subpoena. Consult with JC before providing such information to another agency. Please note that this applies even to transfers to the Department of Justice/U.S. Attorney's Offices.

## 707.09 Reimbursement

Generally, subpoenaed parties are not entitled to reimbursement from the OIG for the costs of searching, assembling, and copying subpoenaed records. However, there are two notable exceptions to this rule:

- Financial institutions are authorized to seek reimbursement for the costs of gathering, reproducing, and transporting customer financial records subpoenaed under the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 et seq. The reimbursement is at such rates and under such conditions as the Board of Governors of the Federal Reserve System prescribes, as set out in 12 C.F.R. Part 219, Subpart A. A full explanation of RFPA requirements is found in paragraph 707.08 above.

- Custodians of electronic communications, i.e., telecommunication carriers, are authorized to charge a reasonable fee to cover the direct costs of searching for and providing information responsive to a subpoena pursuant to 18 U.S.C. § 2706. Reimbursement, however, is not required to the extent that a subpoena seeks "records or other information maintained by a common carrier that relate to telephone toll records and telephone listings." SAs are cautioned that telecommunication carriers may interpret virtually any request that does not use the words "telephone toll records" as being subject to reimbursement. The term "telephone toll records" generally includes records of outgoing long distance calls made from a landline and records of all incoming and outgoing calls made to/from a cellular phone. With respect to landlines specifically, the cost of searching for records of incoming and outgoing local calls is reimbursable, and the cost of searching for records of incoming long distance calls may also be reimbursable.

In situations where reimbursement applies, SAs should ensure that the subpoena seeks necessary information in a cost-effective manner. For example, SAs may use their discretion to contact financial institutions and telecommunication carriers prior to initiating the subpoena request to ascertain the types of records available as well as any costs, that may apply. If the invoice should not be paid, JC will inform the subpoenaed party by letter.

Upon receipt of an invoice for records provided by any entity, the recipient will forward the invoice to his or her component's designated purchase card holder for payment. If the cost of the invoice is under the micro-purchase limit, it will be processed for payment by the component's designated purchase card holder. If the invoice is over the micro-purchase limit, the purchase card holder will forward the invoice along with a copy of the recurring services procurement request to JP for payment.

## 707.10 Subpoena Enforcement Actions

### 707.10A Responsibility for OIG Subpoena Enforcement Actions

JC is responsible for initiating judicial enforcement of OIG subpoenas in those instances where subpoenaed parties refuse to produce, in whole or in part, documents required by those subpoenas. In situations where difficulty in obtaining compliance is anticipated, early coordination with JC is required.

#### 707.10B Elements of Subpoena Enforcement Actions

The following elements must be established by the Government in order to obtain judicial enforcement of OIG subpoenas:

1. Proof of service. This element is established by completion of the certificate of return of service on the reverse side of the subpoena.
2. Proof of failure to comply. Unless the subpoenaed party expresses in writing his/her intention not to comply with the subpoena, an affidavit is prepared for the signature of the officer before whom that party was to appear, stating that said party failed to appear (or otherwise comply) at the designated time and place.
3. The issuance of the subpoena and the investigation to which it relates are within the authority of the OIG. To the extent that such a question does arise, the responsibility for its resolution lies with JC. If a question arises about the authority and jurisdiction of the OIG in a particular matter, JC is responsible for addressing and resolving the issue.
4. The documents sought are reasonably relevant to the inquiry. To be relevant, a document must tend to make the existence of a fact of consequence in the investigation more or less probable than it would be without the document. Material that is itself relevant or that may lead to the identification of relevant evidence is within the proper scope of an OIG subpoena.
5. The demand for documents is neither "unduly burdensome" nor "overly broad." Mere difficulty in compliance or the broad scope of the demand will not, standing alone, prevent judicial enforcement of an OIG subpoena. The demand must be unduly burdensome or unreasonably broad, and the burden of establishing this is upon the subpoenaed party.

Effective Date 3/27/2013

## 708.00 CIVIL FRAUD AND OTHER CIVIL LITIGATION

### 708.01 OIG Policy on Civil Litigation

It is the policy of the OIG that, to the extent possible, civil aspects of fraud cases be pursued as vigorously as criminal aspects. In all cases involving criminal conduct, consideration must be given to civil aspects of the case that may warrant audit or investigative effort. It is important that these civil aspects (e.g., quantifying damages) be developed fully, and as early as possible, due to the potential legal problems involved in continuing or initiating an investigation in support of a proposed civil action at the same time that a grand jury is conducting a criminal investigation.

Whenever it is apparent that audit or investigative activity is needed in support of a potential civil action after a criminal referral has been made (and while a criminal investigation or prosecution is still pending), consultation with JC is required to protect against parallel proceedings problems. See manual section on OIG personnel as grand jury agents, Subchapter 506.00.

### 708.02 Responsibility for OIG Development and Referral of Civil Fraud and Other Civil Cases

JC has overall responsibility for the coordination and control of civil fraud and other civil litigation and related matters involving the OIG. JC has responsibility for providing guidance on the civil potential of matters disclosed through audit and investigation. JC refers all cases that are exclusively civil to DOJ or the U.S. Attorneys' Offices and coordinates OIG support and assistance to those offices after referral. Where appropriate, JC participates with DOJ or the U.S. Attorneys' Offices in the handling of civil litigation and related matters involving the OIG. Also JC participates with and assists in all civil/administrative cases handled by the Office of General Counsel.

Jl and JA will promptly advise JC of any matters or cases in process having potential for civil recovery, including cases under current criminal investigation. JC will participate with Jl in any civil referral of cases also having criminal potential. If DOJ's Criminal Division or the U.S. Attorneys' Offices forwards a criminal referral for civil consideration, Jl will promptly notify JC.

### 708.03 Special Procedures for Defective Pricing/Price Reduction Cases

Upon completion of an audit report that contains a finding of defective pricing/price reductions, the report will be referred to JC. JC, in consultation with JA, will evaluate the audit report. The evaluation process will include reviewing the contract file and any other relevant documents, reviewing any contractor response to the audit report, and conducting any interviews (e.g., the Contracting Officer and contract negotiator) as are necessary to make a determination as to the disposition of the matter.

If, as a result of the evaluation process, JC and JA determine that referral of the audit report to the Contracting Officer for administrative action is appropriate, then the referral will be made by JA. JA and JC will render assistance to the Contracting Officer as is appropriate until a contractual resolution of the matter is achieved.

If, as a result of the evaluation process, JC and JA determine that there is evidence of potential fraud and that investigative assistance is required, they will request such assistance from Jl. Jl will make a decision

whether to investigate the matter in consultation with JA and JC. If JI decides to investigate the matter, it will be jointly handled by JI, JA and JC.

If it is determined, either upon the initial evaluation or after further investigation, that a defective pricing/price reduction allegation has civil litigative merit, JC, after coordination with the relevant components, will refer the matter to the Department of Justice or the United States Attorney's Office as is appropriate. Once referral is made, JC, JA, and JI will render whatever appropriate and necessary legal, investigative and audit assistance is requested by the Department of Justice or United States Attorney's Office until the matter is resolved.

If at any time during the course of an audit or the evaluation process for a defective pricing/price reduction matter, JA or JC discovers evidence of criminal activity, JI will be notified immediately.

#### 708.04 Special Procedures for Qui Tam Actions

The qui tam provisions of the civil False Claims Act (see Section 708.07 below) allow private citizens to bring fraud actions on behalf of the Government. Depending on whether the Government takes over the suit from the private citizen (called "the relator") and proceeds with the action itself, the relator may receive anywhere from 15 percent to 30 percent of any fraud recovery, whether by settlement or judgment.

The statute has been set up to put these cases on a fast track that necessarily impacts any investigative or audit effort. The relator is required to file his suit under seal, which means that only the Government and the relator know about it. Although the filing of the lawsuit itself is sealed, the existence of the investigation is not necessarily required to be kept a secret. A copy of the complaint is served on both the U.S. Attorney's office and the Civil Division of the Department of Justice and those two offices will work out who will handle the case and who will arrange for any audit or investigation. The Government has 60 days from the time the complaint is served to investigate the complaint and decide whether to intervene in the suit, in which case the Government would take control of the suit from the relator. The Government can seek an extension of the 60-day limit from the court.

Usually, JC will be notified by DOJ or the U.S. Attorney's Office of the filing of any qui tam action. In the event JI receives notification of any such action directly from DOJ or the U.S. Attorney's Office, it will immediately notify JC. JC will provide JI and JA with copies of the materials filed in the suit and will coordinate any audit and investigative effort needed in the matter. JC has the responsibility for notifying DOJ or the U.S. Attorney's Office of the agency's recommendation to intervene or not intervene in the qui tam action.

#### 708.05 Settlement of Civil Fraud Cases

Generally, agency approval must be obtained prior to any settlement of a civil case by DOJ or the U.S. Attorney's Office. For matters arising under the civil False Claims Act or other civil fraud statutes, as long as a prospective settlement does not cause a change in the agency's policies and procedures, Counsel to the Inspector General is the settlement authority on behalf of the agency (February 3, 1997 Memorandum of Emily Hewitt, General Counsel). For any fraud cases that would cause a change in the agency's policies and procedures, the GSA General Counsel is the settlement authority. JC has responsibility for coordinating approval of such settlements with General Counsel's Office.

## 708.06 Discovery Requests

The OIG often receives requests for documents (particularly audit reports, workpapers, and investigative files) and requests for testimony of OIG personnel sought in discovery in litigation to which GSA is a party. All such requests should be brought immediately to the attention of JC. For documents, JC will determine any applicable privileges and will coordinate the release of the requested materials to the litigating office (OGC or DOJ/U.S. Attorney). For testimony, JC will coordinate the need for and timing of the requested OIG personnel. Generally, subpoenas and other similar demands for official GSA information through either documents or testimony of present or former GSA employees need to be handled in accordance with the agency's Touhy regulations found at 41 C.F.R. Subpart 105-60.6. Only the Inspector General or the Counsel to the Inspector General may accept service of a subpoena or other legal demand related to information, which is the responsibility of the OIG. For discovery requests in criminal relating to impeachment information concerning OIG special agents, see the section on the OIG's Giglio/Henthorn policy at Subchapter 901.05.

## 708.07 Civil and Administrative Fraud Remedies

In addition to the criminal statutes, there are a variety of civil and administrative remedies used by the appropriate Government authorities to pursue OIG-developed cases involving fraud in GSA's contracting programs.

### Civil Fraud

Civil False Claims Act--The Civil False Claims Act, 31 U.S.C. §§ 3729 et seq., has always been the Government's primary vehicle for pursuing civil fraud cases. The Act imposes liability for seven enumerated acts, including knowingly presenting a false record or statement to get a false or fraudulent claim paid or approved by the government. A knowing submission may be shown by either (1) actual knowledge of the false information, (2) a deliberate ignorance of the information or (3) a reckless disregard of the truth or falsity of the information. The United States need only prove its fraud case by a preponderance of the evidence and as of September 29, 1999, may recover up to three times the amount of damages and additional civil penalties of between \$5,500 and \$11,000 for each violation. 31 U.S.C. § 3729(a). The civil False Claims Act has two alternative statutes of limitations. A civil fraud suit must be filed either (1) within 6 years after a false claim has been submitted or a false statement in support of a false claim has been made or (2) within 3 years after the material facts are known to the Government, but in no event later than 10 years after the false claims or statements were made.

Contract Disputes Act--The Contract Disputes Act (CDA), 41 U.S.C. §§ 601-613, provides a process for resolution of contractual disputes generally. Section 604 of the CDA provides a specific remedy against fraudulent claims brought by contractors under Government contracts. Section 604 provides that contractors who are unable to support a portion of a claim they have submitted to the Government for payment, because of misrepresentations of fact or fraud, may be liable to the Government for the amount of the unsupported portion of the fraudulent claim together with any costs to the Government of reviewing the unsupported claim. This remedy, which is intended to prevent contractors from submitting inflated claims, carries with it a six-year statute of limitations and, unlike standard CDA claims, is required to be asserted by the Department of Justice in either federal district court or the Court of Federal Claims.

Special Plea in Fraud (Forfeiture)--The Special Plea in Fraud provision, at 28 U.S.C. § 2514, provides for the forfeiture of claims against the United States if the submitter of the claim corruptly practices or attempts to practice any fraud against the United States in the proof, statement, establishment or allowance of the claim. This remedy, which allows for forfeiture of the entire claim (including nonfraudulent portions), is only available to the Government in the Court of Federal Claims.

#### Administrative Remedies

Program Fraud Civil Remedies Act - The Program Fraud Civil Remedies Act, 31 U.S.C. §§ 3801 et seq. (PFCRA). The PFCRA was designed to cover small dollar frauds that were not economical for the Department of Justice to bring or for the district courts to decide. The Act applies to cases involving \$150,000 or less and its provisions essentially track those of the civil False Claims Act, except that the PFCRA also provides for the imposition of a civil penalty for the submission of a false statement unrelated to a claim for payment which is accompanied by an express certification. Under the PFCRA, the Government may recover up to double damages and a civil penalty of up to \$5,500 (as of September 29, 1999) for each claim.

PFCRA cases are handled by the Office of General Counsel, with the Department of Justice providing some general oversight. By regulation, the OIG (JI) handles investigations of PFCRA cases. 41 C.F.R. Part 105-70. JI should consult with JC before making any referrals of PFCRA cases. JC is responsible for providing legal advice and support to OGC in the litigation of these cases. Counsel to the IG must approve any settlements of PFCRA cases.

Progress Payment Fraud - This provision, found at 41 U.S.C. § 255(g), provides that if a federal agency finds there is substantial evidence that a contractor's request for advance, partial or progress payments is based on fraud, it can suspend or reduce the contractor's request for further payments. The regulations implementing this provision are found at 48 C.F.R. § 32.006.

Subcontractor Payment Protections - Statutory and regulatory requirements generally give the contracting officer an oversight role in ensuring proper payment by prime contractors to subcontractors and suppliers. 31 U.S.C. § 3903; 48 C.F.R. § 32.112. The regulations require a contracting officer to investigate assertions by a subcontractor or supplier that it was not being paid in accordance with its subcontract or other agreement and take remedial action if appropriate. If a contracting officer determines that a contractor's certification of payment to its subcontractors and suppliers is inaccurate in any material respect, he or she must initiate administrative or remedial proceedings. 48 C.F.R. § 112-1(c). At GSA, the contracting officer is required to report any material inaccuracy in such a certification to the Office of Inspector General. GSAR § 532.112-1.

Effective Date 7/9/2014

## 709.00 PROCESSING OF CONTRACTOR SELF-DISCLOSURES

The OIG views disclosure reviews as a critical part of the OIG mission to detect and prevent fraud, waste, and abuse. Accordingly, we will provide incentives to contractors to encourage their use of the disclosure program, as the alternative means of collection are much costlier to both the Government and industry. While we will not provide a safe harbor or otherwise protect a disclosing contractor from the appropriate civil or criminal remedies, if warranted, we accept that disclosures are made in good faith on the part of the disclosing contractor. Barring other factors, our review will expeditiously verify the information provided by the contractor's internal investigation, to the extent that investigation is complete and accurate.

### 709.01 Status Reports Regarding Contractor Self-Disclosures

Effective December 12, 2008, federal contractors are required by FAR 9.406-2, 9.407-2, and 52.203-13 to self-disclose to the OIG when they have credible evidence of a violation of the federal civil False Claims Act or a criminal violation under title 18 of the United States Code involving fraud, bribery, conflicts of interest, and gratuities. To encourage contractors to be forthcoming, the OIG will provide periodic status reports, as appropriate, to contractors that make disclosures.

#### 709.01A Report of Receipt

After the OIG receives a self-disclosure from a contractor, JA will prepare a letter confirming receipt of the self-disclosure to be sent to the contractor under JC letterhead, including the disclosure tracking number, and the OIG point of contact regarding the disclosure. If the disclosure was not made via the OIG electronic reporting form, JA will ensure the Department of Justice is notified of the disclosure.

If the disclosure appears on its face to contain inadequate information to identify the nature and extent of the offense disclosed, the OIG will follow the letter confirming receipt with a letter detailing the further information that is required.

For procedures on obtaining further information regarding disclosures generally, see Part 709.02A.

#### 709.01B Interim Status Report

After the receipt of a self-disclosure and prior to the resolution of any audit, investigation, or other action related to the disclosure, if the OIG has not been in contact with representatives of the disclosing contractor, the OIG may send an interim status report or reports to inform the contractor of the disclosure's status in the review process.

Any interim status report will be sent by JA. Interim status reports will not be sent if JI, JA, or JC objects for any reason, including (1) an OIG representative is in communication with the contractor about the disclosure; (2) the Department of Justice asks that no interim report be sent; or (3) other good cause exists for not providing an interim report.

The status report will state that the OIG is continuing to review the disclosure, and include the date and tracking number of the initial disclosure and the OIG point of contact for any further questions.

## 709.01C Closeout Report

The closeout report is a communication with the contractor, whether by letter or email, informing the contractor that the OIG has concluded its review of the disclosure, and that no further OIG action is anticipated based on the information available at the time. The communication will include the date and tracking number of the initial disclosure, and a point of contact for any further questions. All closeout reports will be sent by JA.

For disclosures that the OIG has pursued as civil or criminal violations, the project will be closed out upon notification that legal proceedings have been concluded.

For disclosures that the OIG determined to be overpayments, with no civil or criminal implications, the project will be closed out upon either JA's determination that no further OIG action is anticipated or upon notification by the Contracting Officer (CO) of resolution of the JA findings.

For those reviews that have concluded without a finding of civil or criminal violation, or the need for additional action by the CO, the project will be closed and the contractor will be notified that the OIG has concluded its review of the disclosure, and that based on the information available at the time, no further OIG action is anticipated.

The Department of Justice also will be notified in writing when a disclosure is closed out without DOJ involvement.

## 709.01D Responsibilities

JA will initially process all disclosures and ensure a copy is provided to JI and relevant personnel in DOJ.

JI will determine whether an investigation is warranted, and provide a copy of the disclosure to the relevant CO, if known.

JC maintains a telephone line, with the number posted on the OIG website that contractors can call with any questions. JC is also responsible for reviewing and signing all receipt reports.

JPM maintains the electronic self-reporting form on the OIG website. Submissions using that form will be made available to JA, JI, and JC, and to the Department of Justice, as it has requested.

## 709.02 Involving Stakeholders and Accepting Settlements

### 709.02A Initial Disclosure Meetings

Unless the information in the disclosure indicates that a meeting would be unwarranted, after receiving a contractor disclosure, a representative of JI, JA, or JC will contact the disclosing party and arrange an in-person meeting between representatives of the contractor, OIG representatives, and other relevant stakeholders, defined more particularly below.

At this meeting, the OIG will request from the contractor any information that is known at the time to be necessary to evaluate and resolve the disclosure. Representatives of the OIG and the disclosing contractor will establish points of contact for future communication necessary to resolve the disclosure.

Following the meeting, the OIG will determine whether an audit or investigation will be opened in order to verify and resolve the disclosure.

If the contractor proposes at the meeting an amount that it has calculated is owed to the government, OIG representatives may, at this time, suggest that the contractor promptly contact the appropriate Contracting Officer (CO) and pay the stated amount before the OIG performs further review. However, the OIG may not request or accept any immediate payment. Rather, that function belongs to the CO and the relevant payment office. The OIG should contact the CO under these circumstances to ensure the CO is aware of the issue and possible payment, and to ensure the CO accepts the payment without providing the contractor a release of liability. A release of liability should only be provided once the OIG has independently verified, and relevant stakeholders have concurred with, the amount owed to the government.

#### 709.02B Participation of the Department of Justice

Officials of the Department of Justice (DOJ)'s Criminal and Civil Fraud Sections have requested notification of all disclosures received by the OIG. Upon receiving copies of disclosures, Criminal and Civil Fraud attorneys may decline the matter immediately; accept the matter for further investigation and possible judicial proceedings; or reserve judgment on the disclosure until further facts have been developed.

#### 709.02C Notification of Contracting Officers

As discussed in Part 709.01D, JI will notify the responsible CO, if known, regarding receipt of a contractor disclosure. When the disclosure involves potential wrongdoing on the part of federal employees, JI—based on consultation with JA and JC—will determine when it would be appropriate to notify the CO. The OIG may determine in other circumstances that it is appropriate to delay notification of the CO, for example, in order to avoid possible disclosure of an ongoing covert criminal investigation, by the OIG or another law enforcement organization.

When appropriate, COs will also be invited to participate in initial disclosure meetings.

As discussed further in Part 709.02E, below, the CO responsible for a current contract is an official authorized to demand payments from disclosing contractors. Therefore, if a disclosure involves an ongoing contract and the CO does not participate in the initial disclosure meeting, after the initial meeting, a representative of JC, JI, or JA will contact the CO. The representative will inform the CO of the information provided by the contractor; the OIG's impressions regarding the accuracy of the information and the possibility of further amounts involved; and the OIG's audit and investigation plan for resolving the disclosure.

#### 709.02D Resolution Through Litigation

The OIG will determine whether to refer disclosure matters to the Department of Justice (DOJ) for resolution by litigation under the civil False Claims Act (FCA) if, under the circumstances of a particular disclosure, this is the most appropriate manner of resolution. In making this determination, the OIG will consider appropriate relevant factors as determined by JC, in consultation with JI and JA.

In the event that a disclosure is resolved under the FCA or the Truth in Negotiations Act (TINA), the Office of Inspector General has the authority to approve settlement agreements on behalf of the General Services Administration, if it is clear that the proposed settlement will not cause a change in GSA's policies or program activities. See Memorandum from Emily C. Hewitt, General Counsel, General Services Administration, to Kathleen Tighe, Counsel to the Inspector General, General Services Administration (Feb. 3, 1997). The OIG does not accept payments itself.

Therefore, if GSA has referred and DOJ has accepted a disclosure for resolution under the FCA or TINA, the CO should be advised not to accept any interim payment without DOJ concurrence. DOJ representatives, in conjunction with OIG representatives, may also undertake negotiations with a disclosing contractor when there is not agreement regarding the amount owed. After a final amount owed has been determined, DOJ attorneys may accept payment from a disclosing contractor of the amount owed in settlement of potential FCA or TINA claims.

#### 709.02E Administrative Resolution

If a disclosure is not resolved through FCA or TINA litigation or criminal prosecution, it must be resolved administratively under the authority of the Contracting Officer. (In administrative matters, the OIG may not concur in a settlement amount on behalf of the agency.)

In such a situation, the relevant GSA payment office may accept a payment offered by a contractor. The CO may issue a demand for payment and use the procedures in FAR Subpart 32.6 if the contractor does not agree on the amount owed; these payments are also collected by the finance office. See GSA Order ADM P 2030.2C, Audit Resolution and Followup System, ch. 4, ¶ 4(i); ch. 5, pt. 3.

In order that the OIG and the CO have a consistent understanding of the contractor's conduct and the amount owed, JI or JA representatives will periodically inform the responsible CO of the progress of OIG review of disclosures that have not been referred to and accepted by DOJ and that pertain to current GSA contracts.

In the event that a disclosing contractor offers payment of an amount owed with its initial disclosure, the decision on whether to accept that offer rests with the contracting officer. The OIG will not object (if asked) to a Contracting Officer accepting that payment insofar as (1) the contracting officer's actions do not constitute the Government's agreement as to the contractor's ultimate civil or criminal liability for the matter(s) disclosed, and (2) acceptance shall not prejudice the Government's right to obtain additional damages, fines, and penalties for the matter(s) disclosed. If subsequent review of the disclosure indicates that the initial payment was less than the amount owed, the OIG will recommend that the CO collect the unpaid amount. The OIG will work with the CO to ensure that the disclosing entity understands that acceptance of the initial payment does not waive the government's right to collect any amounts owed in excess of the initial payment.

If the contract has been closed out, or if the CO last assigned to the contract is no longer available, the GSA program office that issued the original contract can assign another CO to the contract to issue a demand letter and coordinate collection of any post-closeout amounts due with the finance office.

Effective Date 3/28/2013

## 711.00 FREEDOM OF INFORMATION ACT REQUESTS

Unless otherwise stipulated by this Manual or otherwise required by law, all requests for documents that have been developed by, or are under the control of the OIG, are processed in accordance with the Freedom of Information Act (FOIA) (5 U.S.C. § 552).

### 711.01 OIG Policy on FOIA Requests

The FOIA requires the disclosure of documents maintained by Federal agencies upon request, unless the requested documents, or portions thereof, fall within certain specific exemptions to the basic disclosure requirement. The assertion of an appropriate FOIA exemption in order to deny disclosure is discretionary on the part of the agency deciding official(s).

With respect to records developed and/or maintained by the OIG, the IG, DIG, and Counsel to the IG are the only Agency officials who may sign a FOIA disclosure or initial denial letter to a requestor.

Because of the specific statutory requirements governing FOIA matters, consultation with JC and adherence to the procedures set forth herein are essential in all such matters.

#### 711.01A New Requirements Regarding Electronic Records

The Electronic FOIA Amendments of 1996, Pub. L. No. 104-231, addresses the subject of electronic records created and/or maintained by an agency. The statute defines the term "record" as including records "maintained by an agency in any format, including an electronic format." The statute establishes the requirement for agencies to maintain "electronic reading rooms" for certain documents, including records processed and disclosed in response to a FOIA request that the agency determines "have become or are likely to become the subject of subsequent requests for substantially the same records."

The statute also requires that agency records created after November 1, 1996, must be made available to the public by electronic means. It requires agencies to provide requested records "in any form or format requested . . . if the record is readily reproducible by the agency in that form or format." The statute also requires agencies to "make reasonable efforts to search for [electronic] records in electronic form or format, except where such efforts would significantly interfere with the operation of the agency's automated information system."

### 711.02 Responsibility for OIG Processing of FOIA Requests

JC serves as the OIG focal point for all FOIA policy and related matters, and is responsible for coordinating the processing of each FOIA request within the OIG and for dealing with Agency personnel on such matters.

## 711.03 OIG Procedures for Processing FOIA Requests

### 711.03A Referral of FOIA Requests to JC

Each request for information received by an OIG headquarters or field unit is immediately forwarded to JC. The requestor is notified by the receiving unit that the request has been forwarded for review and processing. JC examines each information request to: ascertain the nature of the request; identify statutory provisions governing release; and determine the appropriate method of handling.

### 711.03B Processing of FOIA Requests by OIG Components

JC provides a copy of the request to the OIG component that has possession or control of the requested material. The component processes (reviewing and redacting as necessary) the requested material by the date assigned, and returns the same to JC for review and concurrence.

### 711.03C FOIA Disclosure/Denial Decision and Transmittal of OIG Reply

JC reviews the disclosure/withholding as proposed by the OIG component to determine the appropriateness and legality of the proposed disclosure/withholding.

A final transmittal letter to the requestor is prepared by JC and signed by the Counsel to the Inspector General, if the request is an initial request. An appeal from a denial of an initial request is signed by the IG or the DIG.

### 711.03D Time Deadlines for Responding to FOIA Requests

The Electronic FOIA Amendments of 1996 extended the previous time limit for responses to initial FOIA requests to 20 working days after receipt of a request. Requesters have 120 days to appeal a denial of an initial request for disclosure, and the OIG must make determinations on appeals within 20 working days after receipt of an appeal. The OIG may take an additional 10 days to respond to an initial request based upon "unusual circumstances" relating to the request itself, e.g., the volume of records sought. This additional time may not be taken due to predictable agency OIG backlogs of FOIA requests.

### 711.03E Web Links to GSA/OIG FOIA/PA Procedures/Regulations

GSA's internal procedures for handling FOIA requests may be found at:

<http://www.gsa.gov/portal/content/105305>

GSA's regulations for the implementation of FOIA are found at 41 C.F.R. Part 105-60, and may be accessed by linking to:

<http://www.gsa.gov/portal/directive/d0/content/526106>

The OIG's procedures for FOIA/PA requests may be accessed by linking to:

<http://www.gsa.gov/portal/content/105305>

Effective Date 3/28/2013

## 712.00 PRIVACY ACT REQUESTS AND NOTICES

### 712.01 Privacy Act of 1974

The Privacy Act of 1974 (5 U.S.C. § 552a) provides for the safeguarding of documents maintained by Federal agencies that contain information about individuals. Further, this statute requires that access to such records be granted on request to the individual about whom such information is maintained unless a specific statutory exception exists.

Information about individuals that can be retrieved by some personal identifier must be maintained within a system of records as prescribed by the provisions of the Privacy Act. All GSA/OIG investigative reports and related materials are maintained in the GSA System of Records titled "Investigation Case Files (GSA/ADM-24)." All such materials must continue to be maintained within this System of Records in order to ensure compliance with the Privacy Act.

GSA/OIG materials otherwise protected from disclosure under the Privacy Act may be disclosed under any one of 12 statutory exceptions: 1) "need to know" within the agency; 2) disclosures required under FOIA; 3) routine uses; 4) disclosure to the Bureau of the Census; 5) disclosure for statistical research; 6) disclosure to the National Archives; 7) disclosure to another agency or governmental unit for civil or criminal law enforcement activity; 8) disclosure for the health or safety of an individual; 9) disclosure to Congress; 10) disclosure to the General Accounting Office; 11) disclosure "pursuant to the order of a court of competent jurisdiction"; and 12) disclosure to a consumer reporting agency in accordance with the provisions of the Debt Collection Act.

### 712.02 OIG Policy on Privacy Act Requests

All requests made by a specific person for access to OIG documents that pertain specifically to that individual are processed under the access provisions of the Privacy Act. However, in the case of OIG documents maintained in GSA/ADM-24, materials maintained in this System of Records are exempt from the access provisions of the Privacy Act pursuant to 5 U.S.C. § 552a(j)(2) and (k)(2). If, however, greater disclosure would be provided to the requestor under the FOIA, rather than under the Privacy Act, then such a request will be processed under the provisions of the FOIA.

### 712.03 Responsibility for OIG Processing of Privacy Act Requests

JC serves as the focal point for all Privacy Act policy matters, and is responsible for coordinating the processing of each Privacy Act request within the OIG and for dealing with Agency personnel on such matters.

### 712.04 Procedures for OIG Processing of Privacy Act Requests

#### 712.04A Referral to JC

Each request for information under the Privacy Act received by an OIG headquarters or field office is immediately forwarded to JC. The requestor is notified by the receiving unit that the request has been forwarded for review and processing. JC examines each request to determine the appropriate method of handling.

#### 712.04B Processing of Privacy Act Requests by OIG Components

JC provides a copy of the request to the OIG component that has possession or control of the requested material. The component processes the requested material, reviewing and redacting as necessary, by the date assigned and returns the same, along with a draft transmittal letter, to JC for review and concurrence.

#### 712.04C Disclosure/Denial Decision and Transmittal of OIG Reply

JC reviews the disclosure/withholding as proposed by the component to determine the appropriateness and legality of the proposed disclosure/withholding.

A final transmittal letter is prepared by JC. The Counsel to the Inspector General signs the letter, if the request is an initial request for information. An appeal from a denial of an initial request is signed by the IG or the DIG.

#### 712.05 Privacy Act Notice Provisions

The Privacy Act also contains explicit notice provisions that must be complied with in conducting OIG investigations, audits, and inspections, unless specifically exempted by rules promulgated by the Administrator.

Whenever an official of the OIG conducts an interview or requests information from an individual, the results of that interview or the information obtained is maintained in the Privacy Act System of Records controlled by the OIG (Investigative Case Files, GSA/ADM-24). This Act requires that the individual be informed in writing of the authority for the solicitation, the principal purpose of the solicitation, the routine uses of the information obtained, the effects of nondisclosure, and whether disclosure is mandatory or voluntary. In such cases, individuals are provided with a copy of the Notice Pursuant to the Privacy Act of 1974. The individual conducting the interview notes in his/her report that a copy of this Privacy Act notice was provided.

With respect to this System of Records, an exemption from this notice requirement has been established for interviews conducted and information requests made in the course of a criminal investigation. Thus, to the extent that information is being sought directly in connection with a criminal investigation and/or the enforcement of criminal laws, a Privacy Act notice is not required.

Effective Date 6/15/2015

## 713.00 CONGRESSIONAL REQUESTS FOR INFORMATION

### 713.01 OIG Policy on Congressional Requests for Information

All congressional inquiries or requests for OIG information or documents are handled in the manner provided for under this section, unless otherwise directed by the IG, the DIG, an AIG, the Associate IG, or the Counsel to the IG. Congressional inquiries or requests for information are handled as responsibly and promptly as circumstances permit. As a general matter, the Congressional Liaison acts for the OIG on all congressional requests for information.

Inquiries or requests for information or documents are regarded as “congressional” if they are official requests made by or on behalf of a Senator, Representative, committee, subcommittee, or other organizational body or unit of the Congress, including the GAO and the Library of Congress. For purposes of FOIA or Privacy Act exemptions, an inquiry or request by a Senator or Representative that is clearly being made as an individual and not on behalf of a Committee is handled in the same manner as a request from any other individual.

Accordingly, in such situations any applicable FOIA or Privacy Act exemptions that would otherwise be asserted are asserted to a member of Congress seeking information as an individual (See 713.04).

### 713.02 OIG Control of Congressional Requests for Information

Any congressional inquiry or request for information is promptly referred to the Office of the Inspector General (J) for control purposes, with simultaneous notice to the Congressional Liaison. Any oral inquiry should be brought to the attention of the IG, DIG, and the Congressional Liaison.

### 713.03 Responsibilities of OIG Components for Processing Congressional Requests for Information

Congressional inquiries and requests for information are generally coordinated by the Office of the Inspector General (J), with notice to the Congressional Liaison. OIG components compile information, materials, and draft responses in strict compliance with established due dates.

Any proposed nondisclosure of information (e.g., where the material requested is extremely sensitive due to an ongoing investigation) is coordinated with JC. Final determinations on nondisclosure of information can be made only by the IG or the DIG.

### 713.04 Constituent-Based Requests for Information

If a congressional request for OIG information or documents is being made on behalf of a constituent, then the request is treated in the same manner as if the constituent had directly requested the material under either the FOIA or the Privacy Act. Any such requests should be forwarded to the Congressional Liaison and to JC for processing.

### 713.05 Protective Marking of Proprietary Data and Other Sensitive Material

When a response to a congressional request for information involves the disclosure of proprietary or other sensitive information, protective markings may be placed on each released page containing such material. The Congressional Liaison and JC will as necessary develop such markings.

All controlled unclassified information (sensitive material) provided to the Congress is transmitted with a cover letter that specifically references the inclusion of the sensitive data and includes a statement cautioning against unauthorized disclosure and, as appropriate, warning of the potential penalties.

Effective Date 3/28/2013

715.00 OBTAINING DUN AND BRADSTREET REPORTS

Printed Dun and Bradstreet reports can be obtained by calling 800-352-3425. Computerized reports can be obtained using "Crosstalk" applications on designated OIG computers. Questions should be referred to the Investigations Operations Division.

Effective Date 3/28/2013

## 716.00 OIG ACTION WHEN COMPANIES OR INDIVIDUALS UNDER AUDIT OR INVESTIGATION FILE FOR BANKRUPTCY

### 716.01 Procedures for Situations when Companies or Individuals Under Audit or Investigation File for Bankruptcy

The following procedures apply when OIG personnel receive indications of bankruptcy proceedings involving companies or individuals under audit or investigation:

- ☐ The auditor or investigator makes a reasonable attempt to confirm or deny any suspicions, rumors, or leads that the company or individual has filed for bankruptcy. Methods may include: (1) discreet inquiries to employees; (2) checks of bankruptcy court records; and (3) regular checks of the business section of the local newspaper.
- ☐ After verifying that a bankruptcy filing has been made or is planned, the auditor or investigator immediately contacts Central Office JA or JI, through regional channels, by telephone to brief them on the situation. The Central Office contact then immediately notifies JC of pertinent facts.
- ☐ Based upon the facts and urgency of the situation, JC asks JA or JI to provide a memorandum summarizing the nature and scope of the audit or investigation, its status and estimated completion date, the estimated potential dollar loss to the Government (if known), information and documentation concerning the bankruptcy filing, and the status of that proceeding. JC requests the minimum information necessary for GSA to file a proof of claim.
- ☐ JC then reviews all information provided and, when appropriate, refers the matter to either the Department of Justice or United States Attorney's Office (for fraud matters referred to DOJ) or to the GSA Office of General Counsel (for non-fraud matters), for the filing of a proof of claim.
- ☐ If determined by JC and the GSA Office of General Counsel to be necessary, JI checks into the possibility that the company or individual may have fraudulently transferred assets before filing for bankruptcy.
- ☐ If a case has already been referred to DOJ for criminal or civil action, then JC (in civil cases) or JI (in criminal cases) seeks the concurrence of DOJ (or the U.S. Attorney) before releasing information to the GSA Office of General Counsel. This is to avoid compromising a potential criminal or civil action because of the premature disclosure of critical information.
- ☐ JA and JI provide additional information to JC, if necessary, to ensure that the Government's claims in connection with the bankruptcy proceeding are aggressively pursued, without compromising the integrity of future criminal or civil litigation.

Effective Date 2/26/2018

## 718.00 OIG GOVERNMENT PURCHASE CARD POLICY

### 718.01 Purpose

The objective of this policy is to ensure that all OIG authorized Government Purchase Card (GPC) users are aware of their responsibilities. Specific guidance governing the Government Purchase Card Program (also known as the GSA SmartPay program) can be found in:

- 4200.1B OAS Management and Use of the GSA SmartPay® Purchase Card; and
- The GSA SmartPay2 Master Contract, Terms and Conditions

With the exception of the provisions discussed below, the OIG adopts GSA Order OAS 4200.1B Management and Use of the GSA SmartPay® Purchase Card in its entirety. As such, all OIG Cardholders must comply with the requirements contained in the GSA Purchase Card, including the requirement to complete refresher training every two years, to purchase from required sources before purchasing on the open market, and to re-certify as required.

Per FAR 8.002, the required Government sources are listed below in order of priority:

#### (1) Supplies

(i) Inventories of the requiring agency.

(ii) Excess from other agencies.

(iii) Federal Prison Industries, Inc. (not required for items totaling \$3,500 or less per FAR 8.605).

(iv) Supplies that are on the Procurement List maintained by the Committee for Purchase From People Who Are Blind or Severely Disabled.

(v) Wholesale supply sources, such as stock programs of the General Services Administration (GSA) (see 41 CFR 101-26.3), the Defense Logistics Agency (see 41 CFR 101-26.6), the Department of Veterans Affairs (see 41 CFR 101-26.704), and military inventory control points.

(2) Services. Services that are on the Procurement List maintained by the Committee for Purchase From People Who Are Blind or Severely Disabled.

### 718.02 Designating OIG Card Holders

Component Heads are responsible for appointing cardholders and/or designating approving officials (AO) in their respective components. Neither AIGs nor Office Directors may serve as both requesting officials and AOs.

### 718.03 Requesting OIG Government Purchase Cards

All requests for Government Purchase Cards must be made through the Deputy AIG for Administration. See GSA Order OAS 4200.1B, Section 5. JP will coordinate applications for setup, maintenance and cancellation of charge card accounts for all OIG cardholders and AOs.

### 718.04 Prohibited Purchases

In addition to prohibited purchases noted in GSA Order OAS 4200.1B, Section 33, OIG purchase cardholders except for those in JPC, shall not procure the following:

a. Services which are more suitably obtained through a Purchase Order:

- recurring services over the micro-purchase threshold,
- maintenance plans,
- software renewals, and
- services requiring a statement of work;

b. Information Technology Equipment or software\* except for:

- consumable supplies such as those listed in the attachment, and
- purchases made by JI in exigent circumstances to support an investigation or mission, which are not to be connected to the OIG network;

c. Smartphones;

d. Furniture\*\* requests regardless of price. Furniture includes non-consumable office items such as desks, chairs, tables, lamps, filing cabinets, storage units, safes (in excess of 200 lbs and needed by JI in exigent circumstances to support an investigation or mission), artwork and systems with locking and interconnecting panels;

e. Building services and construction (i.e. changing locks, requesting new keys, electrical services, mounting TVs, etc.);\*\*

f. Contracts with hotels and event venues;

g. Any type of clothing items including bullet proof vests (use OIG Blanket Purchase Agreement (BPA)), jackets, shirts and pants; and

h. Firearms and ammunition (excluding wearable parts).

i. Transportation and storage of vehicles (in excess of the micro-purchase threshold)

\* Information Technology Equipment or software requests must be forwarded to the Information Technology Division (JPM) for approval.

\*\* Furniture requests must be forwarded to the Facilities and Support Services Division (JPF) for approval. All building services (outside normal building maintenance and services) and construction projects must also be forwarded through JPF

Although AOs may issue written blanket authorizations for supplies routinely needed, per GSA Order OAS 4200.1B, Section 23, the authorization limitations for each OIG cardholders shall not exceed \$1,000 per month.

#### 718.05 Strategic Sourcing & Green Purchasing

All OIG government purchase cardholders must utilize the FSSI BPAs unless a better value can be obtained. OIG cardholders must properly document any "better value" determinations in the purchase card file. Similarly, while the OIG encourages employees to purchase "green" products, compliance with GSA's Green Purchasing Plan is not mandatory at this time.

#### 718.06 Mandatory Logging of Transactions

When logging purchases, the cardholder should include as much detail regarding the purchase as possible in the description field of the Pegasys document. OIG cardholders must specify the items being purchased, e.g., simply stating "office supplies" is not sufficient. See GSA Order OAS 4200.1B, Section 37.

Purchase cardholders must create CLs in Pegasys within three business days of the purchase. Transactions must be reconciled within 10 calendar days of the bank statement date.

Furthermore, OIG cardholders must keep and upload supporting documentation in Pegasys per GSA Order OAS 4200.1B, Section 38. At a minimum, documentation include:

- a. Order form or pre-written authorization must be uploaded when the log is created in Pegasys;
- b. Invoice or receipt must be uploaded within five business days of receiving the goods from the vendor; and
- c. Independent receipt and acceptance of goods and services for purchases over \$500 must be uploaded within five business days of receiving the goods from the vendor.

#### 718.07 Acceptance of Training Services

OIG cardholders and AOs must obtain and upload documentation showing receipt and acceptance of training attended by an OIG employee. Attendees must submit an email certifying their attendance and/or a copy of the training certificate to the cardholder.

#### 718.08 Convenience Checks

This policy permits JPC and other component purchase cardholders authorized by JP to issue convenience checks. If a needed service or supply can only be purchased with a check (i.e. the vendor does not accept the Government Purchase Card), the OIG cardholder authorized to issue convenience checks may do so.

## 718.09 Approving Official (AO) Responsibilities

- Approving Officials are required to monitor the purchase card activity of assigned cardholders and ensure that the purchase card is used properly. See GSA Order OAS 4200.1B, Section 1.e. Approving Officials should: Authorize all purchase card transactions in writing before purchases are made by the cardholder (e-mail is acceptable). If the AO is not available, a higher level official in line of authority over the AO may issue written authorizations for purchase card transactions.
- Review and certify Pegasys Monthly Credit Card Transactions reports within 10 days of receipt. The AO should certify the reports even if there are no purchase card charges for the statement cycle;
- Ensure that cardholders maintain all required documentation;
- Ensure that the cardholder's purchase card transactions are logged within three business days of purchase and reconciled within 10 calendar days from receipt of the bank statement line; and
- Ensure that cardholders respond timely to audit requests for documentation.

Effective Date 4/3/2015

## 719.00 TRANSMITTAL OF SENSITIVE INFORMATION VIA EMAIL

The policy addresses Office of Inspector General (OIG) encryption of any email transmission that contains or attaches sensitive information where that transmission is to a location outside the OIG network.

### 719.01 Background

The OIG follows applicable laws, regulations, and policies governing protection of sensitive information. See, e.g, GSA IT Security Policy Handbook, CIO P 2100.1J (December 22, 2015).

Because the OIG has its own network and IT responsibilities and operates outside the GSA firewall, the OIG has adopted the following policy regarding email transmittals of sensitive information.

### 719.02 Applicability

This policy applies to all sensitive information, including PII. While individual offices may designate specific information as sensitive, that term generally encompasses, but is not limited to:

- (1) confidential business or commercial information, including trade secrets, processes, operations, style of work, or apparatus, security controls, confidential statistical data, or amount or source of any income, profits, losses, or expenditures, belonging to any person, firm, partnership, corporation, or association;
- (2) any restricted work products;
- (3) information about any person that includes
  - a) his or her name or other identifier, and
  - b) sensitive, confidential, or personal information regarding that person, such as medical or genetic information; performance, disciplinary, or other personnel information; the fact of that person's involvement (as a subject or a witness) in a criminal investigation; or the person's personal telephone number or address; or
- (4) a full Social Security number or personally-owned credit card number (regardless of whether other identifying information is included).

### 719.03 Policy

All sensitive information transmitted through the OIG's email network must be encrypted when sent outside the OIG. If either the email or the attachment contains sensitive information, the user must encrypt both. This policy includes transmission to employees of GSA, other government agencies, and non-government entities. Procedures for encryption and guidance for assisting email recipients outside the OIG will be provided separately.

[1] The term “Personally Identifiable Information (PII), as defined in OMB Memorandum M-07-16, refers to information that can be used to distinguish or trace an individual’s identity (e.g., their name, social security number, etc.), either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Effective Date 6/2/2016

## 720.00 CONTRACTOR ACCESS TO SENSITIVE DATA OR USE OF INFORMATION TECHNOLOGY RESOURCES

### 720.01 Purpose

The objective of this policy is to ensure that OIG contracts involving information technology (IT) resources and handling of sensitive data (Chapter 719.02) are compliant with Federal security standards, policies and reporting requirements, including the Federal Information Security Management Act (FISMA), the Office of Management and Budget (OMB) Circular A-130, OMB Memorandum M-15-01 and National Institute of Standards and Technology (NIST) Standard SP 800-137.

### 720.02 Applicability

This requirement applies to all contracts, regardless of dollar value, awarded by or on behalf of the OIG that involve access to sensitive data and IT resources to conduct OIG business.

### 720.03 Policy

The OIG accepts and follows GSA Acquisition Letter MV-15-01 except where the provisions in that Order conflict with OIG policy including the GSA policy referenced below:

#### CIO 2160.4A Provisioning of Information Technology (IT) Devices

In addition to the policies referenced by Acquisition Letter MV-15-01, OIG contractors must also follow these OIG specific policies:

OIG P 5410.1B OIG Procedures and Policies, Chapters 420 (Collaborative Resources and Social Media), 434 (OIG IT Security Policy), and 424 (IT Equipment Request Policy).

## CHAPTER 800 - AUDIT POLICIES AND PROCEDURES

### 801.00 OFFICE OF AUDITS RESPONSIBILITIES AND ORGANIZATION

- 801.01 Audit Responsibilities and Standards
- 801.02 Audit Mission
- 801.03 Organizational Structure and Assigned Roles
- 801.04 Performance Team Member Responsibilities
- 801.05 Audit Independence and Personal Impairments
- 801.06 Access to Records
- 801.07 FAR Rule for Contractor Disclosure

### 802.00 AUDIT AND ATTESTATION ENGAGEMENT PLANNING

- 802.01 Planning Requirements
- 802.02 Planning Responsibilities
- 802.03 Annual Plan Preparation

### 803.00 INTERNAL AUDITS

- 803.01 General
- 803.02 Nature of Performance and Financial Auditing
- 803.03 Types of Performance and Financial Audits
- 803.04 Auditing Methodology
- 803.05 Engagement Letter
- 803.06 Audit Survey
- 803.07 Audit Plan
- 803.08 Entrance Conference
- 803.09 Communications with Agency and Other Officials
- 803.10 Audit Results and Recommendations
- 803.11 Fraud, Illegal Acts, Abuse and Noncompliance with Laws and Regulations
- 803.12 Computing Funds Put to Better Use and Questioned Costs
- 803.13 Exit Conference
- 803.14 Project Cancellation

### 804.00 EXTERNAL REVIEWS

- 804.01 General
- 804.02 Types of External Reviews
- 804.03 Identification of External Reviews to be Performed
- 804.04 Initiating External Reviews
- 804.05 Engagement Meetings and Discussions with Contracting Officials
- 804.06 Conferences with Contractor Personnel
- 804.07 Access to Contractor Records
- 804.08 Standard Report Objectives for External Reviews
- 804.09 Scope of External Reviews
- 804.10 GAGAS Statement for All External Reviews
- 804.11 Negative Assurance Statements
- 804.12 Reporting Views of Contractors
- 804.13 Referring Preliminary Results to Contracting Officials
- 804.14 Computing Funds Put to Better Use and Questioned Costs

805.00 DOCUMENTATION SUPPORTING AUDITS AND REVIEWS

- 805.01 Definition and Purpose of Documentation
- 805.02 Electronic Documentation
- 805.03 Instant Messaging
- 805.04 Paper-Based Documentation
- 805.05 Paper-Based Documentation Index Format
- 805.06 Supervisory Review of Documentation
- 805.07 Access to Documentation and Safeguarding Information
- 805.08 Maintenance and Disposition of Official Files

806.00 DRAFT AND FINAL REPORTS

- 806.01 Draft Reports
- 806.02 Independent Public Accountant (IPA) Draft Reports
- 806.03 Final Reports
- 806.04 Types of Final Reports
- 806.05 Report Format and Content
- 806.06 Referencing
- 806.07 Final Report Signature, Distribution, and Posting
- 806.08 Decision Records
- 806.09 DAIGA/RIGA Assessments of Final Internal Audits and External Reviews
- 806.10 Customer Satisfaction Questionnaires
- 806.11 Value-Added Assessment Form for Internal Audit
- 806.12 Quality Assurance Program

807.00 POST REPORT ACTIONS

- 807.01 Resolution of Internal Audit Reports and External Reviews
- 807.02 Implementation Reviews
- 807.03 JA Professional's Role in Contract Negotiations
- 807.04 Multiple Award Schedule Assessment Program and Database

808.00 NONAUDIT SERVICES

- 808.01 Nature of Nonaudit Services
- 808.02 Nonaudit Services That Do Not Impair Independence
- 808.03 Nonaudit Services if Supplemental Safeguards Are Taken
- 808.04 Nonaudit Services That Impair Independence

Effective Date 1/22/2010

## 801.00 OFFICE OF AUDITS RESPONSIBILITIES AND ORGANIZATION

### 801.01 Audit Responsibilities and Standards

The Inspector General (IG) Act establishes the fundamental responsibilities for conducting auditing activities. Also, Office of Management and Budget's (OMB) Circular A-50 contains policies for the audit of Federal operations and programs. Both the IG Act and OMB Circular A-50 require that audits of Federal operations and programs be performed in accordance with generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States. The IG Act further requires the appointment of an Assistant Inspector General for Auditing (AIGA).

Within GSA, the AIGA heads the Office of Audits (JA) with responsibilities for auditing activities and conducting reviews that cover GSA's management structure, operating programs, financial activities, companies with contractual relationships with GSA, and special mandates. As needed, JA also provides its expertise to other components of the Office of Inspector General (OIG).

### 801.02 Audit Mission

JA provides timely, cost effective, useful, and professional services to Agency officials. As such, JA uses authorized resources to provide audit and other products that contribute to the effective management of GSA's operations. In doing so, JA professionals perform all work in accordance with applicable standards, while seeking to complete projects within established or agreed upon time frames. Projects can include financial and performance audits, preaward and postaward external reviews, and other related products. The resultant products are provided to GSA managers and contracting officials; Congress; the Office of Management and Budget(OMB); the Government Accountability Office (GAO); the Department of Justice; and the public.

### 801.03 Organizational Structure and Assigned Roles

As depicted by the organizational chart below, the JA organization is comprised of Central Office management and staff offices, and national and regional managers.

- Assistant Inspector General for Auditing (AIGA) and Principal Deputy Assistant Inspector General for Auditing (PDAIGA) are responsible for all activities within the Office of Audits. They provide national direction and management oversight for all professionals within the Office of Audits. Formalized direction is not only contained within this chapter but can be supplemented with staff memoranda and/or technical guidance released from the immediate office of JA.
- Staff Directors from the Special Projects (JA), Audit Planning, Policy, and Operations Staff (JAO) and Administration and Data Systems Staff (JAS) support and assist the AIGA and the PDAIGA with new initiatives, planning, operational oversight, quality assurance reviews, and administrative activities.
- Deputy Assistant Inspectors General for Auditing (DAIGAs) have general audit responsibility specific to each of the five major functions in GSA:
  - o Internal Audits
  - o Acquisition (JA-A)

- ☒ Finance and Administrative (JA-F)
- ☒ Real Property (JA-R)
- ☒ Information Technology (JA-T)
  - o External Reviews
- ☒ Contract (JA-C)

As listed above, DAIGAs are responsible for overseeing four major internal areas and one external review function. JA-A is responsible for performance audits of all program activities of the Federal Acquisition Service. JA-F has responsibility for audits of GSA's financial and administrative functions. JA-R is responsible for performance audits of the real property programs of the Public Buildings Service. JA-T is responsible for all audits of GSA information technology systems and controls. Finally, JA-C is responsible for external attestation reviews of proposed and awarded contracts, including claims.

DAIGAs support the AIGA and PDAIGA in planning, coordinating, and facilitating nationwide audit activities within their area of responsibility. DAIGA responsibilities include serving as audit committee leaders, developing annual audit plans, and carrying out audit assignments with immediate staff members. In addition, they maintain continuing contacts and relationships with Agency officials. They monitor ongoing audit work including proposed recommendations as well as resolution decisions for sensitive, controversial, and significant audit efforts impacting their area of responsibility.

DAIGAs are the human resource managers for their office activities. They are responsible for overall management of audit operations and accomplishment of the portions of the annual audit program assigned to them. In this capacity, they serve as expert advisors to audit managers and performance teams. They ensure compliance with auditing standards and monitor compliance with established milestones. In addition, they transmit final reports to Heads of Service and Staff Offices (HSSOs) and Regional Administrators (RAs). DAIGAs also control the allocation of audit resources, as well as the assignment of annual workload requirements. Finally, they sign all non-routine correspondence addressed to HSSOs, RAs, and OIG components.

- Regional Inspectors General for Auditing (RIGAs) carry out the AIGA's internal audit and external review plans and serve as the JA representative in the region they are located. RIGAs provide liaison with regional or headquarters officials, and assist in both long-term resource utilization planning and policy formulation.

RIGAs are to notify DAIGAs of entrance, exit, and story conferences for performance audits not performed by the DAIGA's staff and within the DAIGA's area of responsibility. RIGAs should also provide copies of engagement letters and audit objectives. In addition, to ensure a consistent audit position, RIGAs should afford the DAIGA an opportunity to review draft reports prior to issuance.

Like the DAIGAs, RIGAs are responsible for overall management of their offices. RIGAs are responsible for managing human resources, accomplishing their portion of the annual audit plan, providing expert advice, ensuring compliance with auditing standards, and signing all non-routine correspondence to GSA managers.

- Audit Managers are responsible for all phases of the audit/review process. This includes the performance of fieldwork and the preparation of reports by JA professionals. As the principal manager of the performance team, the audit manager develops both team capabilities and individual competencies. They approve audit/review plans and finalize objectives. In addition, audit managers assign work and provide technical direction. They review supporting evidence throughout the fieldwork

process, as well as, ensure that all documented evidence that supports the report's findings and conclusions is reviewed prior to report issuance. They also review and sign internal and external reports. Finally, audit managers sign routine requests for information, and request legal opinions.

#### 801.04 Performance Team Member Responsibilities

Typically, performance teams are comprised of professional employees within the Office of Audits. Led by an audit manager, these team members conduct audits or external reviews. The team members are collectively responsible for work performance. Structured team meetings are used to encourage open discussion of objectives, scope, and methodologies. In addition, the meetings ensure that expectations and milestones are understood.

Team members are responsible for performing assigned duties in accordance with OIG policies and procedures, GAGAS, and established performance plans. Besides ensuring that individual assignments are professionally accomplished, JA professionals' responsibilities include working with team members and managers collegially. Auditors, management analysts, and information technology specialists are responsible for sharing technical knowledge and expertise openly.

On occasion, a performance team member is assigned to assist another team or office. In these instances, the JA activity to which the team member is assigned has responsibility for audit management responsibilities. This includes the approval of leave and training requests. For lengthy assignments, the manager for whom the team member is working for is responsible for preparing a written evaluation of the team member's performance. Professionals assigned to other OIG activities will be supervised by an audit manager and DAIGA/RIGA in the permanent duty station.

#### 801.05 Audit Independence and Personal Impairments

Under GAGAS, JA professionals have a responsibility to maintain personal independence so that their opinions, findings, conclusions, judgments, and recommendations are viewed as impartial by objective third parties with knowledge of the relevant information. Towards this end, JA professionals attend ethics briefings and annually complete a financial disclosure statement and a Statement of Independence. This ensures that they are free from personal and external impairments to independence, and have no reason to believe that a knowledgeable person would perceive them as not being independent.

As part of the planning process for every assignment, the entire team must address the issue of impairments and document those results in the Statement of Conformance. The same process is repeated for an individual who joins a project already in progress.

If potential impairments do exist, JA professionals are responsible for notifying their audit manager and DAIGA/RIGA of any potential impairment issues. The cognizant DAIGA/RIGA, in consultation with the responsible audit manager, is the designated official that will make "impairment determinations" on a case-by-case basis. Such determinations would be based on the employee's prior work experiences, relationships, and/or ideas or biases that might taint the conclusions reached on the impending work assignment.

Personal impairments generally result from relationships or beliefs that might cause a JA professional to limit the extent of inquiry, limit disclosure, or weaken or slant audit findings in any way. The GAGAS cites several of the generally recognized personal impairments, including when a professional has:

- A close family member who is an officer, employee, or person of influence over a program or entity under audit;
- A personal financial interest that is direct, or significant/material though indirect, in an audited entity or program;
- Prior responsibility for management or decision making that could affect the operations of the organization being audited, prior performance of accounting functions of the audited organization, or sought employment with the organization; and,
- Preconceived ideas toward individuals, groups, organizations, or objectives of a program that could bias the review, including biases induced by political and social convictions.

The Statement of Conformance must record that no impairments exist or how the DAIGA/RIGA resolved the potential impairment. The statement and supporting evidence should be maintained in the internal audit or external review's official file.

#### 801.06 Access to Records

The Office of Inspector General's professional employees have unrestricted access to all GSA documents, records, reports, papers, and other relevant information available to GSA personnel. This includes full explanations regarding management actions and decisions for the area under audit or review (GSA Administrative Manual, OAD P 5410.1, Chapter 9). Any denial of records or explanations should be immediately reported to JA management officials (AIGA, PDAIGA, and cognizant DAIGA). If not resolved, the issue will be reported to the Administrator and the Congress as a violation of the Inspector General Act.

#### 801.07 FAR Rule for Contractor Disclosure

FAR 52.203-13, Contractor Code of Business Ethics and Conduct, requires contractors to provide timely notification to the Government when credible evidence exists of certain violations of criminal law, violations of the civil False Claims Act, bribery, gratuity, fraud, conflicts of interest or significant overpayments. The rule provides for suspension or debarment of a contractor for knowing failure by a principal to disclose in a timely manner in writing to the agency OIG, with a copy to the contracting officer, these types of violations. The Office of Counsel to the Inspector General has developed a policy for processing these self-disclosures. Any disclosures provided to JA will be forwarded to JA-C for evaluation to determine if the disclosure involves audit issues. JA-C will provide the results of this evaluation to JA for appropriate action.

Effective Date 1/22/2010

## 802.00 AUDIT AND ATTESTATION ENGAGEMENT PLANNING

### 802.01 Planning Requirements

The Office of Audits annually plans its audits and reviews in order to identify and establish the workload for the fiscal year. The plan has two components; internal audits and contract reviews. In addition, as part of this effort, we identify and develop our management challenges for the upcoming year.

### 802.02 Planning Responsibilities

Overall planning is a shared responsibility. JAO has overall responsibility for maintaining the audit planning system and issuing the annual audit plan. Input for the annual audit plan is provided by the various program offices (i.e., JA-A, JA-F, JA-R, and JA-T) in conjunction with the JA Information Networks. The Contract Audit Office (JA-C) is responsible for identifying, coordinating and executing JA's external reviews. Both offices prepare their respective plans in consultation with JA's major components. Specific responsibilities include:

#### AIGA and PDAIGA

- Provide overall planning guidance and direction;
- Establish JA's goals, objectives and priorities for the year;
- Approve the specific planning process to be used each fiscal year;
- To the extent necessary, participate in the planning process through meetings and discussions;
- Solicit input for the plan from the Administrator and Deputy Administrator, the IG and Deputy IG;
- Authorize the annual audit plan for issuance; and,
- Approve changes to the priority audits established in the annual audit plan.

#### JAO

- Formulates office-wide audit planning policies to assure the development of an annual audit plan;
- Consults with the AIGA and PDAIGA on the specific JA objectives, goals and priorities for the planning year;
- Defines the specific process to be followed each year, including responsibilities, milestones and timetables for preparing the annual audit plan;
- Estimates available direct audit resources and establishes both direct and indirect time standards based on the prior three years of historical data contained in the GPRA reports;

- Maintains a listing of historical audits by service and by focus area which is provided to the DAIGAs/RIGAs for use in determining auditable areas;
- Maintains a listing of audits issued that includes the hours and days needed to complete each audit by audit type (program, system, MCR, etc.) for both internal audits and external reviews that allows for the establishment of time standards;
- Transmits memoranda to GSA's HSSOs and Regional Administrators informing them: that the audit planning process is underway, of the importance of their input, and that the cognizant DAIGA/RIGA will be contacting them to discuss how JA may assist them;
- Consults with the field audit offices and audit committees throughout the process, providing guidance and direction as required;
- Approves changes, as delegated from the PDAIGA, to the priority workload established in the audit plan;
- Prepares the formal audit plan for issuance to GSA management and OIG officials as well as the operating plan, including business plan data, for issuance to JA professionals;
- Maintains historical files on the development of the annual audit plan; and,
- Monitors the annual audit plan's implementation progress.

#### JA-C

- Establishes, with JAO, the time available for external reviews;
- Works with the RIGAs and the Federal Acquisition Service (FAS) to identify the specific Multiple Award Schedule contracts to be reviewed. The process is explained more fully in Subchapter 804, External Reviews; and,

#### DAIGAs and RIGAs

- Solicit input for the plan and management challenges from HSSOs and regional management;
- Solicit input from the Information Network (committees of JA professionals with experience in selected areas of expertise);
- Prepare risk assessments for their areas of responsibility to define the most significant vulnerabilities and challenges;
- Establish an inventory of potential audits that can be performed locally or nationally during the upcoming fiscal year;
- Recommend audit areas for inclusion in the annual audit plan, prioritizing recommended projects and preparing Audit Assignment Records as needed; and,

- Participate in planning meetings.

In addition, DAIGAs can approve changes to local audits on the plan and specific objectives for each audit.

### 802.03 Annual Plan Preparation

To meet the needs of GSA's fluid operating environment, each year JA will review and adjust the audit plan's development process as needed before the planning process begins. The process will remain within the broad outline of this policy.

There are five broad phases of the planning cycle; Planning Strategy Development, Information Gathering, Project Development, Plan Consolidation, and Plan Issuance.

**Planning Strategy Development** - The annual audit plan is developed through collaborative participation of each of JA's organizational components. At the beginning of the process, the AIGA, PDAIGA, DAIGAs, and JAO discuss planning strategies for the upcoming year. The AIGA/PDAIGA's concerns and requirements are determined and emphasized at the outset of the plan's development. Specific steps include identifying: the basic approach to be used to develop the plan, key duties and responsibilities of audit staff, timeframes for the process, preliminary data needed for plan development, and potential audit areas and any GSA management challenges.

**Information Gathering** - The primary sources of information come from GSA management and OIG components. In particular, JA's experienced professionals, especially those associated with the Office of Audit's Information Network, offer unique insights and perspectives into GSA operations and management. This Network consists of the DAIGAs, RIGAs, audit managers and key JA professionals throughout the country. Its mission is to enhance communications and build a continual relationship with management in order to keep current with GSA's ongoing programs, initiatives, and any associated management challenges.

Documentary information should also be used to help formulate the plan. Examples of such information include the OIG Strategic Plan, GSA's and OIG's management challenges, GSA budget and financial statement information, prior audit reports, and other OIG publications. It should also consider GSA business line information, GSA public information, such as newsletters, Government Accountability Office (GAO) reports, and information from other outside parties, such as the Office of Management and Budget and Congress.

**Project Development** – The information gathered from all sources must be properly organized and assembled for further evaluation. The audit assignment record not only serves this purpose but provides the preliminary basis used to identify, select and support new audit assignments. The assignment record contains the following information: audit subject, type, audited GSA service, performing audit office(s), SAR due date, applicable management challenge, audit focus, background information about the audit subject, key issues, and any special instructions.

**Plan Consolidation** – This phase takes place once the Audit Assignment Records have been completed and assembled. The assignment records should contain all relevant data/input obtained during the information-gathering phase, including any Inspector General priority. The records are then prioritized

during the audit selection process, providing the decision makers with the documented support needed to consider audits for the audit plan.

The audit selection process considers the DAIGAs' and planning committees' advice, the JAO Director's judgment and the audit field offices' recommended priorities. The selection of audit assignments must also take into account the availability of JA resources in the upcoming fiscal year.

Towards this end, time projections are developed to determine the resource requirements for each audit office. The available time developed for each office is based on several factors, including the number of JA professionals in each audit office, the time needed to complete carryover audit work, administrative requirements, and other considerations (i.e., employee leave, job training requirements, etc.).

After careful consideration of the information obtained in the aforementioned phases, the audits can be selected and the audit plan prepared. Once the plan is prepared, draft copies are submitted to HSSOs, RAs, and audit field offices for comment. JAO evaluates the comments and adjusts the audit plan as necessary.

Plan Issuance - The Office of Audits issues the final audit plan for internal reviews for the subsequent fiscal year by September 30 of each year. A copy of the internal audit plan is given to GSA management. The operating version of the plan is given to all components of the OIG on-line. The external review plan, which spans a two-year period, is provided to the RIGAs and is maintained by JA-C.

Effective Date 1/22/2010

## 803.00 INTERNAL AUDITS

### 803.01 General

The Office of Audits conducts internal audits of GSA's functions, with particular attention given to Acquisition, Finance and Administrative, Information Technology, and Real Property. Internal audits generally cover either performance or financial aspects of GSA's functions.

Such audits conform to the Government Accountability Office's GAGAS requirements, and integrate, when needed, guidance from the Council of Inspectors General on Integrity and Efficiency (CIGIE) and the Office of Management and Budget (OMB).

### 803.02 Nature of Performance and Financial Auditing

Performance Audits focus on improving Agency operations by providing information and recommendations to management and decision-makers responsible for delivery of services and public accountability. They also seek to ensure that Government assets and programs are reasonably protected against fraud, waste, and abuse. In addition, the audits attempt to verify that Government assets and programs are used efficiently and effectively.

This subchapter is intended to supplement GAGAS by providing additional guidance for specific audit processes. In addition, it will provide guidance and the methodology for: surveying review areas, establishing audit objectives and scope, planning and conducting fieldwork, developing findings and recommendations, and preparing draft and final reports.

Financial Audits primarily focus on the design and performance of oversight procedures when using Independent Public Accountants (IPAs) and other specialists in the audit of Agency financial statements. The Chief Financial Officers' (CFO) Act of 1990 requires the Inspector General or an independent external auditor (as determined by the Inspector General) to audit the Agency's financial statements. This audit must be performed in accordance with Government Auditing Standards issued by the Comptroller General of the United States. GSA OIG contracts with an IPA to conduct GSA's financial statement audits. To fulfill its audit responsibilities under the CFO Act, JA reviews the IPA's audit work to ensure that GSA's annual financial statement audits are performed in accordance with the standards for financial audits contained in the generally accepted government auditing standards and requirements of OMB Bulletin Number 07-04, "Audit Requirements for Federal Financial Statements."

### 803.03 Types of Performance and Financial Audits

Performance audits consist of an independent, objective assessment of economy and efficiency of operations, program effectiveness of results, compliance with legal requirements, and the adequacy of internal controls. These audits are commonly defined as follows:

- Program Audits are broad-based evaluations of Agency programs, operations, or activities. They can assess how well legislative, Agency, and customer requirements and expectations are being met; if the area is operated in a cost-responsible manner, or whether the program under review could be accomplished more effectively;

- Management Control Audits examine whether the existing system of management controls can reasonably ensure that program assets are safeguarded, efficiently used, appropriately monitored, and used to achieve expected outcomes;
- System Audits evaluate whether automated information systems assist the Agency in meeting customer needs, help management to achieve efficient and effective operations, contain adequate system controls, are properly secured, and meet user requirements;
- Compliance Audits are designed to evaluate the conformance of Agency operations and activities to applicable laws, regulations, policies, and procedures, as well as ensure that reasonable safeguards exist to mitigate against the occurrence of fraudulent activities; and,
- Regulatory Audits include reviews, other than financially related audits, that are mandated by law or regulation.

Financial audits are primarily concerned with providing an independent assessment of and reasonable assurance about whether the agency's financial condition, results, and use of resources are presented fairly in accordance with recognized criteria. This type of audit may also include assessments on financially-related information and processes, and determining compliance with financial regulations, as well as, providing special reports such as specified accounts of a financial statement.

#### 803.04 Auditing Methodology

Performance audits are usually completed in four phases. Each phase is initiated with a story conference. The conferences focus the team's expectations for the forthcoming audit phase. They ensure that team members clearly understand individual assignments, milestones, and team performance requirements. The conferences usually involve all team members, are facilitated by a team member or a JA professional from another audit office, and are conducted in an open forum environment. This structured process ensures that all team members have the opportunity to raise issues and offer suggestions.

During such conferences, the Statement of Conformance will be completed and/or updated as needed to ensure the audit team documents its compliance with GAGAS throughout the performance audit process.

DAIGAs are routinely invited to attend story conferences involving audit work in their area of responsibility. Audit offices should provide sufficient advance notice to the cognizant DAIGA.

The four story conference meetings and principal audit processes accomplished in the subsequent phases are:

- Preliminary Project Meeting is used to plan the survey work and to review team capabilities and responsibilities. The survey is meant to be a fact-finding process that gathers readily available information from as many sources as possible without detailed data examination. This meeting confirms the areas of the review, type of audit, and initial scope parameters. The meeting results in the assignment of survey responsibilities and establishment of completion milestones. The purpose of the survey is to gather enough information to be able to reach a decision on whether to continue with the

audit and, if so, in what areas. The use of a facilitator at this preliminary meeting is optional at the discretion of the DAIGA or RIGA.

The preliminary project meeting is also used to ensure all team members (1) are free from impairments to independence; (2) understand the concepts of reasonable care and professional skepticism; and (3) possess the collective knowledge, skills, and abilities to accomplish the audit objectives (Statement of Conformance).

Following the meeting, audit team members hold an entrance conference with management and begin gathering survey data. (See Section 803.06 for additional information on audit surveys.)

- Survey Assessment Meeting is held upon survey completion. The purpose of this meeting is to thoroughly assess the results and reach a decision regarding the need to continue the audit. Generally, a decision to continue the program review would stem from the identification of potentially material program management weaknesses or significant opportunities for program improvements.

If a decision is made to continue the audit, then the audit team establishes the audit objectives, scope and audit steps. During this meeting, the team discusses and assesses internal controls, information system controls, legal and regulatory requirements, fraud risks, the potential for abuse, and audit criteria that are relevant to the audit objectives. Following this meeting, the performance team formalizes the audit plan, holds an entrance conference with Agency management, and initiates fieldwork testing. (See Section 803.07 for additional information on audit plans).

If the decision is made not to continue the audit, a letter report can be developed to management outlining the nature, scope, and results of the survey work advising that no further audit effort is contemplated. The report should address any specific areas of concern raised by management officials during the survey process. The scope section of the report should note that while critical aspects of the program's management processes were identified, the survey did not assess the effectiveness of the program's management control structure. The report should also state that the survey efforts were performed in accordance with GAGAS.

- Fieldwork Verification Meeting is used to confirm that the results of the fieldwork provide reasonable assurance that the evidence is sufficient, appropriate, and significant to support the audit team's findings and conclusions, and considers audit risk in accordance with GAGAS. In addition, the audit team should obtain an understanding of internal controls and information system controls within the context of the audit objectives. For those controls that are deemed significant, auditors should assess whether the controls have been properly designed and implemented and sufficient, appropriate evidence is obtained to support the assessment of the effectiveness of those controls. Furthermore, the audit team should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect the findings and conclusions. Following this meeting, team members either conduct more fieldwork or move directly to the report-planning meeting.

- Report Planning Meeting is used to formulate the presentation strategy for preparing the audit report, including the development of an outline for each major section of the audit report. Following the meeting, team members draft sections of the audit report for consolidation, editing, and supervisory review. (See Section 803.10 for additional information on audit results and recommendations, and Subchapter 806 for preparing draft and final reports.)

Financial audits follow some of the same general procedures in performing reviews of the IPA's work that are used in conducting performance audits, however, not all GAGAS requirements apply because the standards address audits and attestation engagements, not reviews of audits performed by others. Specifically, the performance team conducting the review will be independent and competent and will use professional judgment. Also, the review will be adequately planned and properly supervised. Further, the performance team will obtain and document in the audit documentation sufficient, competent, and relevant evidence to support any findings and conclusions. Finally, results of the review may be communicated to appropriate GSA officials.

The extent of the review of the IPA's audit documentation and supplemental testing will be based on (1) any standards or requirements pertaining to the Chief Financial Officer (CFO) audit, (2) results of prior reviews, and (3) concerns of OIG management.

#### 803.05 Engagement Letter

For audits identified in the annual audit plan, engagement letters are issued to Agency program officials several weeks prior to project initiation. For regional audits not in the annual audit plan, the project must be coordinated with the respective DAIGA prior to being initiated. This will ensure the review is consistent with existing priorities. Engagement letters are issued for all audits, except where the nature of the audit requires that the JA professional's presence not be disclosed in advance. Engagement letters are generally addressed to Heads of Services and Staff Offices (HSSOs), Regional Administrators (RAs), or their designee, and are signed by the responsible DAIGA or RIGA. (If appropriate, the letter may be addressed to the Regional Commissioner.

The engagement letter for financial statement audits is signed by the Inspector General and issued to the Administrator and the Chief Financial Officer several weeks prior to audit initiation. Per GAGAS, each OIG is required to communicate with the legislative committees having oversight of their Agency whenever an audit is performed pursuant to a law or regulation. Thus, a notification letter is issued to the appropriate Congressional committees announcing the audit engagement. In addition, a memorandum is issued to the CFO and the Associate Administrator of the Office of Congressional and Inter-Governmental Affairs, notifying them that such letters are sent.

#### 803.06 Audit Survey

Audit surveys are fact-finding processes to quickly gather readily available operational, performance, financial, and other program activity information. The information does not contain detailed data verification of supporting information. The audit team should determine the breadth and scope of the audit with awareness of GAGAS requirements. In cases where the audit team considers previously prepared audit guides, the audit team gathers sufficient survey information to ensure that the objectives, scope, and methodology applied by the audit guide are appropriate

#### 803.07 Audit Plan

Using the information gathered during the audit survey, the audit team identifies the areas with the highest potential return considering the expenditure of audit resources. For the selected areas, audit objectives, scope determinations, and field-testing methodologies are developed and incorporated into a written audit guide. Audit objectives should be stated in a question format. Audit guides broadly address the testing methodologies the audit team applies as the review progresses. As the performance

team obtains information during the survey and fieldwork phases of the review, the team should formulate more specific testing methods. The written audit plan for conducting reviews contains: audit objectives, scope determinations, testing methodologies contained in the audit guide, recorded performance milestones, and staff assignments.

The audit team should send the proposed audit objectives, milestone completion dates, and subsequent changes to the respective DAIGA for review and approval.

For financial statement reviews, the performing team should develop a program that provides for the:

- Evaluation of the IPA's independence and objectivity,
- Evaluation of the IPA's qualifications,
- Evaluation of the IPA's system of quality controls,
- Review of the IPA's audit documentation,
  - o A hybrid of a low and a moderate level of review of audit documentation will be performed in accordance with the Government Accountability Office's (GAO) Financial Audit Manual, Section 650 entitled "Using the Work of Others."
- Performance of supplemental tests (if required).

#### 803.08 Entrance Conference

Performance audit entrance conferences are held with program officials when survey efforts are initiated to ensure agreement regarding the focus of the review, the audit process, contact points for status reporting, and any specific areas of management concern or audit emphasis. DAIGAs are routinely notified several days in advance of each entrance conference so they have the opportunity to participate. Following the survey phase of the review, the audit team should meet with program officials to discuss the audit objectives, scope, and field-testing methodologies. In addition, they will discuss milestones for issuance of the draft report. The audit team should inform the cognizant HSSO or RA of the audit objectives if they are not attending the post survey conference.

Financial audit entrance conferences are held with the IPA and management when the audits are initiated. The OIG/IPA discusses the audit process, contact points for status reporting or Notification of Findings, and any specific areas of management concern or audit emphasis. The OIG/IPA should discuss audit objectives, scope, and field-testing methodologies, as well as milestones for issuance of the draft report.

#### 803.09 Communications with Agency and Other Officials

Audit and oversight team members should maintain a continuing dialogue with management and IPA officials as the audit progresses and hold periodic status meetings with the designated contact point. This dialogue ensures that Agency management is kept informed of the audit progress and any issues that are under audit. The periodic meetings allow for early discussion of potential findings and conclusions, afford managers the opportunity to provide additional information that could be pertinent to the audit results, and allow Agency officials to promptly initiate corrective action. Issues having

material impact upon GSA operations should be immediately brought to the attention of Agency officials using Alert Reports (See Section 806.04) or interim reporting techniques.

### 803.10 Audit Results and Recommendations

When conducting fieldwork, the performance team collects extensive amounts of evidence. The audit team's analysis and conclusions of the evidence serve as the foundation for audit results and recommendations. Conclusions can either support management's actions or show that an activity's operations should be revised.

Reportable results need to be significant and material to warrant inclusion in formal audit reports, which are subject to an extensive resolution process. The elements of a reportable result are: condition, criteria, cause, effect, and recommendation. Audit recommendations should be constructive and directed toward significant performance problems, potential improvements in operations, or instances of noncompliance.

### Tracking the Independent Public Accountant's (IPA) Audit Results

In addition to its audit reports, the IPA is also required to report various matters concerning GSA's internal control structure noted during the audit. The IPA reports its results in the Report on Internal Control, the Report on Compliance with Laws and Regulations, and in management letters. The IPA classifies these results as material weaknesses, significant deficiencies, or control deficiencies. As part of its oversight responsibilities, JA monitors and reports on management's progress in resolving prior year audit findings via the subsequent IPA audit. The Agency's Internal Control and Audit Division tracks IPA recommendations.

### 803.11 Fraud, Illegal Acts, Abuse and Noncompliance with Laws and Regulations

The JA team should not discuss with GSA or contractor officials potentially illegal or improper activities disclosed during audits and reviews. Instead, the team members should refer such activities to the appropriate components, in accordance with the procedures in the OIG Policy and Procedures Manual, Subchapter 705, entitled "Audit Referrals of Potential Irregularities to JI." In addition, possible noncompliance with laws and regulations should be referred to the respective DAIGA or JAO, as appropriate, in order that alternative approaches can be pursued.

### IPA Assessment of Fraud and Illegal Acts, and Noncompliance with Laws and Regulations

The IPA is responsible for properly assessing and evaluating fraud and illegal activities in accordance with Statements on Auditing Standards (SAS) 99, Consideration of Fraud in a Financial Statement Audit. Potentially illegal or improper activities identified during IPA audits should be brought to JA-F's attention, which will then follow the policies outlined in this section.

### 803.12 Computing Funds Put to Better Use and Questioned Costs

Savings that could result from audit efforts should be quantified using the guidance from GSA's Internal Audit Followup Handbook (ADM P 2030.2C), and from JA position papers.

The calculation of funds put to better use should be based on one-time savings for operational improvements or single year savings for multiyear improvements identified from performance audits. Also, the potential impact of the calculated funds put to better use on the Agency's budget should be determined.

Questioned costs refer to a computed refund amount that is owed the Government.

The calculation and amount of the funds put to better use and questioned costs are shown in the Management Decision Record for Internal Audit. This document becomes part of the audit resolution process that the Agency and the OIG are responsible for monitoring.

#### 803.13 Exit Conference

Although a continuing dialogue during the audit should minimize any surprises, the audit team holds exit conferences with management officials at the conclusion of the audit. At the exit conference, the audit team communicates the results of the audit, including potential results and recommendations. The conference also serves as a forum to elicit management's views regarding reported facts, potential results, and recommendations. The conference offers officials the opportunity to provide information that may affect the conclusions reached by the audit team. While the HSSO, RA, and program managers are usually invited to or receive exit conference materials, regional protocols should be considered to the extent possible. To ensure his/her participation, the respective DAIGA should also be given ample advanced notice of all exit conferences.

Audit results can be communicated using a fact sheet/PowerPoint briefing, or by providing management an "advance draft" of the report. If the "advance draft" is used, then the respective DAIGA should review it prior to the exit conference. Advance drafts should be transmitted via email or hand delivered with a routing slip prior to the exit conference, noting that the OIG is soliciting management's oral comments at the exit conference prior to finalizing the official draft report for formal written comments.

The financial audit oversight team holds exit conferences with the IPA and management officials at the conclusion of the audit to communicate the audit results and recommendations. The conference also serves as a forum to elicit management's views regarding reported facts and potential findings and recommendations, and provide officials the opportunity to provide information that may impact the IPA's conclusions.

#### 803.14 Project Cancellation

If at any time during the review process the audit team concludes that a project should be canceled, the RIGA should inform the respective DAIGA to the rationale for canceling the project. The DAIGA will notify the PDAIGA and JAO Director of the cancellation. The audit team will issue a closeout report to management outlining the nature, scope, and results of the work performed, and advising that no further effort is contemplated. In addition, the report should respond to any concerns raised by management officials during the audit.

Effective Date 1/22/2010

## 804.00 EXTERNAL REVIEWS

### 804.01 General

The Office of Audits performs external reviews (also referred to as contract reviews) to assist contracting officials in the negotiation, award, re-pricing, administration, and settlement of contracts. External reviews generally follow GAGAS, the American Institute of Certified Public Accountants (AICPA) Standards for Attestation Engagements, as well as the policies and procedures described herein. GAGAS incorporates and expands on the AICPA's general, fieldwork, and reporting standards for attestation engagements.

Attestation engagement standards from GAGAS are summarized as follows:

The general standard states that the subject matter is capable of evaluation against suitable and available criteria.

The eight fieldwork standards cover adequate planning and supervision; sufficiency of evidence; auditor communications with responsible parties; evaluating previous audits and attestations; requiring an understanding of internal controls for examination level engagements; requiring reasonable assurance for examination level engagements; developing elements of the findings; and, documentation.

The nine reporting standards cover what needs to be included in the attestation report. These are: identification of the subject matter; auditor's conclusion about the subject matter; the auditor's significant reservations (if any) about the subject matter; who the report is intended to be used by; cite auditor's compliance with GAGAS; reporting deficiencies in internal controls, fraud, illegal acts, contract violations, and abuse; reporting views of responsible officials; how to report confidential/sensitive information; and, distribution of the report.

Most of the GAGAS standards listed above are based on the AICPA Statement on Standards for Attestation Engagements (SSAE) No. 11, effective June 1, 2001. SSAE No. 11 describes the types of attestation engagements, and limits what can be done under each attestation type or level. An attestation engagement can be performed at one of three levels (from highest to lowest): examination, review, or agreed-upon procedures.

JA currently performs all contract work at the review but will change to the examination level effective for audits starting April 2010. Specific guidance will be issued at a later date.

### 804.02 Types of External Reviews

The Office of Audits' external reviews include:

Preaward reviews are performed to assist contracting officers in negotiating prices for goods and services acquired by the Government. Preaward reviews include claims.

Postaward reviews are performed to assist contracting officials in administering contracts and ensuring that the Government receives contracted goods and services from suppliers. Accordingly, these reviews

seek to determine the propriety, validity, and reasonableness of reimbursable cost submissions, the accuracy of contract information provided by the contractor, or compliance of the contractor with contract provisions. Included in this category are limited scope overbilling reports that could be prepared as a separate report from the main preaward report.

#### 804.03 Identification of External Reviews to be Performed

The process of identifying the external reviews to be performed is the responsibility of the Contract Audit Office. JA-C also has oversight responsibility for the coordination and execution of all external reviews performed in the Office of Audits.

The process for selecting which reviews will be accomplished varies depending on the type of external review. Preaward MAS reviews are identified by JA-C in coordination with JAO, RIGAs, and the Federal Acquisition Service (FAS). The list of preaward MAS reviews scheduled to be performed is distributed by JA-C to JAO, RIGAs and FAS. Postaward reviews, claims reviews, qui tams, hotline complaints, Congressional inquiries, and additional preaward reviews are typically performed as they are identified. Postaward reviews can be initiated by JA, or can be requested by contracting officers. In addition, GSA's Office of General Counsel can request that JA review contractors' claims. Generally, the decision to perform an external review is made by the RIGA in coordination with JA-C, keeping in mind the organizational goal for resource allocation to external reviews.

Occasionally, JA receives additional requests for external reviews not previously identified or planned. These requests originate from FAS officials, contracting officers and other sources. JA-C coordinates these unplanned requests to determine if they can be supported. When evaluating these requests, JA-C considers the following options: (1) coordinate with RIGAs to reprogram JA resources to perform the review; (2) coordinate with the Defense Contract Audit Agency (DCAA) to perform the review (this option will be considered only if DCAA has the expertise to perform the type of review requested); or (3) waiving the review.

#### 804.04 Initiating External Reviews

Contracting officials and JA professionals generally initiate MAS preaward reviews 210 days prior to the expiration date of the contract option. JA professionals work closely with FAS contracting officials while conducting preaward reviews. FAS has issued Procurement Information Notices (PIN) to its contracting staff (e.g., PIN 2006-02 dated September 22, 2006) that explain the contracting officer's responsibilities in the preaward review process.

Other external reviews are initiated at the discretion of the RIGA, in coordination with JA-C, keeping in mind the organizational goal for resource allocation to external reviews.

Before commencing an external review, the JA professional should determine if the contractor's submission is complete. If not complete, the JA professional should work with the contractor and contracting officials to obtain the information necessary to perform the review. Refer to JA audit guides and JA position papers for specific guidance in these areas.

#### 804.05 Engagement Meetings and Discussions with Contracting Officials

Once the decision is made to commence a review, an engagement meeting or discussion is held with contracting officials to clarify the focus of the review effort, determine any special requirements or areas of interest, establish due dates for providing results, and request any technical assistance or analysis needed. While a formal meeting with contracting officials is preferable, telephone or video conferences are acceptable if a face-to-face meeting is not practical. The external review proceeds when performance terms agreeable to the audit team and contracting official are achieved.

When performing external reviews, early and continual communication with contracting officials is essential so the impact of material inaccuracies, incomplete submissions, and contractor delays can be considered. However, care should be taken not to discuss potential fraud, illegal acts, noncompliance matters and abuse. In accordance with OIG Policy and Procedures Manual, Subchapter 705, entitled "Audit Referrals of Potential Irregularities to JI," these issues should be referred. Contracting officials can provide valuable pricing information and help identify issues that may enhance the value of the external review results during negotiations.

#### 804.06 Conferences with Contractor Personnel

Entrance conferences are held with the contractor to discuss the external review process, arrange for access to required records, and determine a point of contact for data requests. During the review, meetings are held with contractor personnel to obtain a complete understanding of proposed and disclosed pricing and to determine whether deficiencies exist. While the JA professional should disclose material duplications, omissions, or math errors, the JA professional should not prematurely discuss material inaccuracies or other exceptions with the contractor.

Upon completion of the fieldwork, an exit conference is held with the contractor. At this conference, the JA professional discusses the factual information obtained during the review and any outstanding issues, and obtains the contractor's comments to the areas discussed. However, information impacting negotiations or indications of potential fraud or abuse should not be discussed.

#### 804.07 Access to Contractor Records

Access to the contractor's records is provided for by statute, contract terms, and agreement between the contractor and contracting officials. In addition to specific access provisions contained in the contract under review, the General Services Administration Acquisition Manual outlines the examination clauses for contracts subject to review.

In instances where the contractor denies access to accounting and other records, the JA professional should immediately contact the audit manager so that appropriate actions can be taken. Actions to be considered include contacting other company officials, GSA contracting officials, JA-C, and the Counsel to the Inspector General.

#### 804.08 Standard Report Objectives for External Reviews

Preaward MAS (Products): The objectives of the review were to determine whether: (1) the Commercial Sales Practices (CSP) information submitted by the company is current, accurate and complete; (2) the company's sales monitoring and billing systems ensure proper administration of the price reduction

provisions and billing terms of the contract; and, (3) the company adequately accumulates and reports schedule sales for Industrial Funding Fee (IFF) payment purposes.

Preaward MAS (Services): In addition to the three listed objectives for preawards of products, preawards of services contracts add the following objectives:

(4) employees assigned to work on task orders placed under the GSA schedule are qualified for the billable positions; and (5) the company has an adequate accounting system for the segregation and accumulation of labor hours, material costs, and other direct costs on time and material task orders.

Postaward MAS (Products): The objectives of the review were to determine whether: (1) the company complied with the price reduction clause and billing provisions of the contract; and (2) all GSA schedule sales were accurately compiled and reported in accordance with the Industrial Funding Fee (IFF) provisions of the contract.

Postaward MAS (Services): In addition to the two listed objectives for postawards of products, postawards of services contracts add the following objectives:

(3) the hours billed to government customers on time and material (T&M) task orders are adequately supported with appropriate labor time-keeping records; and (4) the employees' qualifications meet or exceed the contractual requirements for the labor disciplines offered and billed on the task orders.

Cost or Pricing Reviews: The objectives of the review were to determine whether the cost or pricing data submitted in the proposal were fairly presented, supported by appropriate cost records, and prepared in accordance with the cost principles set forth in the Federal Acquisition Regulation (FAR) and the provisions of the GSA contract.

Regulation and/or guidance in evaluating specific contract issues may be found in the FAR, Cost Accounting Standards, DCAA Contract Audit Manual, Federal Acquisition Service's guidance, GSA OIG Audit Guides and JA's position papers. For example, FAR 31.205-1 to 31.205-52 discusses cost reasonableness and the allowance for and allocation of selected costs.

#### 804.09 Scope of External Reviews

The scope of an external review is based on the subject matter of the review and how it relates to the review objectives. The following two areas can greatly impact the external review's scope of work. As of April 2010, the audits will be performed at the examination level and additional instructions will be issued.

#### Internal Controls

For attestation engagements at the review level, GAGAS does not require an understanding of internal controls, so no review steps are required. As such, no reference to internal controls in the review report is necessary.

#### Fraud, Illegal Acts, Contract Violations and Abuse

Attestation engagements performed at the review level do not require “reasonable assurance” for detecting fraud, illegal acts, contract violations and abuse. (The terms “reasonable assurance” is based on AICPA auditing standards.) GAGAS also makes it clear that the JA professionals’ general responsibilities include limiting exposure to fraud, waste, mismanagement and abuse. However, the amount of planned work in this area varies depending on the type of audit assignment.

If, however, during the course of the engagement, information comes to the JA professionals’ attention indicating that fraud, illegal acts, or violations of provisions of contracts may have occurred, they should perform additional procedures. These procedures include determining if fraud, illegal acts, or contract violations are likely to have occurred and, if so, determine how these acts affect the review engagement.

JA professionals are responsible for being knowledgeable about fraud indicators and to pursue such indicators in all the work that JA performs. The IG Act of 1978 broadly covers the IG’s responsibility for detecting and preventing fraud and abuse in Agency programs and operations. Where fraud, waste and/or abuse are suspected, the JA professional should follow the procedures described in OIG Policy and Procedures Manual, Subchapter 705, entitled “Audit Referrals of Potential Irregularities to JI.” The potential irregularities should not be discussed with, or disclosed to, Agency or contractor officials. If it appears necessary to discuss such issues with contracting officials, then the Office of Investigations and Office of Counsel to the Inspector General should be contacted to ensure that an appropriate course of action, agreeable to all OIG components, is pursued. Possible noncompliance with laws, regulations, or contract provisions should be referred to JA-C so that alternative approaches can be pursued.

#### 804.10 GAGAS Statement for All External Reviews

The standard GAGAS statement is as follows:

Our review was conducted at (contractor’s name) offices located in (location), in accordance with generally accepted government auditing standards. The scope of a review is less than that of an examination. An examination would require an opinion regarding the acceptability of the offer for negotiation purposes and an assessment of the company’s internal control structure. Accordingly, we are not expressing any such opinion; instead, we are providing information relative to our review objectives to assist the contracting officer in the negotiation process.

#### 804.11 Negative Assurance Statements

JA professionals perform sufficient testing during external reviews to express a conclusion about whether any information came to their attention that indicates that a contractor’s submission is not presented (or fairly stated) in all material respects. External reviews usually contain negative assurance statements to contracting officials with regard to the material accuracy and completeness of contractor costs, submissions, proposals, or claims.

- Unqualified Negative Assurance – During the course of our review, nothing came to our attention that would affect the contracting officer’s determinations as to whether the proposal is acceptable for negotiation purposes.

- Qualified Negative Assurance – During the course of our review, except as noted above, nothing additional came to our attention that would affect the contracting officer’s determinations as to whether the proposal is acceptable for negotiation purposes.
- Adverse – The cumulative effect of the matters discussed in the following paragraph(s), and detailed in the results section of this report, may impact the contracting officer’s ability to effectively use the contractor’s proposal to negotiate an acceptable contract.

It is important to distinguish between negative assurance and positive assurance. Positive assurance is characterized by the JA professional’s opinion and can only be expressed if the attestation engagement is performed at the examination level. Since we currently conduct review level engagements, the expression of an opinion in our report could be misleading and lead readers to think that the more comprehensive level of an examination engagement was done. Furthermore, work done in accordance with review level standards can only be referred to as a “review”, not as an audit or examination.

#### 804.12 Reporting Views of Contractors

GAGAS provides that the views of responsible officials of the reviewed entity be included in the final report. For external reviews the discussion of certain results are limited in accordance with 804.06. The discussion is limited to factual information obtained during the review, outstanding issues, and the contractor’s comments. The contractor’s comments should be incorporated into the final report for the contracting officer to address. Verbal comments are acceptable as long as adequately documented. Section 806.01 addresses instances where draft reports are used to obtain formal written comments for postaward review results.

#### 804.13 Referring Preliminary Results to Contracting Officials

When a contracting officer requests review results before a report can be finalized, preliminary information can be furnished orally by the audit manager and supplemented by reviewed draft report appendixes or copies of fieldwork documentation (see section 805.06). If a decision is made to provide a preliminary draft of the review report, the JA professional should ensure that the contracting officer understands that the draft is not a final product and therefore subject to change. All pages of a preliminary draft report and any preliminary information provided to the contracting officer should be clearly labeled as draft.

#### 804.14 Computing Funds Put to Better Use and Questioned Costs

Savings that could result from review efforts should be quantified using the guidance from GSA’s Internal Audit Followup Handbook (ADM P 2030.2C) and JA position papers.

When determining potential funds put to better use savings, the calculation should be based on savings over the remaining contract period covered by the review report. The computation is based on what the Government could save in the future if the contract pricing was negotiated to reflect the information in the review report.

Questioned costs refer to a computed refund amount that the contractor owes the Government. Questioned costs result from postaward or overbillings review reports.

The calculation and amount of the funds put to better use and questioned costs are shown in the Decision Record for External Review. The basis for these amounts should be explained in the report and clearly shown in the decision record. This document becomes part of the audit resolution process that the Agency and the OIG are responsible for monitoring.

Effective Date 1/22/2010

## 805.00 DOCUMENTATION SUPPORTING AUDITS AND REVIEWS

### 805.01 Definition and Purpose of Documentation

Audit documentation is recorded information showing the planning, performance, and reporting of an audit or external review. It constitutes the principal record of the work that JA professionals have performed in accordance with standards and the conclusions that these professionals have reached. Documentation can include schedules, papers, analyses, interviews, correspondence, and other materials obtained, prepared, or collected during the review process. These materials become documentation when the reviewer approves and signs off on them. They can be in an electronic form or contained in a paper-based documentation file.

Documentation is the link between project planning, fieldwork execution, and the final report product. As such, documentation is a record of the audit procedures applied during the audit assignment. The form and content of documentation should be designed based upon the circumstances of the particular audit assignment. Documentation also serves as the essential element of audit quality by: providing the principal support for JA professionals' report, aiding the professionals in conducting and supervising the audit, and allowing for the review of audit quality. As such, documentation should contain sufficient information to enable an experienced JA professional, having no previous connection with the audit or review, to ascertain that the evidence supports the judgments and conclusions included in issued reports.

### 805.02 Electronic Documentation

JA uses CCH® TeamMate (TeamMate) as the method for documenting audit evidence in electronic format. The use of TeamMate is required for all performance audits, financial audits, and external reviews. Exceptions to this policy must be approved by the PDAIGA and should be submitted through the JAS Director for consideration.

The following discusses the policies related to performing backups of electronic audit documentation in TeamMate, indexing paper-based (or hardcopy) documentation that is used in conjunction with TeamMate, and the finalization of TeamMate files. More specific TeamMate guidance can be found in JA's document entitled "Protocol for Using TeamMate EWP."

Backing up electronic audit documentation is essential. TeamMate will allow several versions of backups. JA professionals will maintain at least two backup versions. When working in the field remotely, the JA professional will back-up the audit or review (replica) daily and keep the backup file in a location separate from the replica file. In the office, the JA professional will back up the audit daily to a file location separate from the master file location. Teams may need to maintain some hardcopy (HC) documentation outside of TeamMate. HC documents might include regulations, contracts, sensitive documents, large graphic files, or databases. In the case of HC documents maintained outside of TeamMate, use the following naming convention: preface the document index with "HC-".

TeamMate files are to be finalized within five working days after issuance of the final report. The TeamMate file should be backed up, finalized, and moved to the Finalized tab. The finalized TeamMate

file should contain all of the information and analyses supporting the issued report. Any activity subsequent to report issuance, including additional analysis, copies of signed MDR, DR, price negotiation memorandum (PNM), agency action plan, etc., will be maintained in a separate file – a backup copy of the finalized file – which will then become the current “working” file.

#### 805.03 Instant Messaging

Instant Messaging shall not be used to conduct official business. Further, instant messages shall not be maintained in our official system of records. Instant messages and instant messaging histories should be deleted (see Section XXX).

#### 805.04 Paper-Based Documentation

When using paper-based methods to document audit evidence, either in conjunction with TeamMate or in a standalone fashion when authorized, the following should be observed.

Documentation files should be consistent in physical size, binding methods, sectional identification, and exterior labeling techniques.

Each page of documentation should contain a project number and title; each page should show the preparer and preparation date, reviewer and review date; and show the source of documentation data.

Major documentation sections should explain the purpose and scope of the review effort and summarize the conclusions or judgments reached.

#### 805.05 Paper-Based Documentation Index Format

The index format described herein is to be used only when TeamMate is not used as the primary methodology for documenting audit/review evidence. The format follows a sectional methodology, where the first four sections of the paper-based evidence trail are considered mandatory. These mandatory sections contain materials that are common to all work projects and are indexed as follows:

Documentation Section	Index
Audit/Project/Review Reports	A
Conferences and Correspondence	B
Audit/Project/Review Guidance	C
Audit/Project/Review Follow-up	D

Optional documentation sections should continue the alphabetical index and as such follow the mandatory sections. The optional sections address the specific review objectives by recording the work conducted, such as: materials gathered, analyses performed, conclusions reached, etc.

Any data maintained by the JA professional during the audit or external review outside of the stored methodologies described herein are considered “administrative.” Such administrative data, which may contain useful information for the duration of the JA assignment, is not considered part of the official documentation file. However, if the audit or external review has been identified by the U.S. Department of Justice as part of a litigation hold, this information must be retained (see section 805.07).

#### 805.06 Supervisory Review of Documentation

Audit managers or designated senior JA professionals monitor work efforts and review documentation prepared by team members throughout the fieldwork process. This includes working with performance team members to ensure that instructions are fully understood and followed for gathering data; analyses and tests are adequately performed; and finalized results are recorded as documentation, as described in sections 805.2 through 805.4. Supervisors should record decisions made and instructions given regarding the review process. This ensures that compliance can be validated during subsequent supervisory or quality control reviews.

Supervisory reviews of completed analyses, tests, and determinations should ensure that appropriate evidence or information exists to support significant findings, conclusions, observations, recommendations and/or alternatives. Managers and senior JA professionals should record supervisory reviews in either the electronic (TeamMate) or paper-based documentation formats. The document should include responses by the team members and final determinations by the supervisory reviewer. Supervisory review must be completed for all documented evidence that supports the report's findings and conclusions prior to report issuance. All other documented evidence must be reviewed prior to final report issuance.

#### 805.07 Access to Documentation and Safeguarding Information

Documentation, prepared in accordance with sections 805.2 through 805.4, is considered an official government record and team members must safeguard it in accordance with existing legal and administrative requirements. They must take care to ensure that documentation is not lost, stolen, altered, destroyed, or accessed by unauthorized persons. Material obtained during the review may be proprietary contractor information or contain sensitive program data. Team members should not leave documentation unattended or unsecured. In addition, team members should not make the documentation available outside of JA without the knowledge of JA management. Additional guidance is provided in the OIG Policy and Procedures Manual, Subchapter 505.

If documentation must be released, the audit team should stamp each individual page of documentation or file section released "AUDIT CONFIDENTIAL." Then the audit team should transmit a memorandum advising that the materials should not be disclosed without written approval from the releasing OIG official.

#### 805.08 Maintenance and Disposition of Official Files

Electronic Documentation - TeamMate files are electronic records. As such the maintenance and disposition of the files must be in accordance with Title 36, Code of Federal Regulations, Part 1234 – Electronic Records Management, and GSA Order OAD P 1820.1, GSA Records Maintenance and Disposition System, or its successor.

Once the final audit report is issued, the Finalized TeamMate Audit file should be transferred to a CD-ROM through the TeamMate backup process. Two additional backups on CD-ROM also should be maintained.

- The first CD-ROM backup of the audit is the official TeamMate version of the audit. Each audit office is responsible for storage of the CD-ROM in a safe and secure environment, for eight years following the

end of the fiscal year in which the audit is closed. ScanDisk or similar software should be used on a periodic basis to ensure the integrity of the CD-ROM after the third year of storage and every year thereafter. This CD-ROM can be destroyed eight years after the audit is closed.

- The second CD-ROM backup of the audit is to be forwarded to and maintained by JAS for eight years following the end of the fiscal year in which the audit is closed. ScanDisk or similar software will be used on a periodic basis to ensure the integrity of the CD-ROM after the third year of storage and every year thereafter. This CD-ROM can be destroyed eight years after the audit is closed.
- The third CD-ROM backup of the audit should be filed with the hardcopy documentation. At the end of the fiscal year in which the audit is closed, hold the hardcopy documentation and this CD-ROM for two years and retire to the Federal Records Center. The hardcopy documentation and this CD-ROM will be maintained and destroyed in accordance with Federal Records Center regulations.

#### Paper-Based Documentation

The field audit offices are responsible for maintaining and disposing of official audit and project files in accordance with GSA Records Schedule 03A025a, or its successor. That schedule is available through the web on Insite at GSA Records Schedule 03A025a or through JC. Official files consist of the final reports, documentation, and related correspondence.

Financial and performance audit project files are closed upon receipt of notification that the action plan has been fully implemented. External review files are closed upon receipt of documentation showing management's determination to recover funds or avoid their expenditure.

Generally, closed files are retained in the field audit office for two years from the end of the fiscal year in which the case is closed; then files are retired to the Federal Records Center (and destroyed six years later). Closed files will be retained in the field audit office (and not sent to the Federal Records Center) under the following circumstances:

- an implementation review is scheduled or will be scheduled;
- the files relate to an ongoing investigation or ongoing litigation;
- the files relate to a significant audit that is expected to generate continued inquiries from parties outside the OIG; or,
- the files relate to specific audits or reviews that have been identified by the U.S. Department of Justice as part of a litigation hold.

Effective Date 1/22/2010

## 806.00 DRAFT AND FINAL REPORTS

Draft and final reports are prepared for internal audits. However, while most external reviews only require a final report, there are instances when a draft report is prepared for selected external reviews. The following describes the processes used to prepare draft and final reports for both internal audits and external reviews.

### 806.01 Draft Reports

#### Draft Reports for Internal Audits

Discussion draft report (optional) – Even though management officials are normally kept apprised of identified issues during the review, the discussion draft report is the first formal document that provides a written description of the JA audit team’s results and the potential impact to the Agency and/or its operations. Given to management officials prior to the exit conference, the discussion draft is not only used to facilitate discussion at the exit conference but also to elicit verbal or written comments. Since management will have another opportunity to officially comment on the report prior to final report issuance, the comment period for a discussion draft report should be limited to not more than 7 days.

While discussion draft reports do not need to be prepared in the format used for the “official draft report,” doing so allows management to identify any misperceptions or errors that can easily be corrected when preparing the official draft. Such reports do not normally contain recommendations, a signature page or a distribution appendix. In addition, the title page of the discussion draft report should include the draft restrictive notice (See section 806.05). Also, “DISCUSSION DRAFT - FOR OFFICIAL USE ONLY” should be placed at the top and bottom of every page.

The DAIGA/RIGA should review the discussion draft report and ensure it is referenced before it is released electronically to the appropriate management officials. The discussion draft report is strictly an exit conference tool and should not be further disseminated without the AIGA’s approval.

Official Draft Report (mandatory) - This formal draft report contains recommendations that are transmitted by the DAIGA/RIGA to the Heads of Services and Staff Offices (HSSOs) and/or Regional Administrators (RAs). This allows the audit team to receive management’s official written comments and incorporate them into the final report. The respective DAIGA/RIGA should review the official draft report and ensure it is referenced before it is released to management officials. The AIGA transmits draft reports to the Administrator or to officials external to the Agency.

Official draft reports are issued with white covers, and transmitted by cover letter requesting that comments be submitted within 30 days. Unlike final reports, official draft reports do not contain a signature page or a distribution appendix. If audit results and recommendations are presented in a PowerPoint format, the official draft report should include a title page and letter report summarizing the results with the PowerPoint presentation included as an appendix. In addition, the title page of the official draft report should include a restrictive notice (See section 806.05). Also, “DRAFT - FOR OFFICIAL USE ONLY” should be placed at the top and bottom of every page.

Since final audit results are to be made publicly available (unless restricted by law or regulation), DAIGAs/RIGAs and their respective audit managers are responsible for ensuring that the official draft report does not contain privileged or confidential information. The audit team should present official draft reports in such a manner that non-technical users can readily comprehend the fundamental nature of the reported facts, analysis, and conclusions. Having a “cold reader” review the official draft report before release is an effective and proven technique to improve report quality.

When the DAIGA/RIGA restricts a performance audit report, the audit team should include the determination as part of the audit documentation. The audit team should notify the AIGA of the determination before the final report is issued.

#### Draft Report for Selected External Reviews

Two scenarios typically arise that call for the issuance of draft reports for specific external reviews.

- Claims that are requested by the GSA’s Office of General Counsel, other litigation authority, or before the Board of Contract Appeals may be issued as a white cover draft report. Copies of the draft report should be issued to the requesting official, the Office of Counsel to the Inspector General and the Contract Audit Office.
- Postaward reviews with indications that potential civil and/or criminal fraud is present are typically issued as a white cover draft report to the Office of Counsel to the Inspector General and the Contract Audit Office. The Office of Counsel to the Inspector General will evaluate the issues identified in the report, and determine if the report should be forwarded to the U.S. Department of Justice. If the decision is made to resolve the issue administratively, the DAIGA/RIGA should discuss the issues with the contracting officer. If the contracting officer has no administrative concerns, a white cover draft report is transmitted to the contractor to obtain a written response, with a copy to the Contract Audit Office.

The format for draft reports is the same as for final reports, except that draft reports do not contain a signature page or a distribution appendix. Such reports are also issued with white cover and include restrictive clauses, as identified in section 806.05. However, the above procedure does not apply to limited scope overbillings reports. These reports are issued in red cover directly to the contracting officer for resolution. They also require electronic distribution to the immediate office of the Inspector General (See section 806.07 for details).

Under both scenarios, when the identified results in the draft report are finally settled or the contractor’s response is received, a final red cover report is issued to the cognizant contracting officer together with a Decision Record (DR). Since the contracting officer does not need to respond to results that have been settled, the DR should be noted accordingly. Alternative scenarios should be discussed with the Contract Audit Office.

#### 806.02 Independent Public Accountant (IPA) Draft Reports

IPA audit reports containing recommendations are transmitted by the DAIGA to the Chief Financial Officer in draft form requesting official written comments within three days for incorporation into the final audit report. Draft reports should be reviewed by the cognizant DAIGA.

## 806.03 Final Reports

Final reports are used to convey internal audit findings and external review results to GSA officials along with recommendations and information for improving Agency operations or contracting activities. Written reports facilitate management actions as well as provide an avenue to follow-up on actions taken. However, unlike internal audits, preaward MAS external reviews are advisory in nature and do not contain recommendations. In addition, as preaward reviews support contract negotiations and re-pricing and costs potentially under litigation, the JA does not issue final reports to the contractor or their representatives. However, contracting officials can release (with the JA's concurrence) these reports to the contractors.

## 806.04 Types of Final Reports

The results of financial and performance audits are issued in the format of either a standard or letter report. Further, there may be instances when a need arises to communicate quickly with management on an issue. This may be done through an interim or alert audit report. External reviews are issued as standard or letter reports. Standard, letter, interim, and alert reports are defined below.

Standard Reports are issued in accordance with prescribed formats to convey audit and external review results. Standard reports address complex issues or comment upon multiple concerns. Prescribed formats ensure that reported conditions are logically and consistently presented.

Letter Reports are issued in memoranda format when audit or external review results, generally without findings, can be presented in five pages or less (excluding the title page, appendices, and the Management Decision Record). Internal audits and external reviews without recommendations are usually issued as letter reports.

This type of report can also be used to close out a review at the end of the survey phase, when the decision is made not to do further audit/review work. (See Section 803.04 – Survey Assessment Meeting).

Interim or Alert Reports are typically issued when significant internal audit concerns need to be conveyed to GSA officials before the completion of an ongoing audit assignment. Due to the nature of the concern, these reports do not contain formal recommendations, but focus on notifying GSA officials of the weakness or deficiency identified. The final report is issued under orange cover and is required to notify management that the noted weakness or deficiency will be incorporated in the final (green or red cover) audit report.

Such reports go through an expedited draft and final report process. Draft alert reports (white cover) are transmitted to GSA officials shortly before an interim exit conference with management. As with any draft report, it is used to elicit comments from management that will be included into the final alert report.

These reports are issued in either the standard or letter report format, are assigned a sequence number, must comply with GAGAS, and be referenced prior to draft issuance. These reports are distributed in the same manner as unrestricted or restricted reports, except that Management Decision Records are not used. Final unrestricted reports are posted on both the OIG public website and the OIG intranet. Restricted reports are posted to the OIG intranet only.

Other Memoranda – occasionally the need arises to communicate a concern when a full audit has not been conducted. These concerns can be communicated to management through memoranda. This provides management with preliminary observations on matters needing timely attention and action. Compliance with GAGAS and referencing the memoranda contents are decided on a case by case basis with concurrence by JAO.

#### 806.05 Report Format and Content

Report format and content requirements are as follows:

- Required and Optional Sections for standard and letter reports are shown in Figure 807-01. Report sections start on separate pages and, where applicable, are centered, capitalized, and underlined. Subsections are identified by lower case side captions that are not underlined.
- Report Covers distinguish the type of report. All reports with restrictive designation are issued with red covers.
- “FOR OFFICIAL USE ONLY” is placed at the top and bottom of each page of all draft reports, final external reviews, and final performance/financial reports that contain information that are restricted or should not be distributed to the public.
- Report Titles are centered within the report cover window. The title is capitalized and includes the audit number, sequence number, and issuance date.

External review report titles also identify the solicitation or contract number, and contract period, if appropriate. Standard titles for external reviews are summarized below:

PREAWARD REVIEW OF  
MULTIPLE AWARD SCHEDULE  
CONTRACT EXTENSION  
ABC CORP.  
CONTRACT NUMBER GS-35F-1234J  
REPORT NUMBER A040000/F/3/X11111

REVIEW OF MULTIPLE AWARD SCHEDULE  
CONTRACT NUMBER GS-35F-1234J  
FOR THE PERIOD MARCH 14, 1999 TO  
JULY 31, 2004  
ABC CORP.  
REPORT NUMBER A040000/F/3/X11112

REVIEW OF A CLAIM  
ABC CONSTRUCTION CORP., INC.  
CONTRACT NUMBER GS-02P-99-DTC-0006  
REPORT NUMBER A040000/P/2/X11111

PREAWARD REVIEW OF CHANGE ORDER PROPOSAL  
ABC CONSTRUCTION CORP., INC.

CONTRACT NUMBER GS-02P-99-DTC-0006  
REPORT NUMBER A04000/P/2/X11111

PREAWARD REVIEW OF ARCHITECT ENGINEER PROPOSAL  
ABC DESIGN INDUSTRIES, INC.  
CONTRACT NUMBER GS-02P-99-DTC-0006  
REPORT NUMBER A04000/P/2/X11111

PREAWARD REVIEW OF TERMINATION  
SETTLEMENT PROPOSAL  
ABC CONSTRUCTION CORP., INC.  
CONTRACT NUMBER GS-02P-99-DTC-0006  
REPORT NUMBER A04000/P/2/X11111

- Dissemination Notice for Unrestricted Draft Reports - Draft financial and performance audits, and include the following dissemination notice on the bottom of the title page:

This draft report has been prepared by and is the property of the Office of Audits, Office of Inspector General. It was prepared by the staff as a basis for obtaining advance review and comment by those having responsibilities concerning the subjects addressed in the draft. It has not been fully reviewed within the Office of Inspector General and is, therefore, subject to revision.

Copies of the report are provided to Agency personnel for official purposes only and should not be disseminated further. Agency officials who receive requests to release this report to anyone outside the General Services Administration should refer the requestor to the Office of Inspector General, Office of Counsel – Freedom of Information Officer.

- Restrictive Notices for Draft and Final Reports – Audit reports and other products that are restricted by law, regulation or content that should not be disseminated to the public have restrictive notices placed on the bottom of the report title page. This includes all draft and final external reviews and performance and financial audits, when restricted; and other restricted reports, as follows:

#### PREAWARD EXTERNAL REVIEWS AND CLAIMS

This report contains information that the Office of Inspector General has determined is \*\*\* (use “proprietary and pre-decisional”, “classified” “or other designations, as appropriate) and distribution is restricted to Agency officials and other cognizant Federal officials. The Office of Inspector General has no objection to the release of this report, at the discretion of the contracting officer, to authorized representatives of (insert name of contractor or subcontractor to which the report pertains). Persons disclosing this information publicly or to others not having an official need to know are subject to possible administrative or civil penalties, or criminal penalties pursuant to the Trade Secrets Act (18 U.S.C. Section 1905).

This report should be safeguarded to prevent improper disclosure at all times. Agency officials who receive requests for the report from other than (insert name of contractor or subcontractor to which the report pertains) should refer the requestor to the Office of Inspector General, Office of Counsel – Freedom of Information Officer.

## POSTAWARD EXTERNAL REVIEWS

This report contains information that the Office of Inspector General has determined is \*\*\* (use “proprietary and pre-decisional”, “classified”, “or other designations, as appropriate) and distribution is restricted to Agency officials and other cognizant Federal officials. Persons disclosing this information publicly or to others not having an official need to know are subject to possible administrative or civil penalties, or criminal penalties pursuant to the Trade Secrets Act (18 U.S.C. Section 1905).

The Office of Inspector General does not want this report released without prior approval from the Office of Inspector General’s Office of Counsel. Accordingly, this report should be safeguarded to prevent improper disclosure at all times. Agency officials who receive requests to release this report, including requests from (insert name of contractor or subcontractor to which the report pertains), should refer the requestor to the Office of Inspector General, Office of Counsel – Freedom of Information Officer.

## DRAFT AND FINAL PERFORMANCE AND FINANCIAL AUDIT REPORTS, AND OTHER AUDIT PRODUCT REPORTS

This report contains information that the Office of Inspector General has determined is \*\*\* (use “proprietary and pre-decisional”, “classified”, “or other designations, as appropriate) and distribution is restricted to Agency officials and other cognizant Federal officials. Persons disclosing this information publicly or to others not having an official need to know are subject to possible administrative or civil penalties, or criminal penalties pursuant to the Trade Secrets Act (18 U.S.C. Section 1905).

This report should be safeguarded to prevent improper disclosure at all times. Agency officials who receive requests to release this report should refer the requestor to the Office of Inspector General, Office of Counsel – Freedom of Information Officer.

## 806.06 Referencing

Referencing is a detailed, documented, independent review of all internal audits and external reviews (both draft and final) and supporting documentation by a JA professional not associated with the assignment.

Referencing confirms that sufficient and appropriate evidence exists as documentation to support reported results and conclusions. The referencer’s primary responsibility is to assure that an experienced JA professional, having no previous connection to the review, could reach the same conclusions based upon an objective interpretation of the data characterized in the audit documentation. It is important to remember that accurate indexing is the responsibility of the audit team, however, it is the referencer’s responsibility to check these indexed cites to ensure they adequately support the facts in the report.

The DAIGA/RIGA designates the referencer and ensures that draft and final reports have been referenced by a grade GS-12 or above JA professional before transmitting them to management officials. If there is a disagreement between the audit team and the referencer that cannot be resolved, the DAIGA/RIGA makes the final decision.

The manual referencing process is documented by completion of a referencing worksheet. This worksheet records the referencer's points or comments and the audit team's response to the points. Upon completion of the referencing process, the referencer and audit manager must physically sign and date the first page of the referencing worksheet.

In those instances where the DAIGA/RIGA had to resolve issues, the decision is annotated on the referencing worksheet, and initialed and dated by the DAIGA/RIGA. The referencing worksheet remains with the documentation file.

When TeamMate is used for the referencing process, the referencer shall embed Coaching Notes into the indexed report located in the TeamMate project file. Once the referencing process is completed, the referencer uses TeamMate to generate a "referencing worksheet" that will be stored in the TeamMate project file. The referencer will annotate the cover of the indexed report located in the TeamMate project file with the statement "All referencing comments have been resolved" and sign off on this report as "preparer." The Audit Manager will sign the TeamMate referencing worksheet as "reviewer". In those instances that required DAIGA/RIGA involvement to resolve issues, the DAIGA/RIGA will document in a Coaching Note their reason(s) for accepting or rejecting the audit team's response.

More specific guidance on referencing can be found in JA's Referencing Manual.

#### 806.07 Final Report Signature, Distribution, and Posting

In most cases, final reports are signed by the performing audit manager and distributed by transmittal letter signed by the DAIGA/RIGA. When the Administrator or an official outside of GSA is the report addressee, the final report is signed by the AIGA and transmitted by the Inspector General.

Final reports are distributed based on the nature of the review, type of report, and report recipient. In addition, the number of reports distributed to officials varies depending upon the specific circumstances of each review. The distribution of restricted reports must be determined on an individual report basis depending upon the nature of the restriction.

Final audit reports and external reviews are to be posted to the OIG public and/or intranet sites within one business day of final report issuance. More specific guidance on posting can be found on JA's intranet site.

#### 806.08 Decision Records

The audit team prepares a Management Decision Record (MDR) for financial and performance internal audit reports. For external reviews, the audit team prepares a Decision Record for External Review (DR). The MDR/DR is transmitted along with the final report and sent to HSSOs, RAs, or contracting officials and serve as the instrument for documenting the Agency's audit resolution process. The performing audit office completes section A before the MDR/DR is transmitted with the final report to the report addressee. Instructions for completing a MDR/DR are contained in GSA's Internal Audit Followup Handbook (ADM P 2030.2C).

## 806.09 DAIGA/RIGA Assessments of Final Internal Audits and External Reviews

Annually, the DAIGA/RIGA should assess the quality of completed work products issued by their respective regions/functional areas during a fiscal year. The reviews are part of JA's efforts to monitor compliance with its quality control policies and procedures. The reviews should provide evidence that the documentation has been examined for compliance with audit standards and JA policies and procedures. The reviews should be maintained by each DAIGA/RIGA outside of TeamMate. They will be included in JA's annual summary assessment of its system of quality control, as described in section 806.12 - Quality Assurance Program. In addition, the reviews support the annual certification needed to document compliance with the requirements of the Federal Managers' Financial Integrity Act.

## 806.10 Customer Satisfaction Questionnaires

Customer satisfaction questionnaires are provided to the primary recipient of every final internal audit and external review. The questionnaire should be provided electronically with the final work product. Each questionnaire should be returned to the JAO Director.

## 806.11 Value-Added Assessment Form for Internal Audit

Value-added assessment forms are completed by the AM and sent to the JAS Director upon receipt of the JA resolution letter.

## 806.12 Quality Assurance Program

The Quality Assurance Program is an internal evaluation program designed to provide reasonable assurance that JA carries out its work in accordance with established policies and procedures, including Government Auditing Standards, applicable OMB and GAO guidance, and statutory provisions applicable to GSA's Office of Inspector General. Specifically, it addresses: (1) leadership responsibilities for JA's audit quality, independence, legal, and ethical requirements; (2) the initiation, acceptance, and continuance of audit and attestation engagements; (3) personnel and staffing responsibilities, i.e. adequate skills, education, experience, and knowledge; (4) audit and attestation engagement performance, documentation, and reporting; and (5) the quality of internal monitoring efforts for adhering to professional standards and legal requirements. It is structured to ensure an objective, timely, and comprehensive appraisal of JA operations.

**Team Dynamics** - On a periodic basis, at least annually, JAO examines completed audits and external reviews. JAO may select a team of auditors/management analysts to assist in performing the reviews. The team leader: plans the review; selects the sample of audits/attestation engagements to review; assigns the selection to the team members; and, provides necessary guidance to team members to complete their respective reviews.

**Sample Selection** - A list of completed audits/engagements is identified using the Inspector's General recent publications of the "Semiannual Report to the Congress." Selection criteria considers work from all of JA's audit offices, the knowledge and experience of JA's professionals, the nature and complexity of the audit/review work, and prior "quality assurance" or "peer review" coverage and results.

**Relevant Guidance** - The quality assurance reviewers use the Council of Inspectors General on Integrity and Efficiency (CIGIE) Peer Review guidance relevant to the assigned review type, and OIG policy and procedures manual (blue book) to perform quality assurance reviews of the selected audits/engagements. From time to time, the review process also covers other issues or points of interest raised by JA management (i.e., "best practice" situations, assessments of corrective action activity that were based on prior quality assurance reviews or peer reviews.)

Review Results Documentation and Expected Outcome – Team members enter their review results onto the applicable Council of Inspectors General on Integrity and Efficiency (CIGIE) Review Checklist, a CIGIE Checklists Summary form, and when warranted, a JA prepared questionnaire designed to capture issues or points of interest raised by JA management. As needed, the team members also supplement this data with evidence to support their conclusions and comments from the supervisor of the activity being reviewed. The team leader examines the results to assure a complete understanding of the issues or points raised, and may confirm the results with both the quality assurance reviewer and the supervisor of the activity being reviewed. The leader will then compile and share the overall review results with JA management. As needed, the results are used to revise JA practices and/or policies, identify training needs, and share best practices.

On an annual basis, JA will summarize the results of its monitoring procedures, identifying any systemic issues that need improvement and recommendations for corrective action. Such summarization can include the evidence of supervision performed on both internal audits and external reviews as well as the reports stemming from that work (e.g. DAIGA/RIGA reviews, referencing).

Effective Date 1/22/2010

## 807.00 POST REPORT ACTIONS

### 807.01 Resolution of Internal Audit Reports and External Reviews

Final audit reports and external reviews are subject to resolution requirements set forth in GSA's Internal Audit Followup Handbook (ADM P 2030.2C) and in Public Law 104-106. These require the resolution of all report results and recommendations within six months of the report issuance date and completion of corrective actions by management within 12 months of the report issuance date. Reports not meeting the resolution and final action requirement are required to be reported to the Congress in the Inspector General's Semiannual Report to the Congress.

Upon receipt of a final audit report or external review, an Agency official completes the accompanying Management Decision Record for Internal or Financial Audit(MDR)or Decision Record for External Review (DR), attaches an action plan (internal audits only), and returns the MDR or DR to the Office of Audits so the management decision process can be completed.

For financial and performance audits, if audit officials find that the proposed action plan is satisfactory, a resolution letter stating that resolution has been accomplished is forwarded to management. If the MDR is not received or the action plan is not satisfactory when received, audit officials from the performing audit office should meet with Agency officials to discuss the issues. In instances where resolution cannot be achieved, the issuing RIGA should initiate the formal resolution process and provide the DAIGA with copies of all pertinent correspondence. The performing audit office is responsible for ensuring compliance with time frames and processing procedures contained in the ADM P 2030.2C.

When reviewing proposed action plans for financial and performance audits, time frames for completing final action more than 12 months from the report issuance date should be carefully considered. If warranted, the RIGA should contact the action office to ascertain whether an accelerated implementation time frame can be achieved. For action packages where final action is planned for more than 12 months, the resolution letter should notify management that the OIG must report incomplete actions to the Congress in the Inspector General's Semiannual Report to the Congress.

For external reviews, the performing audit office maintains a suspense file for tracking resolution and final action. Appropriate notification should be made to contracting officials regarding resolution and final action deadlines. The performing audit office is responsible for ensuring compliance with time frames and processing procedures contained in the ADM P 2030.2C, Chapter 4, Inspector General External (Contract) Review Reports.

### 807.02 Implementation Reviews

Implementation reviews are conducted to determine whether appropriate corrective action as stated in the proposed action plan has been taken by management on financial and performance audit reports. The scope of the review is limited to an examination of management's actions in response to the recommendations, but should include appropriate testing to ensure that reported conditions have been corrected by the actions taken.

Implementation reviews asserting that management's actions have been implemented in accordance with the action plans should be issued in letter report format. Reviews asserting that actions have not been implemented in accordance with the action plan (or actions taken have not corrected the reported condition) should be issued in either letter or standard report format, but must include management's response as an appendix to the report.

In cases where actions are not being implemented or actions taken have not corrected the reported condition, the final report transmittal letter should inform the management action official that a revised action plan should be submitted to GSA's Internal Control and Audit Division (BEI) within 30 days. A copy of the transmittal letter should be sent to BEI with the final report.

Since implementation reviews are not audits, the report format should be appropriately revised and no sequence number, other than the number of the original audit, should be included in the title. Distribution of the implementation review report is the same as for the original report. Green covers are generally used; however, if any report information needs to be restricted, red covers are used.

#### 807.03 JA Professional's Role in Contract Negotiations

The negotiation and award of GSA contracts is solely the responsibility of the GSA contracting officer. The GSA contracting officer develops the negotiation position, schedules the negotiations, negotiates the pricing, terms, and conditions of the contract with the vendor, makes the decision that the award is fair and reasonable and awards the contract. The JA professional's role in the negotiation process is to provide assistance to the contracting officer based on the results of the JA professional's preaward review of the vendor's offer and other related analysis performed. This includes providing explanations and clarifications of the reported results and other information provided in our reviews. It can also include providing assistance to the contracting officer regarding any other analysis of any additional information presented by the vendor after the issuance of the external review. The JA professional's attendance at negotiations and information provided during negotiation is at the invitation of the contracting officer. If requested to attend, the JA professional should make every effort to attend negotiations either in person or by telephone. Immediately following the negotiations, the JA professional should prepare a memorandum documenting the results of the negotiation conference.

#### 807.04 Multiple Award Schedule Assessment Program and Database

The Office of Audits collects data concerning Multiple Award Schedule (MAS) preaward and postaward reviews for the purpose of building a body of evidence. This body of evidence should facilitate the analysis of issues, trends, and changes in the MAS program, as well as provide useful, factual, and timely information to assist the FAS in improving the MAS program. All field audit offices will be responsible for the input of review information to the MAS Assessment Program Database for both pre-and post-award attestation reviews, as soon as possible, but no later than 30 days after report issuance (including draft post-award reviews). For specific guidance, contact the Contract Audit Office, JA-C.

Effective Date 1/22/2010

## 808.00 NONAUDIT SERVICES

### 808.01 Nature of Nonaudit Services

JA occasionally receives requests to perform nonaudit services. These services are not required to be GAGAS compliant. Nonaudit services generally fall under three categories:

- Services that do not impair audit organization independence;
- Services that do not impair audit organization independence as long as supplemental safeguards are taken; and
- Services that impair audit organization independence.

All requests for nonaudit services must be referred to JAO for consideration. JAO will try to be responsive to requests, while ensuring that the Office of Audits and assigned professionals remain independent (both in fact and appearance). When JAO approves a request for nonaudit services, JAO will identify any safeguards that must be taken to ensure compliance with the requirements of GAGAS. JAO will then issue a performance determination outlining the required safeguards. Professionals are not to expend resources on nonaudit services until JAO renders the performance determination.

### 808.02 Nonaudit Services That Do Not Impair Independence

JA assists management in improving operations and assessing the best ways to carry out Agency activities. The nonaudit services that do not impair the independence of the organization include the following:

- Task Force Participation. JA professional staff assist Agency task forces in an ex-officio capacity;
- Monitoring Services. JA professional staff are assigned to observe ongoing Agency actions and advise management of potential problems, or whether appropriate controls exist; and,
- Speaking at GSA Meetings and Functions. Sharing expertise with Agency employees.

These services involve providing management with advice based upon the JA professional's technical expertise or knowledge. Such services are often provided verbally, but can be summarized in written form. It may include offering previously prepared materials.

JA professionals should be mindful that they are not permitted to make management decisions, or perform management functions. These actions impair the independence of JA and the JA professional.

### 808.03 Nonaudit Services If Supplemental Safeguards Are Taken

These nonaudit services represent tasks that audit organizations conduct for Agency officials. They directly support operational activities. They are for the sole benefit of the requesting official or operating entity. These services consist of providing technical advice, or gathering and explaining information requested by Agency officials. These services differ from audits in that JA professionals provide data to managers without verification, analysis, or evaluations. In addition, the effort does not provide a basis for conclusions, recommendations, or opinions. These services may or may not result in a report.

These services can compromise the independence of JA or the JA professional if supplemental safeguards are not taken. When the JA receives a request for such nonaudit services, it is responsibility of JAO to determine what supplemental safeguards team members must take to prevent impairment to independence.

#### 808.04 Nonaudit Services That Impair Independence

JA professionals are not permitted to perform nonaudit services that include efforts where JA professionals perform management functions or make management decisions. An example would be if JA professionals post accounting transactions for the Agency. In addition, JA professionals cannot audit their own work or provide services that could be significant or material to the subject matter of ongoing, planned, or future audit activities. These efforts impair the independence of JA and the JA professional.

## CHAPTER 900 - INVESTIGATIVE POLICIES AND PROCEDURES

### 901.00 INVESTIGATIVE POLICIES AND STANDARDS

901.01 Intent of Chapter

901.02 Investigative Authority, Responsibilities, and Jurisdiction

901.03 Special Principles of Jurisdiction

901.03A Exclusive Jurisdiction

901.03B Concurrent Jurisdiction

901.03C The Assimilative Crimes Act

901.03D Law Enforcement Authority

901.03E Arrest Authority

901.03F Authority of State and Local Law Enforcement Officers Upon Federal Property

901.03G The Attorney General's Guidelines for Domestic FBI Operations

901.04 Investigative Standards

901.04A CIGIE Standards for Investigations

901.04B Additional OIG Standards for Investigations

901.05 Policy Regarding Disclosure to Prosecutors of Potential Impeachment Information

901.05A Purpose

901.05B Definitions

901.05C Policy

901.05D Compiling and Disseminating Information

901.05E Transfer or Reassignment of Employee

901.05F Records Retention

901.06 Policy Regarding Maintenance of Investigation Records in Anticipation of Litigation and Potential Discovery

901.06A Discovery Generally

901.06B Policy

901.07 Policies and Procedures Relating to Press Releases

## 901 FIGURES

- 901-01 September 1, 1983 OMB Memorandum Titled “Procedures for Investigating Allegations Concerning Certain Senior Administration Officials” and March 22, 1996 Executive Order Titled “Administrative Allegations Against Inspectors General”
- 901-02 December 8, 2003 DOJ Memorandum Titled “Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority”
- 901-03 Oath of Office – Law Enforcement Officer – GSA-OIG
- 901-04 (b) (7)(E)
- 901-05 The Attorney General’s Guidelines on for Domestic FBI Operations
- 901-06 CIGIE Quality Standards for Investigations
- 901-07 (b) (7)(E)
- 901-08 Policy Regarding the Disclosure to Prosecutors of Potential Impeachment Information Concerning Law Enforcement Agency Witnesses (“Giglio Policy”)
- 901-09 Guidance for Prosecutors Regarding Criminal Discovery (January 4, 2010)
- 901-10 Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases (March 30, 2011)
- 901-11 Release of information by personnel of the DOJ relating to criminal and civil proceedings

## 902.00 POLICIES AND PROCEDURES RELATING TO THE USE OF FORCE

902.01 Use of Force Generally

902.02 Reporting Requirements

902.03 Law Enforcement Control Tactics and Intermediate Weapon Training Program

902.04 (b) (7)(E)

902.04A GSA OIG Policy on (b) (7)(E)

902.04B Procedures for (b) (7)(E)

902.04C (b) (7)(E)

902.05 (b) (7)(E)

902.05A GSA OIG Policy on (b) (7)(E)

902.05B Procedures for (b) (7)(E)

902.06 Authority to Carry Firearms

- 902.07 Requirements for Carrying Firearms
- 902.08 Firearms Qualification and Training Program
- 902.09 OIG Authorized Firearms, Ammunition, and Holsters
- 902.10 Procedures for Carrying Firearms
- 902.11 Procedures for Storing Firearms
- 902.12 Repair of OIG Firearms
- 902.13 Maintenance of Firearms
- 902.14 Carrying a Firearm Aboard Commercial Aircraft
- 902.15 Medical Treatment
- 902.16 Intervention Policy

902 FIGURES

- 902-01 Law Governing the Use of Force
- 902-02 Use of Deadly Force
- 902-03 (b) (7)(E)
- 902-04 (b) (7)(E)
- 902-05 (b) (7)(E)
- 902-06 (b) (7)(E)
- 902-07 (b) (7)(E)
- 902-08 (b) (7)(E)
- 902-09 (b) (7)(E)
- 902-10 Law Enforcement Authorization Form
- 902-11 (b) (7)(E) Lautenberg Qualification Inquiry
- 902-12 (b) (7)(E)
- 902-13 GSA OIG Qualification Score Card
- 902-14 (b) (7)(E) Course
- 902-15 (b) (7)(E) Course
  
- 902-16 (b) (7)(E) Course
- 902-17 (b) (7)(E)

- 902-18 (b) (7)(E)
- 902-19 (b) (7)(E)
- 902-20 (b) (7)(E)
- 902-21 (b) (7)(E)
- 902-22 GSA OIG Training Program Attendance

#### 903.00 RESERVED

#### 904.00 CRITICAL INCIDENT POLICY

904.01 Purpose

904.02 Policy

904.02A Definitions

904.03 Responsibilities

904.03A Shooting Incident Procedures for Special Agents

904.03B Shooting Incident Procedures for Field Supervisors

904.03C GSA-OIG Headquarters Responsibilities

904.03D Post Incident Procedures

904.03E Injured Agent Procedures

904.03F Management Follow-Up

904.03G Legal Considerations

#### 905.00 POLICY AND PROCEDURES RELATING TO VICTIM AND WITNESS ASSISTANCE

905.01 Purpose

905.02 Background

905.03 Definitions

905.04 Policy

905.05 Procedures

#### 905 FIGURES

- 905-01 Victim/Witness Log

## 906.00 INVESTIGATIVE CASE MANAGEMENT PROCEDURES

### 906.01 Initiating Investigative Cases

#### 906.01A Creating Matters Not Investigated (MNI) Files

#### 906.01B Creating Complaint Files

#### 906.01C Creating Zero Files

#### 906.01D Opening Investigative Cases

#### 906.01E Assigning Investigative Case Priorities

### 906.02 Proactive Investigative Activities

#### 906.02A Structured Proactive Reviews of Program Areas

### 906.03 Case Management and Monitoring

#### 906.03A Case Management

#### 906.03B Referrals To and From Office of Audits (JA)

### 906.04 Collateral Investigative Leads

#### 906.04A OIG Policy on Collateral Investigative Leads

#### 906.04B Requesting Assistance on Collateral Investigative Leads

#### 906.04C Responding to Requests for Assistance on Collateral Investigative Leads

### 906.05 Case Closing

#### 906.05A Retention and Disposition of Investigative Records

## 906 FIGURES

- 906-01 GSA Disposition Schedule 3A056

## 907.00 HOTLINE POLICIES AND PROCEDURES

### 907.01 OIG Hotline

#### 907.01A Organization, Management, and Scope of the Hotline Function

#### 907.01B Receiving Hotline Telephone Calls

#### 907.01C Initial Screening of Hotline Complaints

#### 907.01D Procedures for Controlling GAO and Hotline Complaints

#### 907.01E Referring GAO and Hotline Complaints

907.01F Following Up on Referrals of GAO and Hotline Complaints

907 FIGURES

- 907-01 Hotline Complaint Form

908.00 RELATIONSHIPS WITH PROSECUTIVE AUTHORITIES, OTHER LAW ENFORCEMENT AGENCIES, AND AGENCY OFFICIALS

908.01 JI Relationships with Prosecutive Authorities, Other Law Enforcement Agencies and Agency Officials

908.01A JI Relationship with Offices of U.S. Attorneys

908.01B JI Relationship with the DOJ Antitrust Division

908.01C JI Relationship with the FBI

908.01D JI Relationship with Other Law Enforcement Agencies

908.01E JI Relationship with State and Local Prosecutors

908.01F JI Relationship with the Office of the Special Counsel

908.01G JI Relationships with GSA Officials

909.00 POLICY AND PROCEDURES FOR TRANSMITTING AND SAFEGUARDING CONTROLLED UNCLASSIFIED INFORMATION

909.01 Transmitting and Safeguarding Controlled Unclassified Information

909.02 Procedures for Transmitting and Safeguarding "For Official Use Only" Information

909.02A Special Procedures for Transmitting Items of Evidence, Subpoenaed Materials, and Equally Sensitive Information

909.02B Standard Procedures for Transmitting "For Official Use Only" Information between JI and Field Investigations Offices

909.02C Standard Procedures for Transmitting "For Official Use Only" Information from JI to RAs

909.02D Standard Procedures for Transmitting "For Official Use Only" Information from Field Investigations Offices to RAS

909.02E Standard Procedures for Transmitting "For Official Use Only" Information from JI to GSA Central Office Officials

909.02F Standard Procedures for Transmitting "For Official Use Only" Information from JI Offices to U.S. Attorneys or Other Government Agencies

909 FIGURES

- 909-01 Memorandum for the Heads of Executive Departments and Agencies, “Designation and Sharing of Controlled Unclassified Information”, May 9, 2008
- 909-02 (b) (7)(E)

#### 910.00 POLICY AND PROCEDURES FOR GRAND JURY MATERIALS

910.00 Purpose

910.01 Scope

910.02 Grand Jury Information

910.03 Policy

910.04 Limitations on Use of Grand Jury Materials

910.05 Responsibilities

910.06 Procedures

910.07 Safeguards During Use

910.08 Storage Requirements

910.09 Return of Grand Jury Information

#### 910 FIGURES

- 910-01 Federal Rules of Criminal Procedure - Rule 6. The Grand Jury

#### 911.00 MEDICAL STANDARDS FOR OIG SPECIAL AGENTS

911.01 General

911.01A Purpose

911.01B Regulatory Requirements

911.01C Background

911.02 Coverage

911.02A Scope

911.02B Policy

911.03 Functional Requirements and Environmental Factors

911.03A Functional Requirements

911.03B Environmental Factors

911.04 Medical Standards

911.04A Purpose

911.04B Applicability

911.04C Medical Conditions

911.05 Determination of Fitness for Duty

911.05A Examining Physician

911.05B Medical Review Officer

911.05C Report of Medical Review Officer

911.05D Medical Review Officer's Statement

911.05E Treatment of Applicants

911.05F Treatment of Special Agents

911.05G Employability Determination

911.05H Reconsideration

911.05I Waivers and Reasonable Accommodation

911.06 Physical Fitness Program

911.06A Medical Screening

911.06B Physical Fitness Activities

911.06C Program Management

911.06D Injuries

## 911 FIGURES

- 911-01 Physical Examination Form
- 911-02 Medical Review Form
- 911-03 Authorization for Release of Health Information Pursuant to HIPAA
- 911-04 PT Authorization Memorandum

## 912.00 STANDARDS AND PROCEDURES FOR INVESTIGATIVE INTERVIEWS

912.01 General Standards and Procedures for Investigative Interviews

912.01A Purposes of Investigative Interviews

912.01B Scope and Conduct of Investigative Interviews

912.01C Arranging Investigative Interviews of GSA Employees

912.01D Scheduling Interviews of Subjects of Investigation

912.01E Union Representation at Investigative Interviews

912.01F Legal and Other Non-Union Representation at Investigative Interviews

912.01G Privacy Act Notice Requirements Relating to Investigative Interviews

912.01H Confidentiality During Investigative Interviews

912.01I Waivers of Disciplinary Action During Investigative Interviews

912.01J Administering Oaths and Affirmations During Investigative Interviews

912.01K Documenting Investigative Interviews: Use of Recording Devices

912.01L Documenting Investigative Interviews: Notes of Interview

912.01M Documenting Investigative Interviews: Formal Records of Interview

912.01N Processing and Use of Formal Records of Interviews

912.02 Warnings and Assurances During Criminal Investigation Interviews

912.02A Providing Information on Targets and Subjects of Criminal Investigations

912.02B Specific Warnings and Assurances During Custodial Criminal Investigation Interviews

912.02C Specific Warnings and Assurances During Non-Custodial Criminal Investigation Interviews

912.02D Specific Warnings and Assurances During Criminal Investigation Interviews of Non-Federal Employees Directed by a Prosecutor or During Grand Jury Investigations

912.02E Warnings and Assurances to Federal Employees During Non-Custodial Interviews in a Criminal Investigation

912.03 Warnings and Assurances During Administrative Misconduct Interviews

## 912 FIGURES

- 912-01 Guidelines for Application of the Supreme Court's Decision in *NASA v. FLRA* Regarding Union Representation During OIG Interviews
- 912-02 Privacy Act Notice
- 912-03 Affidavit Format
- 912-04 Custodial (Miranda) Warning - Employee
- 912-05 Custodial (Miranda) Warning – Non-Employee

- 912-06 Non-Custodial Warning and Assurance to Employee: This Statement is Voluntary and May Be Used Against You in a Criminal Proceeding (Garrity)
- 912-07 Warning and Assurance to Employee: This Statement May Not Be Used Against You in a Criminal Proceeding (Kalkines)

#### 913.00 CONSENSUAL MONITORING

913.01 Policy

913.02 References

913.03 Scope

913.04 Consensual Monitoring Guidelines

913.05 General Consensual Monitoring Considerations

913.06 Obtaining Consenting Parties' Permission for Consensual Monitoring

913.07 Authorization

913.08 Duplicating, Securing, and Transcribing Recordings

913.09 Control, Inventory and Maintenance of Consensual Monitoring Equipment

#### 913 FIGURES

- 913-01 May 30, 2002, Memorandum From Attorney General Titled "Procedures for Lawful, Warrantless Monitoring of Verbal Communications"
- 913-02 Attorney General Memo Guidelines for IG with Statutory LE Authority
- 913-03 (b) (7)(E)
- 913-04 Request for Authorization to Use Electronic Equipment for Consensual Monitoring
- 913-05 (b) (7)(E)
- 913-06 Agreement for Temporary Interagency Loan of Equipment

#### 914.00 POLICY FOR UNDERCOVER OPERATIONS

914.01 Definitions

914.02 External Guidelines Affecting Undercover Operations

914.03 Types of Undercover Operations

914.04 Considerations

914.05 Application and Authorization to Conduct Undercover Activities

914.06 Approval for Undercover Activity Under Exigent Circumstances

914.07 Duration of Authorization

914.08 Requirement to Notify the FBI

914.09 Record Keeping and Reporting Requirements

914.10 Oversight and Review of Group I and Group II Undercover Operations

914.11 Termination and Closure of Undercover Operations

914.12 Cover Agents

914.13 Undercover Agents

914.14 Duties and Responsibilities of Undercover Agents

914.15 Participation in Illegal Activity by Undercover Agents

914.16 Participation in Undercover Activities Led by Other Law Enforcement Agencies

914.17 Coordination of Undercover Operations with Prosecutor

#### 914 FIGURES

- 914-01 CIGIE Guidelines for Undercover Activity, June 2013

#### 915.00 CONFIDENTIAL SOURCES AND CONFIDENTIAL INFORMANTS

915.01 Use of Sources of Information

915.02 Types of Sources of Information

915.03 Determination of Suitability and Documentation of Confidential Informants (CIs)

915.03A Conditions Requiring Review of the Confidential Informant Review Committee

915.03B Conditions Requiring Permission of Federal Prosecutor Before Use

915.04 Registration of CIs

915.05 Prohibition on Commitments of Immunity

915.06 Protecting the Identity of CIs and Cooperating Persons

915.07 Interaction with CIs and Cooperating Persons

915.08 Illegal Activity by CIs

915.09 Headquarters and Field Responsibilities

915.10 OIG Confidential Fund

915.119 Use of Confidential Funds

- 915.12 Approval for Use of Confidential Funds
- 915.13 Disbursement of Confidential Funds from (b) (7)(E)
- 915.14 Security of Confidential Funds
- 915.15 Payment of Confidential Funds
- 915.16 Accounting for Confidential Funds
- 915.17 Loss of Confidential Funds
- 915.18 Return of Confidential Funds to Headquarters

#### 915 FIGURES

- 915-01 The Attorney General's Guidelines Regarding the Use of Confidential Informants
- 915-02 Source Suitability Report and Recommendation
- 915-03 (b) (7)(E)
- 915-04 (b) (7)(E)
- 915-05 (b) (7)(E)

#### 916.00 SUSPENSION/DEBARMENT INVESTIGATIONS AND REFERRALS

- 916.01 Definition and Regulatory Basis of Suspensions/Debarments
- 916.02 Causes for Suspensions/Debarments
- 916.03 OIG Policy on Suspension/Debarment Investigations and Referrals
- 916.04 Documentation, Format, and Contents of Referrals for Suspensions
- 916.05 Documentation, Format, Contents, and Timing of Referrals for Debarment

#### 916 FIGURES

- 916-01 Documentation, Format and Contents of Referrals for Suspensions
- 916-02 Documentation, Format, Contents, and Timing of Referrals for Debarment

#### 917.00 SEARCHES, SEIZURES, AND INVENTORIES

- 917.01 Search and Seizure
  - 917.01A OIG Policy on Search and Seizure
  - 917.01B OIG Policy on Obtaining Search Warrants
  - 917.01C Special Agents' Authority to Serve and Execute Search Warrants

- 917.01D Executing Search Warrants
- 917.01E Searches Under Search Warrants
- 917.01F Searches Incidental to Arrest
- 917.01G Searches by Consent
- 917.01H Emergency Searches
- 917.01I Searches for Work-Related Evidence
- 917.02 Inventory Policy
  - 917.02A Purpose
  - 917.02B Definition
  - 917.02C Policy
  - 917.02D Inventories of Vehicles
  - 917.02E Scope of Inventory
  - 917.02F Property Control

917 FIGURES

- 917-01 (b) (7)(E)
- 917-02 (b) (7)(E)
- 917-03 Inventory Log Form

918.00 REPORTS OF INVESTIGATION AND LETTERHEAD REPORTS

- 918.01 OIG Policy on Reports of Investigation and Letterhead Reports
  - 918.01A Communicating Investigative Findings in Reports of Investigation versus Letterhead Reports
  - 918.01B Standards for Reports of Investigation and Letterhead Reports
- 918.02 Presentation Guidelines for Reports of Investigation and Letterhead
- 918.03 Format and Contents of Reports of Investigation
  - 918.03A General Format of Reports of Investigation
  - 918.03B Format and Contents of Administrative Data Page(s)
  - 918.03C Format and Contents of Table of Contents
  - 918.03D Format and Contents of Basis for Investigation
  - 918.03E Format and Contents of Synopsis

918.03F Format and Contents of Details of Investigation

918.03G Format and Contents of Potential Offenses

918.03H Format and Contents of Subjects and Defense Counsel

918.03I Format and Contest of List of Witnesses

918.03J Format and Contents of List of Exhibits

918.03K Report Inserts

918.04 Format and Contents of Letterhead Reports

918.04A Preparing Referrals for Criminal Prosecutive Consideration

#### 918 FIGURES

- 918-01 Sample Report of Investigation (Mandatory Sections)
- 918-02 Sample Report of Investigation (Optional Sections)
- 918-03 Sample Letterhead Report Issued for Information Only
- 918-04 Sample Letterhead Report Issued for Action Consideration
- 918-05 Memorandum of Interview
- 918-06 Memorandum of Activity

#### 919.00 REFERRALS AND POST-INVESTIGATIVE ACTIVITY

919.01 Referrals for Criminal Prosecutive Consideration

919.01A Reporting and Following Up on Referrals for Criminal Prosecutive Consideration

919.02 Referrals to GSA Management Officials for Administrative Action or Information

919.02A Purposes of Administrative/Information Referrals to GSA Management Officials

919.02B Making Administrative/Information Referrals

919.02C Following Up on Administrative Referrals to GSA Management Officials

919.03 Referrals to Other Agencies

919.03A Referrals to the FBI

919.03B Referrals to Other Law Enforcement Agencies

919.03C Referrals to Executive Branch Agencies

919.03D Referrals to the Office of Government Ethics

#### 919 FIGURES

- 919-01 Sample Memorandum for Transmitting Reports of Investigation Referrals to GSA Management Officials for Consideration of Administrative Action (Other Than Suspension and Debarment)
- 919-02 Disposition Report Form

#### 920.00 PROGRAM FRAUD CIVIL REMEDIES ACT INVESTIGATIONS AND REFERRALS

920.01 Investigations and Referrals Under the Program Fraud Civil Remedies Act (PFCRA)

920.01A Definition and Regulator basis for Administrative Action Under the PFCRA

920.01B Causes for Litigating Under the PFCRA

920.01C OIG Policy on Investigations and Referrals Involving the PFCRA

#### 921.00 POLICY FOR COMPUTER FORENSICS

921.01A Purpose

921.01B Reference

921.01C Definitions

921.01D Authority

921.01E Responsibilities

921.01F Selection for DCFU Personnel

921.01G Competency

921.01H Training and Professional Development for DCFU Personnel

921.01I Resources

921.01J Requesting Digital Forensic Assistance

921.01K Forensic Examination Standard Operating Procedures

921.01L Forensic Documentation Requirements

921.01M Forensic Reporting Requirements

921.01N Quality Management

#### 921 FIGURES

- 921-01 Digital Forensics Request Form
- 921-01A Search Warrant Support Request Form

- 921-02 (b) (7)(E)
- 921-03 (b) (7)(E)
- 921-04 (b) (7)(E)
- 921-05 (b) (7)(E)
- 921-06 (b) (7)(E)

922.00 SPECIALIZED INVESTIGATIVE TECHNIQUES

922.01 Purpose

922.02 (b) (7)(E) Information

922.02A Requests for (b) (7)(E) Information Other Than (b) (7)(E) Information

922.02B Ex Parte Requests for (b) (7)(E) Information

922.02C Requests for (b) (7)(E) Information

922.03 Obtaining (b) (7)(E) Information

922.03A Obtaining (b) (7)(E)

922.03B Obtaining (b) (7)(E)

922.03C Obtaining (b) (7)(E)

922.04 (b) (7)(E)

922.05 Questioned Documents

922.05A Definition of Questioned Documents

922.05B Standards for Comparison With Questioned Documents

922.05C Obtaining Handwriting Exemplars

922.05D Using Questioned Document Examiners and Examination Facilities

922.06 Title III or Electronic Surveillance Requiring a Warrant or Court Order

922.06A Title III Interception of Communications

922.06B Electronic Tracking Devices

922.06C Pen Registers and Trap and Trace Devices

922.06D Cell Phone Tracking

922.06E Video-Only Surveillance

922.07 Surveillances

922.07A Definition of and Reasons for Surveillances

922.07B OIG Policy on Surveillances

922 FIGURES

- 922-01 (b) (7)(E)

923.00 PENDING UPDATE

924.00 GOVERNMENT OWNED VEHICLES

924.01 Purpose

924.02 Policy

924.03 Administrative Requirements

924.03A Registration

924.03B Tolls

924.03C Assignments

924.03D Motor Vehicle Control Officers

924.03E Authorized Drivers and Reporting Requirements

924.04 Use of GOVs

924.04A Authority

924.04B Adverse Personnel Action

924.04C Official Purposes

924.04D Parking

924.04E Consumption of Alcohol

924.04F Storage

924.04G Home-to-Work (HTW) Transportation

924.04H Firearms

924.04I Transporting Others

924.04J Use of Other Federal Agency's GOVs

924.04K Vehicle Stops

924.04L Pursuits

924.04M Use of Emergency Response Equipment

924.04N Operating Safety

924.05 Maintenance, Repairs, and Services

924.06 Administrative Control of Credit Cards

924.07 Cash Purchases in Lieu of Credit Cards

924.08 Accidents and Damage to Vehicles

924.08A Theft and Vandalism

924.08B Accidents

924.08C Injury to a Third Party or Damage to a Third Party's Property

#### 924 FIGURES

- 924-01 Authorization Memorandum
- 924-02 Approval Certification

#### 925.00 EVIDENCE

925.01 Law of Evidence

925.02 Evidence Determination

925.03 Receiving, Identifying, and Preserving Evidence

925.03A Chain of Custody

925.04B Receiving, Identifying, and Tagging Records and Documents

925.03C Identifying and Tagging Seized Documentary Evidence

925.03D Identifying and Tagging Physical Evidence

925.03E Preserving Documentary and Physical Evidence

925.03F Disposition of Evidence

925.04 Grand Jury Evidence

#### 925 FIGURES

- 925-01 Evidence Custody Form
- 925-02 Receipt for Property Form

926.00 (b) (7)(E)

926.01 Purpose

926.02 (b) (7)(E)

926.03 Use of (b) (7)(E) Information

926.03A Responsibility

926.03B Controls

926.03C Requests for Information

926.03D Guidelines on the Dissemination of (b) (7)(E) Information Obtained from Computerized System

926.03E Standards of Discipline

926.03F Dissemination of (b) (7)(E) Information Obtained from Other Sources

## 927.00 PREAPPOINTMENT INVESTIGATIONS

927.01 General

927.01A OIG Applicants for Noncritical-Sensitive Positions

927.01B OIG Applicants for Critical-Sensitive Positions

927.02 Procedures for Conducting Preappointment Investigations

927.02A Responsibilities

927.02B General Guidelines for Investigative Coverage

927.02C Format and Distribution of Letter Reports

## 927 FIGURES

- 927-01 Authorization for Release of Information
- 927-02 Sample of Transmittal Memorandum, Disposition Report, and Letter Report (For All Applicants)

## 928.00 LAW ENFORCEMENT AVAILABILITY PAY

928.01 Definitions

928.02 General Rules

928.03 Reporting Requirements

929.00 RESERVED

930.00 INVENTORY AND PROPERTY MANAGEMENT POLICY

930.01 Purpose and Scope

930.02 Definitions

930.03 Responsibilities

930.04 Inventory Management

930.05 Lost or Stolen Property

930.06 Disposal of Property

930 FIGURES

- 930-01 Equipment List

Effective Date 9/3/2014

## 901.00 INVESTIGATIVE POLICIES AND STANDARDS

### 901.01 Intent of Chapter 900

Chapter 900 prescribes policy and standards for accomplishing the investigative mission of the Office of Inspector General (OIG). The guidelines constitute internal Office of Investigations (OI) guidance; they are not intended to, nor do they, create any legal rights (substantive or procedural) in any civil or criminal matter. Further, they place no limitations on otherwise lawful investigative or litigative prerogatives of the OIG. The Special Agent in Charge (SAC) of each Regional Office of Investigations may provide additional guidance, direction or supplementation to the policies set forth in this manual. Any issue or policy not specifically addressed in this chapter may be addressed at the regional level by the responsible SAC for that region.

### 901.02 Investigative Authority, Responsibilities, and Jurisdiction

The investigative authority and responsibilities of the OIG are contained in the IG Act (Figure 101-01); General Services Administration (GSA) Administrative Manual, OAD P 5410.1, Chapter 9, Part 3, Investigative Activities; OMB memorandum dated September 1, 1983, Procedures for Investigating Allegations Concerning Certain Senior Administration Officials and Executive Order dated March 22, 1996, Administrative Allegations Against Inspectors General (Figure 901-01); Attorney General's Guidelines for the Offices of Inspectors General with Statutory Law Enforcement Authority dated December 8, 2003 (Figure 901-02); and Inspector General's Delegation of Authority. Special Agents (SAs) exercise law enforcement authority pursuant to the P.L. 107.296 as defined in the Attorney General's Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority dated December 8, 2003 (Figure 901-02). Upon commencement of duties as a GSA-OIG SA, the agent will be sworn in by the Assistant Inspector General for Investigations (AIGI, Deputy Assistant Inspector General for Investigations (DAIGI), SAC, or designee and recite the GSA-OIG Oath of Office (Figure 901-03).

The investigative jurisdiction of the OIG includes all allegations of fraud, waste, abuse, and mismanagement, and any apparent or suspected violations of a statute, order, regulation, directive, or GSA Standards of Conduct in connection with any program or operation of GSA.

The OIG also receives and investigates:

- allegations of wrongdoing on the part of the GSA Administrator, unless the allegations are of such a nature that they must be referred to the Department of Justice (DOJ) or other officials;
- reports of alleged violations of the Sherman Antitrust Act;
- reports of alleged violations of labor laws (i.e., the Davis-Bacon Act, the Contract Work Hours and Safety Standards Act, and the Copeland Anti-Kickback Act) when there are indications of significant false statements;

- requests for investigative support from GSA, including: (1) inquiries into arrest dispositions involving GSA employees and (2) security and personnel matters where GSA , after initial review and factual analysis, determines that a problem warrants investigative referral to the OIG; and

- requests for investigative support from the GSA Office of General Counsel in tort claim and indebtedness matters, and in connection with litigation that has been initiated by or against GSA.

Investigations into allegations of wrongdoing on the part of the IG are conducted by the Department of Justice (DOJ), the Office of Government Ethics, the Office of Special Counsel, or the CIGIE (Executive Order 12993, 3/22/96) as appropriate.

### 901.03 Special Principles of Jurisdiction

Principles of jurisdiction in federal buildings and areas that impact on the exercise of the law enforcement authorities of JI personnel are discussed below. Field office investigative personnel should be familiar with jurisdiction within their regional office.

#### 901.03A Exclusive Jurisdiction

Exclusive federal jurisdiction is acquired by the United States when such jurisdiction is ceded to the United States by the state within whose boundaries the land is located, or by reservation by the United States upon admission of a State into the Union.

#### 901.03B Concurrent Jurisdiction

Concurrent jurisdiction exists whenever exclusive jurisdiction does not.

#### 901.03C The Assimilative Crimes Act

This statute (18 U.S.C. 13) provides that any act or omission occurring in a federal building or area that would be punishable by the laws of the state, district, territory, or possession in which federal property is located, but is not punishable by any act of the Congress, shall be punished as a federal offense. This statute applies when federal jurisdiction is exclusive, and also where jurisdiction is concurrent to the extent that the state has relinquished its police power.

#### 901.03D Law Enforcement Authority

Special Agents in the 1811 series who are supervised by the Assistant Inspector General for Investigations (AIGI) exercise law enforcement authority pursuant to federal statute. Section 812, Public Law 107-296 (11/25/02); 5 U.S.C. App. 3, Section 6(e) (IG Act); and Attorney General Guidelines for OIGs with Statutory Law Enforcement Authority (12/08/03). (Figure 901-02). This law enforcement authority is provided generally for use only within OIG Special Agents' official duties, which are defined by the IG Act as activities related to GSA's programs and operations. The AG's guidelines provide explicitly that "individuals exercising law enforcement authorities under Section 6(e) may exercise those powers only for activities authorized under the Inspector General Act of 1978 or other statute, or as expressly authorized by the Attorney General." (See AG's Guidelines, page 4.)

Under these legal authorities, Special Agents, while engaged in the performance of official duties as discussed above, and in addition to any other actions they are authorized to take may:

- seek and execute a warrant for an arrest, for the search of premises, or the seizure of evidence, if such warrant is issued under the authority of the United States upon probable cause to believe that a violation has been committed; and
- carry an OIG issued firearm.

#### 901.03E Arrest Authority

GSA-OIG Special Agents are authorized while engaged in the performance of official duties, to make arrests with or without a warrant for any federal violation, if such violation is committed in the presence of the Special Agent, or if the Special Agent has probable cause to believe that the person to be arrested has committed a felony. GSA-OIG Special Agents may also seek and execute arrest warrants, if such warrants are issued under the authority of the United States upon probable cause to believe that a violation has been committed.

The standards governing arrests by the OIG Special Agents are described below. During most investigations, arrests are made only in situations where necessary in the interest of effective law enforcement or similar exigent circumstances.

If an arrest without a warrant is made, (b) (7)(E)

(Figure 901-04) (b) (7)(E)

#### 901.03F Authority of State and Local Law Enforcement Officers Upon Federal Property

In exclusive jurisdictional areas, state and local law enforcement officers may usually serve civil or criminal process and exercise arrest powers when in pursuit. In concurrent jurisdictional areas, the extent of authority of state and local law enforcement officers is dependent upon the agreement between the state and federal government.

#### 901.03G The Attorney General's Guidelines for Domestic FBI Operations

Special Agents must adhere to the Attorney General's Guidelines for Domestic FBI Operations as published in Figure 901-05.

## 901.04 Investigative Standards

### 901.04A CIGIE Standards for Investigations

Jl investigative operations are required to be conducted in accordance with the general and qualitative standards that have been adopted by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) (Figure 901-06).

### 901.04B Additional OIG Standards for Investigations

Each Office of Inspector General shall make an annual written report to the Attorney General due on November 1 of each year, detailing the investigative and prosecutive activities of that Office of Inspector General. This report shall, at minimum, contain information on the number of (1) federal criminal investigations initiated, (2) undercover operations undertaken, and (3) times any type of electronic surveillance was used. Additionally, the report shall provide information on all significant and credible allegations of abuse of authorities conferred by section 6(e)(1) of the IG Act by Office of Inspector General investigative agents and what, if any, actions were taken as a result. The names of the agents need not be included in such report.

The following additional standards apply to investigations conducted by Jl:

1. An investigation must be conducted in a manner that strikes a balance between the responsibility to investigate violations of law or administrative regulations and the need to protect individual rights.
2. An investigation is opened when there are allegations that reasonably indicate that a violation of Federal criminal statutes, GSA Standards of Conduct, or administrative regulations within OIG responsibility or jurisdiction (Section 901.02) has occurred, is occurring, or will occur. Investigations are conducted with the minimum intrusion into the privacy of individuals, consistent with the need to collect information and evidence in a timely and effective manner.
3. An investigation is promptly terminated when all logical and reasonable investigative steps have been taken, or when priorities or resource constraints preclude continuing the investigation. When appropriate, investigative results are referred for prosecutive opinion. If prosecution is declined in an investigation and an administrative action may be warranted, the investigation is continued to a logical conclusion and the results are referred to appropriate Agency officials. Similarly, if no criminal violations are identified but administrative action is warranted, the investigation is brought to a logical conclusion and then referred to appropriate agency officials.
4. Matters involving allegations that can more appropriately be resolved by entities other than Jl are either referred to that entity or returned to the source. This includes returning allegations to agency managers for resolution without investigative action by Jl.

5. (b) (7)(E)



(b) (7)(E)

## 901.05 Policy Regarding Disclosure to Prosecutors of Potential Impeachment Information

### 901.05A Purpose

This chapter sets forth U.S. General Services Administration (GSA) Office of Inspector General (OIG) procedures for providing potential impeachment information to prosecutors under *Giglio v. United States*, 405 U.S. 150 (1972), and *United States v. Henthorn*, 931 F.2d 29 (9th Cir. 1991). The *Giglio/Henthorn* policy was promulgated to ensure that prosecutors receive potential impeachment information regarding investigative personnel who act as witnesses or affiants in a criminal investigation, while protecting the legitimate privacy rights of Government employees. This chapter conforms to U.S. Attorneys' Manual 9-5.100, Policy Regarding the Disclosure to Prosecutors of Potential Impeachment Information Concerning Law Enforcement Witnesses (*Giglio Policy*), as set forth at Figure 901-08.

### 901.05B Definitions

The following definitions apply to this chapter:

1. Agency Official. The Deputy Assistant Inspector General for Investigations (DAIGI), or his designee, in consultation with the Counsel to the Inspector General or his designee, will serve as the agency point of contact and the Agency Official for potential impeachment information concerning OIG investigative personnel. They are expected to arrive at mutually agreeable positions when operating in this role.
2. Requesting Official. The official designated by each United States Attorney's Office to serve as the prosecuting office point of contact concerning potential impeachment information.
3. Investigative Personnel. Any OIG employee in either an investigative or support role that may be called upon as a witness or affiant in a criminal investigation.
4. Potential impeachment information. For purposes of this policy, potential impeachment information is generally defined as impeaching information which is material to the defense. It also includes information that either casts a substantial doubt upon the accuracy of any evidence – including witness testimony – the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence. This information may include but is not strictly limited to: (a) specific instances of conduct of a witness for the purpose of attacking the witness' credibility or character for truthfulness; (b) evidence in the form of opinion or reputation as to a witness' character for truthfulness; (c) prior inconsistent statements; and (d) information that may be used to suggest that a witness is biased. Specific categories of potential impeachment information are listed later in this policy.

901.05C Policy

OIG investigative personnel are expected to comply with all federal, state and local laws, whether or not related to their official employment. They are expected to conduct themselves in a way that reflects favorably on themselves and the OIG and does not interfere with the efficient operation of the agency.

OIG investigative personnel are obligated to inform prosecutors with whom they work of potential impeachment information as early as possible prior to providing a sworn statement or testimony in any criminal investigation or case.

OIG Investigative personnel must notify (b) (7)(E) if any of the following incidents occur:

- Arrest;
- Detention for questioning in a criminal case; or
- Receipt of a citation, summons or complaint (excluding parking violations and civil processes not related to the performance of official duties).

Thereafter, the employee must (b) (7)(E)

(b) (7)(E)

Under the Giglio Policy, a prosecutor may also request potential impeachment information from the OIG. Potential impeachment information relating to OIG employees may include, but is not limited to, the categories listed below:

- Any finding of misconduct that reflects upon the truthfulness or possible bias of the employee, including a finding of lack of candor during a criminal, civil, or administrative inquiry or proceeding;
- Any past or pending criminal charge brought against the employee;
- Any allegation of misconduct that reflects upon truthfulness, bias, or integrity that is the subject of a pending investigation;
- Prior findings by a judge that an OIG employee has testified untruthfully, made a knowing false statement in writing, engaged in an unlawful search and seizure, illegally obtained a confession, or engaged in other misconduct;
- Any misconduct finding or pending misconduct allegation that either casts a substantial doubt upon the accuracy of any evidence – including witness testimony – that the prosecutor intends to rely on to prove an element of any crime charged, or that might have a significant bearing on the admissibility of prosecution evidence. This includes findings or allegations that relate to substantive violations concerning: (1) failure to follow legal or agency requirements for the collection and handling of evidence, obtaining statements, recording communications, and obtaining consents to search or to record communications; (2) failure to comply with agency procedures for supervising the activities of a

cooperating person; (3) failure to follow mandatory protocols with regard to the forensic analysis of evidence;

- Information that may be used to suggest that the employee is biased for or against a defendant; and
- Information that reflects that the employee's ability to perceive and recall the truth is impaired.

Once a request for impeachment information has been made, the OIG Agency Official shall continue to provide the Requesting Official any additional potential impeachment information that arises during the specific criminal case or investigation in which the OIG employee is a potential witness or affiant, until the prosecuting office advises the case is closed due to a judgment or declination.

Generally, allegations that are not credible or have resulted in exoneration of the accused OIG employee are not considered "potential impeachment information." However, such information which reflects upon the truthfulness or bias of an OIG employee should be provided to the Requesting Official under the following circumstances:

- The information is required by a court in the district where the investigation or case is being pursued.
- The allegation of untruthfulness or bias was made by a federal prosecutor, magistrate judge, or judge.
- The allegation received media publicity.
- Based on exceptional circumstances, the Requesting Official and the OIG Agency Official agree that such disclosure is appropriate.
- Disclosure is otherwise deemed appropriate by the OIG Agency Official.

The OIG Agency Official is responsible for advising the Requesting Official if any aforementioned allegation is unsubstantiated, not credible, or resulted in the employee's exoneration.

The OIG Agency Official will conduct a review for potential impeachment information and provide identified information to the Requesting Official.

#### 901.05D Compiling and Disseminating Information

1. Upon receiving a request for potential impeachment information from a Requesting Official, the OIG Agency Official will advise the employee that a review has been requested.

2. The OIG Agency Official will contact the (b) (7)(E) and will cause a review of the employee's (b) (7)(E) to be conducted so as to determine whether any "potential impeachment information" exists. In addition, the OIG Agency Official will coordinate with the JI (b) (7)(E)

3. If any relevant information is discovered, the OIG Agency Official will advise the employee before disclosure is made to the Requesting Official.

4. Prior to releasing any information, the OIG Agency Official will contact the Requesting Official to ascertain the particular requirements of that United States Attorney's office and assemble the material so as to ensure that any such release conforms to those requirements.

5. The OIG Agency Official will prepare a letter transmitting the potential impeachment information to be signed by (b) (7)(E) . The written OIG response and any attachments thereto shall be forwarded to the Requesting Official and a copy provided to the OIG employee.

6. The OIG Agency Official will maintain judicial rulings and related pleadings on information that was disclosed to the Court or the defense in a manner that allows expeditious access upon the request of any Requesting Official.

#### 901.05E Transfer or Reassignment of Employee

When an OIG employee is transferred or reassigned, the OIG Agency Official will ensure that any potential impeachment material is provided to the Requesting Official in the new district when the employee begins – or is reasonably anticipated to begin – meaningful work on a case or matter. Also, when notified that Giglio material has been transferred to a different office, the OIG Agency Official will provide a prompt update to the new office.

#### 901.05F Records Retention

The OIG Agency Official shall retain all documentation related to the Giglio/Henthorn matter in a confidential file in accordance with OIG records retention schedules.

#### 901.06 Policy Regarding Maintenance of Investigation Records in Anticipation of Litigation and Potential Discovery

The OIG follows the guidance issued by the Department of Justice on discovery, including the January 4, 2010, Guidance for Prosecutors Regarding Criminal Discovery, set forth at Figure 901-09, and the March 30, 2011, Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases, set forth at Figure 901-10. Essentially, SAs should think about the content of any form of e-communication before sending it; use appropriate language; think about whether e-communication is appropriate to the circumstances, or whether an alternative form of communication is more appropriate; and determine in advance how to preserve potentially discoverable information. (“E-communication” as used herein includes emails, text messages, instant messages, voice mail, blogs, social networking sites, and other means of electronic communication.) Some of the main points concerning discovery and the requirement to preserve documents, in both civil and criminal cases, are outlined below.

## 901.06A Discovery Generally

In civil cases, parties may request documents (as well as making other types of requests) on any matter that is relevant to any party's claim or defense, even if the information is not admissible at trial. Hence litigation holds in the civil context apply to all relevant documents. While privileged information such as communications with Government attorneys and pre-decisional documents generally are not subject to discovery, those documents must still be preserved and reviewed.

Criminal discovery is much narrower and generally is limited to substantive or factual material. The specific categories of information that must be provided to criminal defendants are as follows. Under *Brady v. Maryland*, the prosecution is required to provide all information that could be used to reduce the defendant's guilt. *United States v. Giglio* expanded this rule to require that the prosecution provide any information that undermines the reliability of evidence, including witness testimony (as discussed above). The Jencks Act requires that the defense receive the prior written or recorded statements of any prosecution witness, if the statements are on the same subject as the testimony. (This includes "substantially verbatim" notes of statements, and statements that were "adopted" by a witness as his own.) Federal Rule of Criminal Procedure 16 requires the prosecution to provide any written or oral statements made by the defendant (including notes of statements, even if they are not substantially verbatim). Courts do not always allow the prosecution to withhold privileged information in criminal discovery.

## 901.06B Policy

It is not always possible for SAs to know in advance whether an investigation will lead to civil or criminal action, who the defendant will be, or what information will appear exculpatory at the time of trial. Therefore, SAs should treat all information as though it may be subject to production in criminal or civil discovery, including weekly, significant item, and semiannual reports.

SAs should preserve all copies of statements made by any person (witness, subject, or SA) relating to the matter under investigation. This includes SAs' notes of witness statements, MOIs, email messages, audio or video recordings in original format, and all other material conveying any person's statements.

Communications over email regarding the matter under investigation should be saved in (b) (7)(E) or otherwise made part of the SA's permanent file. Retaining emails in the SA's inbox is not sufficient.

Substantive communications using a transitory medium (instant messaging, voicemail, text message) should be permanently saved to the case file. Instant messages can be copied and saved in a Word document; text messages can be emailed and the emails saved; and voicemail messages can be saved as digital audio files. Alternatively, SAs may write down the statements made over these media, in which case the date and speakers should be included.

SAs also should preserve all e-communications sent to or received from potential witnesses who are not law enforcement personnel, regardless of content.

SAs should write down the substance of all oral conversations or statements regarding the subject matter of the investigation (for example, a phone call with a witness) as soon after the statements were

made as possible, noting the date, time, and speaker. All potentially discoverable information must be preserved, regardless of whether the communication is written or oral.

When discussing investigations in any medium, and especially any written medium, SAs should express their thoughts with the expectation that a complete copy of what they say or write will eventually be provided to the defendant. Therefore, editorial comments, exaggerations, comments suggesting personal hostility, or other excessive or unprofessional content are not acceptable.

SAs should avoid making predictions about the outcome of a case or speculating about evidence when discussing the case with any witness, or over any written medium.

#### 901.07 Policies and Procedures Relating to Press Releases

The Attorney General's Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority dated December 8, 2003 (Figure 901-02) are to be followed concerning release of information relating to criminal and civil proceedings as well as joint investigations. See also 28 C.F.R. § 50.2 Release of Information by Personnel of the Department of Justice Relating to Criminal and Civil Proceedings (Figure 901-11). Additionally, see Chapter 604.02.

Effective Date 10/6/2017

## 902.00 POLICIES AND PROCEDURES RELATING TO THE USE OF FORCE

### 902.01 Use of Force Generally

GSA OIG SAs are authorized to conduct investigations, make arrests, execute warrants, carry firearms, and perform enforcement and other duties as authorized by the Inspector General Act of 1978 (as amended), 5 U.S.C. App. 3, and as stated in the Attorney General's Guidelines for the Offices of Inspectors General with Statutory Law Enforcement Authority.

1. Use of Force Considerations. The authority of SAs to use force in the execution of their law enforcement duties carries with it an obligation and responsibility to exercise discipline, restraint, and good judgment. The primary consideration for the use of force is the timely and effective application of the appropriate level of force necessary to lawfully control an individual or situation. Paramount considerations are preserving life and preventing physical injury to the SA or third parties.

2. Law Governing the Use of Force. SAs' use of force is governed by the "objectively reasonable" standard under the Fourth Amendment of the United States Constitution; the reasonableness of a particular use of force will be determined in light of the facts and circumstances confronting the law enforcement officer (special agent) at that time.

In use of force case law the U.S. Supreme Court has provided factors for SAs to consider in determining what level of force is reasonable (see Figure 902-01). A determination of reasonableness must be based on the totality of circumstances and take into account the fact that SAs are often forced to make split-second decisions—in circumstances that are tense, uncertain, and rapidly evolving—about the level of force necessary in a particular situation. SAs may use an objectively reasonable level of force, based upon the totality of the circumstances, including the escalation/de-escalation of resistance and other acts of the subject(s).

3. Department of Justice "Use of Deadly Force" Policy. Regarding the use of deadly force, SAs must abide by the Department of Justice "Use of Deadly Force" Policy (Figure 902-02). In accordance with that policy, SAs may use deadly force only when necessary, that is, when the agent has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the agent or to another person.

### 902.02 Reporting Requirements

SAs will notify (b) (7)(E) whenever they use force in the line of duty. When SAs (b) (7)(E) they must complete an (b) (7)(E) and forward it through (b) (7)(E)

### 902.03 Law Enforcement Control Tactics and Intermediate Weapon Training Program

An objective of the GSA OIG Law Enforcement Control Tactics Training Program (LECTP) is to ensure that SAs are trained in the most current techniques, methods and equipment to assist them in overcoming levels of resistance. Another objective of the LECTP is to provide SAs with the knowledge, skills, and tactics that will enable them to assess the threat and resistance level of an offender and respond with the correct level of force and control.

NOTE: SAs must carry at least one intermediate weapon (b) (7)(E) as intermediate means of control when carrying an OIG issued firearm (on or off-duty), unless JI policy provides otherwise or their SAC has authorized, in writing, a departure from this policy. Waivers of this policy by SACs will be limited to a case by case basis.

1. (b) (7)(E) are selected by their respective SAC and are required to complete the FLETC Law Enforcement Control Tactics Training Program, or a similar FLETC instructor course. (b) (7)(E) will maintain proficiency and expertise in law enforcement control tactics by completing a FLETC-sanctioned refresher course (b) (7)(E). All (b) (7)(E) should complete Basic First Aid and cardiopulmonary resuscitation (CPR) training from an authorized program, and should maintain a current certification. If the (b) (7)(E) did not attend the FLETC Control Tactics Training Course, the (b) (7)(E) should also be trained as an (b) (7)(E) Instructor if possible. (b) (7)(E) duties are as follows:
  - a. serve as primary contact for the (b) (7)(E);
  - b. conduct periodic law enforcement (LE) control tactics training (b) (7)(E);
  - c. maintain records regarding all regional LE control tactics training;
  - d. document topics covered during training and the names of those in attendance on appropriate training attendance forms (Figures 902-05, 902-07, 902-09 or 902-22) and upload the completed training forms and information to (b) (7)(E). (b) (7)(E) will then be prompted to approve each training record entry.
  - e. during control tactics training, brief SAs on OIG policy concerning use of force (b) (7)(E) and LE control tactics, including intermediate weapon use and incident reporting requirements;
  - f. (b) (7)(E);
  - g. maintain an accurate record of all LE control tactics equipment in the office's inventory and provide such to (b) (7)(E); and
  - h. report to SAC any unsafe practices, unusual behavior, or unauthorized activity concerning the use of intermediate weapons.

2. (b) (7)(E) Instructor (b) (7)(E) Instructors (b) (7)(E) are selected by their respective SACs after successfully completed training in the use of (b) (7)(E) by either a law enforcement agency or by an (b) (7)(E) vendor that has established a law enforcement training program. (b) (7)(E) will coordinate with (b) (7)(E) to train SAs in the proper application of (b) (7)(E)

3. Law Enforcement Control Tactics Training Program. SAs must complete initial and refresher training on the GSA OIG Use of Force Policy and law enforcement control tactics. Before being issued a (b) (7)(E) or (b) (7)(E), SAs must complete authorized training for these equipment items. Authorized training includes instruction by GSA OIG, FLETC, or other law enforcement training programs approved by the (b) (7)(E)

a. New SAs. (b) (7)(E) will provide all newly employed SAs with GSA OIG Use of Force Policy and LE control tactics training. At the SAC's discretion, this training may be administered during the next scheduled refresher training session.

b. Refresher Training. Instructors will provide refresher training to SAs during each fiscal year. SACs may schedule training on a (b) (7)(E). Although no set number of hours is mandated, training must be sufficient to maintain skills in control tactics techniques and the use of approved intermediate weapons. (b) (7)(E)

(b) (7)(E) in consultation with the GSA OIG Firearms Instructors, are encouraged to include practical scenarios in the training and to integrate control tactics concepts with (b) (7)(E) firearms training. Additionally, when feasible, (b) (7)(E) are encouraged to conduct joint training sessions with other regional offices.

c. Remedial Training. Any SA who fails to demonstrate a sufficient level of skill will be provided remedial instruction. (b) (7)(E) will document the reasons for remedial training and when the training is completed. Failure to achieve a sufficient level of skill after remedial training will be referred to the SA's supervisor.

d. Authorized Absences. SAs will complete required refresher training, unless excused by the (b) (7)(E) (b) (7)(E) may excuse SAs from refresher training for approved operational needs, medical reasons, or for some other exceptional circumstances (e.g., previously scheduled leave, non-optional temporary duty trips, other scheduled training). SAs should attempt to make up missed training (b) (7)(E). However, (b) (7)(E) may approve one control tactics training waiver to a SA during a fiscal year. (b) (7)(E) will approve waivers in (b) (7)(E). No agent should be granted a waiver for two consecutive training sessions without (b) (7)(E) approval.

e. Training Records. For each control tactics training session, (b) (7)(E) will record the information on the GSA OIG Law Enforcement (b) (7)(E)

(b) (7)(E) will upload the completed required training forms and information to (b) (7)(E). (b) (7)(E) will then be prompted to review and approve each training record entry.

f. Outside Agency Training. In the absence of a GSA OIG (b) (7)(E) the (b) (7)(E) may authorize a FLETC-certified instructor from another agency to provide refresher training to GSA OIG SAs. The (b) (7)(E) or a (b) (7)(E) will coordinate with the outside instructor in advance to ensure that the instructor follows the approved (b) (7)(E). The (b) (7)(E) may also authorize GSA OIG (b) (7)(E) to provide LE control tactics training to other Federal law enforcement SAs/officers.

4. (b) (7)(E) Training Program Policy and Procedures. The objective of the GSA OIG (b) (7)(E) Training Program (b) (7)(E) is to provide SAs with the information, methods, and techniques necessary to (b) (7)(E)

All GSA OIG SAs are required to attend an approved (b) (7)(E) training program. Under normal circumstances SAs will receive this training during basic law enforcement training at FLETC. SAs new to GSAOIG, who have not received (b) (7)(E) training, will be required to receive (b) (7)(E) training from GSA OIG. (b) (7)(E) should also schedule (b) (7)(E) refresher training (b) (7)(E). Refresher training will review the skills and techniques taught during the initial (b) (7)(E) and may be conducted in conjunction with (b) (7)(E). (b) (7)(E)

For the initial (b) (7)(E) and each refresher training session, (b) (7)(E) will record on a GSA OIG (b) (7)(E) (b) (7)(E) will upload the completed required training forms and information to (b) (7)(E) within (b) (7)(E). (b) (7)(E) will then be prompted to review and approve each training record entry.

5. (b) (7)(E) Policy and Procedures. The objective of the GSA OIG (b) (7)(E) is to provide SAs with the information, methods and techniques necessary to properly (b) (7)(E)

(b) (7)(E) lists the skills and techniques that will be taught to SAs.

(b) (7)(E) must have successfully completed training in the use of (b) (7)(E) from either a law enforcement agency or vendor who has an established law enforcement training program. (b) (7)(E) will coordinate with (b) (7)(E) and (b) (7)(E) to train SAs in the proper use of a (b) (7)(E). For the initial (b) (7)(E) and each refresher training session, (b) (7)(E) will record (b) (7)(E) (b) (7)(E) will upload the completed required training forms and information to (b) (7)(E). (b) (7)(E) will then be prompted to review and approve each training record entry.

6. (b) (7)(E)

(b) (7)(E) [Redacted]

902.04 (b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

902.04A GSA OIG Policy on (b) (7)(E) [Redacted]

A SA is authorized to carry an (b) (7)(E) provided that the SA:

1. Successfully completed an (b) (7)(E) training program, which includes (b) (7)(E) [Redacted]; and
2. Has read and follows OIG policies and procedures concerning (b) (7)(E) issued to SAs; and
3. Successfully completes (b) (7)(E) refresher training (b) (7)(E) or obtains an appropriate waiver from their (b) (7)(E) as outlined in 902.03(3)(d).

The authorization to carry an (b) (7)(E) can be revoked if a SA fails, at any time, to meet any of the above requirements.

902.04B Procedures for Carrying (b) (7)(E) [Redacted]

1. Non-Issued (b) (7)(E). (b) (7)(E) [Redacted]
2. Carrying Credential and Badge with (b) (7)(E). SAs must have their credentials and badges on their persons when carrying an (b) (7)(E), (b) (7)(E) [Redacted].

3. Securing an (b) (7)(E). (b) (7)(E)

4. Carrying/Transporting an (b) (7)(E) aboard Commercial Aircraft. (b) (7)(E)

902.04C (b) (7)(E)

(b) (7)(E)

902.05 (b) (7)(E)

All SAs of the GSA OIG in the "1811 Series" who are supervised by the AIGI are authorized to carry (b) (7)(E) provided that they comply with the requirements in 902.05A. (b) (7)(E)

902.05A GSA OIG Policy on (b) (7)(E)

A SA is authorized to carry an OIG issued (b) (7)(E) provided that the SA:

1. Has successfully completed the non-lethal control techniques portion of the FLETC's Criminal Investigator Training Program, or equivalent training that included (b) (7)(E) training, or has successfully completed a GSA OIG approved (b) (7)(E) training program (as further described in Section 902.03(5));
2. Has read and follows GSA OIG's policies and procedures concerning the issued (b) (7)(E) and
3. Successfully completes (b) (7)(E) refresher training (b) (7)(E) or obtains an appropriate waiver from their (b) (7)(E) as outlined in 902.03(3)(d).

(b) (7)(E)

902.05B Procedures for (b) (7)(E)

1. Non-Issued (b) (7)(E) (b) (7)(E)
2. Carrying Credential and Badge with (b) (7)(E) SAs must have their credential and badge on their person when carrying (b) (7)(E)
3. (b) (7)(E). The (b) (7)(E) will be carried in (b) (7)(E) approved by the SA's (b) (7)(E)
4. Securing a (b) (7)(E) (b) (7)(E)
5. Carrying/Transporting a (b) (7)(E) aboard Commercial Aircraft. (b) (7)(E)

902.06 Authority to Carry Firearms

All GSA OIG SAs in the "1811 Series" who are supervised by the AIGI are authorized to carry firearms subject to the requirements set out below. All SAs must abide by the DOJ "Use of Deadly Force" Policy (Figure 902-02).

1. Approving Official. SAs must complete an OIG Law Enforcement Authorization Form (Figure 902-10), which must be approved by (b) (7)(E) before a SA is authorized to carry a firearm.
2. Identification. SAs must carry their badges and credentials at all times when carrying an OIG issued firearm, unless (b) (7)(E).
3. Inventory. SACs are required to conduct an (b) (7)(E) inventory of all firearms, issued SA badges and credentials, and report any discrepancies to the AIGI immediately.
4. Lautenberg Restriction. The Lautenberg Amendment, § 658 of Public Law No. 104-208, 18 U.S.C. § 922(g)(9) prohibits individuals, including federal law enforcement personnel, who have been convicted of misdemeanor crimes of domestic violence from possessing firearms. All GSA OIG SAs are required to indicate on the Law Enforcement Authorization Form (Figure 902-10) when they are first hired, and (b) (7)(E) thereafter, on the Lautenberg Qualification Inquiry (Figure 902-11), whether they have been convicted of a crime of domestic violence. During the course of employment with GSA OIG, should a SA be criminally charged with a crime of domestic violence, the SA must immediately notify their SAC. SACs are required to provide formal notification to the AIGI of the circumstances surrounding the charges.

## 902.07 Requirements for Carrying Firearms

Handguns: When on-duty, and outside the office in an investigative status, a SA is required to carry their issued handgun, credentials, tactical badge, and issued steel handcuffs with double locking feature, at all times (except (b) (7)(E) and are authorized to carry their issued handgun and braided nylon restraints while off-duty. Whenever carrying the OIG issued firearm, SAs must also carry at least one intermediate weapon (b) (7)(E)

1. In order to carry an issued handgun, a SA must have satisfied the following requirements:

- a. completed an OIG Law Enforcement Authorization Form (Figure 902-10), (b) (7)(E)
- b. successfully completed the handgun and non-lethal control techniques portion of the FLETC's Criminal Investigator Training Program (CITP), or equivalent training, and successfully completed an initial OIG (b) (7)(E) handgun qualification course (Figure 902-12), or (b) (7)(E), utilizing their GSA OIG issued handgun, with a score of at least (b) (7)(E). If a SA successfully completed FLETC's CITP, or that of another law enforcement training center, and did not receive training with a (b) (7)(E), they will need to complete GSA OIG's (b) (7)(E)
- c. has read (and follows) the OIG's policies and procedures regarding firearms; and
- d. (b) (7)(E) after initial qualification, SAs must successfully complete OIG handgun qualification (Figure 902-12) with a score of at least (b) (7)(E) points, and complete periodic familiarization training. (See Firearms Qualification and Training Program, (Section 902-08).

SAs shall not be authorized to carry any issued firearms if at any time they fail to meet any of the above requirements. However, a SA may be excused from (b) (7)(E) firearms qualification by the (b) (7)(E) for approved absences when the SA cannot attend either the scheduled (b) (7)(E) firearms qualification or subsequent make-up day(s) during the (b) (7)(E). The waiver shall be recorded on a (b) (7)(E)

Any SA who does not qualify at all for (b) (7)(E) will lose their authorization to carry an issued handgun and shall have their issued handgun recovered by the SAC until such time as qualification is satisfactorily completed.

2. Long Guns: All SAs will receive GSA OIG operator's training, or equivalent training, with GSA OIG's shotguns and sub-machine guns (SMGs), hereafter collectively referred to as long guns. The long guns may only be carried by designated SAs for use in operations in which they are deemed necessary by the (b) (7)(E)

- a. Requirements for carrying long guns are as follows:

i. To operate a shotgun, a SA must have successfully completed a GSA OIG (b) (7)(E) or equivalent training, and the OIG shotgun qualification course (SQC) (Figure 902-14 or Figure 902-15) (b) (7)(E)

ii. To operate a SMG, a SA must have successfully completed a GSA OIG (b) (7)(E) (b) (7)(E) or equivalent training, and the (b) (7)(E) Course (Figure 902-16) (b) (7)(E).

iii. A SA shall not be authorized to carry a long gun if they fail at any time to meet any of the above applicable requirements. Any SA who fires a long gun qualification course, but does not qualify, will lose their authorization to carry that type of long gun until such time as qualification is satisfactorily completed. A SA shall not be permitted to carry a long gun in the event they are unable to qualify with their issued handgun.

3. Reporting Requirement- If a SA fails to qualify during (b) (7)(E) handgun qualification, (b) (7)(E) shotgun qualification, or (b) (7)(E) SMG qualification, their (b) (7)(E) will notify the (b) (7)(E)

4. Firearms Generally- Supervisory personnel, or their designees, are authorized to retrieve an issued firearm from a SA at any time when in their judgment such retrieval is in the best interest of the SA, GSA OIG, or the safety of others.

a. In the event of a temporary physical/medical condition or a temporary disability, a SA:

i. shall consult with his or her physician to determine if participation in the (b) (7)(E) firearms qualifications and training is in the best interest of the SA's health and safety, as well as the safety of the other SAs participating;

ii. shall discuss with the (b) (7)(E) and the (b) (7)(E) any accommodation that might be made, or medical restriction that has been imposed that might require a temporary waiver from participation in firearms qualifications;

iii. shall submit a written request for a temporary waiver from firearms qualifications to their (b) (7)(E) if recommended by his or her physician. Based on the SA's request, the (b) (7)(E) will prepare a memorandum to the (b) (7)(E) for approval. The memorandum will describe the nature of the temporary condition and length of treatment, if known; and

iv. may be granted a temporary waiver from firearms qualifications on a case-by-case basis for the requested time period. In the event the condition extends past the requested time period, the SA may be required to submit an updated request.

b. In the event that a temporary physical/medical condition or an obvious temporary disability comes to the attention of a (b) (7)(E) and the (b) (7)(E) they will:

i. discuss the situation with the SA;

ii. determine what, if any, specialized equipment or special accommodations are necessary to ensure safe uninterrupted firearms qualifications and training; and

iii. Determine if a temporary waiver from firearms qualifications is necessary. Approval for any specialized equipment or accommodations may be granted by the (b) (7)(E) on a case-by-case basis. During the time period of the temporary waiver, SAs should perform their job-related duties, (b) (7)(E) . If a SA is not authorized to carry a firearm, they should not engage in activities that might require a firearm. Their (b) (7)(E) will determine whether to recover their firearm during this period. When the waiver is no longer necessary, the SA will attempt firearms qualification as soon as practicable; at latest, at the next (b) (7)(E) firearms qualifications session.

## 902.08 Firearms Qualification and Training Program

The objective of the GSA OIG Firearms Qualification and Training Program is to ensure that SAs are qualified to employ firearms with accuracy and speed without posing a hazard to themselves, fellow SAs, or other innocent parties.

SAs must demonstrate proficiency with OIG issued firearms and qualify with their issued handgun (b) (7)(E) and with long guns (b) (7)(E) SAs will use OIG issued ammunition in all qualifications.

1. (b) (7)(E) Pistol Course of Fire. (b) (7)(E) is the approved course of fire for OIG (b) (7)(E) pistol qualification:

- a. A minimum of (b) (7)(E), utilizing the agent's standard duty holster and magazine pouches, will be completed during (b) (7)(E) qualification. However, if a SA fails to meet the minimum score they may shoot additional (b) (7)(E)
- b. Each SA is required to qualify (b) (7)(E) with the same firearm and holster they will carry on-duty.
- c. The minimum (b) (7)(E) qualification score for SAs is (b) (7)(E) The score must be documented on the Qualification Score Card (GSA OIG Form FA1) (Figure 902-13).

2. Shotgun Qualification Courses of Fire. (b) (7)(E) are the approved qualification courses of fire for OIG (b) (7)(E) shotgun qualification. The (b) (7)(E) may decide which of the two qualification courses are used.

a. The minimum shotgun qualification score for SAs for the (b) (7)(E) The SAs' scores must be documented on GSA OIG Form FA1\_Rev 08/14/13, Qualification Score Card (Figure 902-13).

3. Submachine Gun Qualification Course of Fire. GSA OIG's (b) (7)(E) Course is the approved qualification course of fire for OIG (b) (7)(E) submachine gun qualification (Figure 902-16).

a. The minimum SMG qualification score for SAs is (b) (7)(E) and their scores must be documented on Qualification Score Card (GSA OIG Form FA1 Figure 902-13).

Qualification scores will be recorded by the (b) (7)(E) on the OIG Firearms Qualification Score Card at the conclusion of each qualification course. The (b) (7)(E) will upload the completed Qualification Score Cards to (b) (7)(E). SACs will then be prompted to review and approve each training record entry.

4. Firearms Qualification and Training. (b) (7)(E) firearms qualification and training will be completed on official time under the supervision of the (b) (7)(E)

A SA in need of further practice may (but is not required to) spend additional time with an OIG issued firearm and OIG issued ammunition at a range approved by the (b) (7)(E)

5. Additional Courses of Familiarization Fire Training. The timing of additional courses of fire beyond the required (b) (7)(E) (902.08(1)) (not including the further practice discussed above) is to be at the discretion of the (b) (7)(E). When a course of fire is specified for familiarization fire the entire course is to be fired and the score recorded but the customary minimum qualification score is waived as it is for familiarization purposes and not qualification. However, a safety violation by the SA during the course of fire may be considered a failure of the familiarization course and at the (b) (7)(E) discretion may create the need to remediate the course of fire. The following familiarization courses are considered necessary to meet the objectives of the OIG Firearms Qualification and Training Program:

- a. (b) (7)(E)
- [Redacted list items]

f. When familiarization training is conducted, the (b) (7)(E) will make a notation on the OIG Firearms Qualification Record.

6. Federal Aviation Administration (FAA) Training. (b) (7)(E) and (b) (7)(E) are responsible for instructing all SAs on an (b) (7)(E) basis in the FAA Law Enforcement Officers Flying Armed Requirements. When the FAA training is conducted, the (b) (7)(E) will make a notation on the OIG Firearms Qualification Record.

7. Use of Force Policy Briefing. (b) (7)(E) are responsible for instructing all SAs (b) (7)(E) on the OIG's policies and procedures relating to the use of force. When the use of force policy briefing is conducted, the (b) (7)(E) will make a notation on the OIG Firearms Qualification Record.

8. (b) (7)(E) All (b) (7)(E) are selected by their respective SAC, and must have successfully completed FLETC's (b) (7)(E) or equivalent training (b) (7)(E) duties are as follows:

- a. issue OIG approved firearms;
  - b. report to the SAC or ASAC the loss or theft of any firearm or ammunition, in their custody;
  - c. conduct (b) (7)(E) firearms qualifications and training;
  - d. ensure that SAs qualify (b) (7)(E) or (b) (7)(E) with their issued firearms and that this is properly documented on the Qualification Score Card (GSA OIG Form FA1 Figure 902-13);
  - e. upload a copy of the Qualification Score Card to (b) (7)(E)
  - f. brief SAs on firearms safety, techniques of shooting, and OIG policy concerning firearms use;
  - g. brief SAs on OIG policy and procedure relating to incidents of firearms discharges;
  - h. ensure that issued firearms are inspected (b) (7)(E) to determine serviceability;
  - i. ensure that an accurate firearms inventory and agent assignment list is maintained in (b) (7)(E)
  - j. ensure that an accurate ammunition inventory is maintained in (b) (7)(E)
  - k. distribute ammunition to SAs for qualification, training, and use on official duty;
  - l. report to SAC any unsafe practices, unusual behavior, failure to qualify, or unauthorized activity concerning issued firearms;
  - m. provide remedial training to any SA who does not qualify with their issued firearm; and
  - n. ensure that each SA maintains their assigned firearm in a clean and properly operating condition at all times.
9. (b) (7)(E). The (b) (7)(E) is appointed by the (b) (7)(E) and is assigned to Headquarters or a Regional Field Office. The (b) (7)(E)
- a. is responsible for administering and overseeing the OIG Firearms Qualification and Training Program;
  - b. provides instructional and administrative assistance to the (b) (7)(E) which includes the standardization of firearms training and reporting procedures;
  - c. is responsible for ensuring that firearms qualifications and training meet the standards approved by the (b) (7)(E)
  - d. maintains an automated master inventory and maintenance, custody, and control record of all OIG issued firearms; and
  - e. with the approval of the (b) (7)(E) establishes the criteria for the certification and recertification of (b) (7)(E)

## 902.09 OIG Authorized Firearms, Ammunition, and Holsters

### Firearms.

1. On-Duty: The issued duty-carry handgun for GSA OIG SAs is the (b) (7)(E) [REDACTED]. The issued shotgun for GSA OIG SAs is the (b) (7)(E) [REDACTED]. The issued SMG for GSA OIG is the (b) (7)(E) [REDACTED]. While on-duty, GSA OIG SAs are only authorized to carry/possess issued firearms.
2. Off-Duty: SAs are authorized by the GSA IG to carry their OIG issued firearm while off-duty as set forth in Section 902.07. While carrying an issued firearm off-duty, all other GSA OIG rules and procedures for carrying firearms apply.
  - a. As law enforcement officers, SAs may choose to carry a privately owned firearm while off-duty under the authority contained in The Law Enforcement Officers Safety Act of 2004, as codified at 18 U.S.C. § 926B. If SAs choose to utilize this authority to carry a privately owned firearm, they should familiarize themselves with the full text of 18 U.S.C. § 926B.
  - b. Ammunition. Only OIG authorized ammunition will be used in an OIG authorized firearm. All qualifications with issued firearms will be accomplished with OIG issued ammunition, except when qualifying at FLETC.
3. Holsters. When carried on a SA's person, handguns must be carried in a holster. SAs are to use an OIG issued holster or an OIG authorized personal holster (b) (7)(E) [REDACTED] that has been approved by the (b) (7)(E) [REDACTED]. Holsters must be worn (b) (7)(E) [REDACTED].
  - a. Upon approval or at the direction of their (b) (7)(E) [REDACTED], SAs must fire an initial qualification utilizing the (b) (7)(E) [REDACTED] and the associated magazine holders prior to utilizing them on-duty and then must fire an (b) (7)(E) [REDACTED] familiarization course utilizing them. These familiarizations will be in addition to the (b) (7)(E) [REDACTED] required (b) (7)(E) [REDACTED] qualification course with the SAs' standard duty carry holster and magazine holders.
4. Enforcement Action. When on an enforcement action, SAs are to wear and carry GSA OIG issued tactical gear appropriate under the circumstances and/or as directed by their (b) (7)(E) [REDACTED].

## 902.10 Procedures for Carrying Firearms

SAs will exercise utmost caution in carrying, removing, and storing the firearm to ensure that it is not accidentally discharged or seized by another person.

1. Non-authorized Firearms. (b) (7)(E) [REDACTED]. While off-duty, SAs are not required to carry a firearm but may carry their GSA OIG issued handgun if they choose.

2. Carrying Credentials and Badge While Armed. SAs must have their badges and credentials on their persons when carrying an OIG issued firearm (with the tactical badge worn in the (b) (7)(E) [REDACTED])

3. Drawing a Firearm (b) (7)(E) [REDACTED]

4. Alcoholic Beverages. (b) (7)(E) [REDACTED]

5. Medication. (b) (7)(E) [REDACTED]

6. Loss or Theft of an OIG issued Firearm. SAs will immediately report the loss or theft of an OIG issued firearm or ammunition to appropriate federal and local law enforcement authorities, as well as (b) (7)(E) [REDACTED]. (b) (7)(E) [REDACTED] will immediately report the loss or theft of a firearm to (b) (7)(E) [REDACTED]. In turn, (b) (7)(E) [REDACTED] will immediately report the loss to (b) (7)(E) [REDACTED] to determine the appropriate follow-up activity. The SA will submit a memorandum to (b) (7)(E) [REDACTED] within (b) (7)(E) [REDACTED] from the date of occurrence setting forth the details of the loss or theft, including measures taken to recover the firearm. (b) (7)(E) [REDACTED] will ensure that the necessary information relating to a lost or stolen firearm is promptly (b) (7)(E) [REDACTED]

7. Discharge of a Firearm. A firearms discharge incident is any discharge of an OIG issued firearm, other than for training at a range, including any discharge of a firearm by a SA in connection with law enforcement activity. (b) (7)(E) [REDACTED]

#### 902.11 Procedures for Storing Firearms

1. Designated loading/unloading areas. SAs will utilize clearing barrels in designated loading/unloading areas to load/unload firearms in the office.

2. Securing a Firearm. (b) (7)(E)

(b) (7)(E)

3. Caution must be taken to prevent children and other persons from having access to firearms, ammunition, and handcuffs. SAs are responsible for the security of their handguns at all times.

(b) (7)(E)

4. Securing Long Guns in Vehicles. When transporting a long gun in a vehicle:

a. (b) (7)(E)

5. Securing Long Guns While on Travel Status (b) (7)(E)

(b) (7)(E)

#### 902.12 Repair of OIG Firearms

(b) (7)(E). All modifications or repairs to OIG issued firearms will be authorized by a GSA OIG (b) (7)(E). Minor repairs or modifications to OIG issued firearms may be completed by a GSA OIG (b) (7)(E). Major repairs will be made by a factory authorized representative.

If a firearm fails to function properly and the (b) (7)(E) cannot correct the problem at the range, (b) (7)(E) will keep the (b) (7)(E) and the SA. The (b) (7)(E)

A firearm in need of repair will be conveyed to the (b) (7)(E). In the event the firearm has to be shipped, it will be shipped to the appropriate (b) (7)(E), and shipper's instructions for shipping firearms will be followed. (b) (7)(E) are required to submit to the (b) (7)(E) copies of invoices of expenditures relating to the repair and maintenance of an issued firearm. (The SA may be given a replacement firearm under these circumstances.)

#### 902.13 Maintenance of Firearms

SAs are responsible for maintaining the proper condition of their issued handguns and assigned long guns.

1. Issued handguns and assigned long guns will be cleaned after each use, including qualification, practice firing, and/or as needed between firings.
2. (b) (7)(E) should inspect handguns and long guns prior to each (b) (7)(E) qualification for deficiencies or damage. At least (b) (7)(E) will conduct a detailed inspection and cleaning of the handguns and long guns under the control of their office.
3. SAs' issued handgun, ammunition, holster, and related firearms equipment are subject to inspection at any time by the (b) (7)(E).

902.14 Carrying a Firearm Aboard Commercial Aircraft

1. 49 C.F.R. § 1544.219 sets forth policy relating to "carriage of accessible weapons" by law enforcement officers aboard aircraft operated by a United States licensed air carrier. (b) (7)(E)

Under the provisions of 49 C.F.R. § 1544.219, several conditions must be met in order for a SA to carry an accessible weapon aboard a commercial aircraft. (b) (7)(E)

(b) (7)(E)

a. Armed SAs must notify the aircraft operator of the flight(s) on which they need to have their weapon accessible at least one (1) hour, or in an emergency as soon as practicable, before departure (49 C.F.R. § 1544.219(a)(3)(i)).

b. Armed SAs must identify themselves to the aircraft operator by presenting their credentials that include a clear full-face picture, signature of the SA, and either the signature of the authorizing GSA OIG official or the official GSA OIG seal. A badge, shield, or similar device may not be used or accepted as the sole means of identification (49 C.F.R. § 1544.219(a)(3)(ii)).

c. Prohibitions regarding alcoholic beverages and LEOs flying armed:

i. No aircraft operator may serve any alcoholic beverage to an armed LEO (49 C.F.R. § 1544.219(c)(1)).

ii. No Armed LEO may:

◦ Consume any alcoholic beverage while aboard an aircraft operated by an aircraft operator;

◦ Board an aircraft armed if they have consumed an alcoholic beverage within the previous 8 hours (49 C.F.R. § 1544.219(c)(2)(i), (ii)).

2. While flying armed, a SA must maintain control of their firearm when carrying it on board the aircraft.

3. (b) (7)(E)

5. SA must remain cognizant of current Transportation Security Administration (TSA) regulations addressing the carriage of firearms aboard a commercial aircraft and comply with those regulations. SAs:

a. shall complete the TSA training program, "Flying While Armed"; and

b. are authorized to fly armed while off-duty on personal travel in accordance with 49 C.F.R. § 1544.219; and

c. must remain aware that the Ground Security Coordinator or Customer Service Supervisor may be able to assist with any problems with authorization from the airline to fly armed.

#### 902.15 Medical Treatment

GSA OIG SAs who cause physical injury by the use of force will immediately seek emergency medical treatment for those persons injured (b) (7)(E), as appropriate.

#### 902.16 Intervention Policy

1. Intervention in Observed Violations of State or Local Laws. The following guidelines should be followed by SAs in deciding whether or not to intervene in an observed violation of state or local law.

(b) (7)(E)

3. Intervention in Observed Violations of Non GSA Related Federal Laws. (b) (7)(E)

(b) (7)(E)

4. Personal Liability for Intervention. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

5. (b) (7)(E)

Effective Date 12/17/2013

## 904.00 CRITICAL INCIDENT POLICY

### 904.01 Purpose

This directive establishes General Services Administration (GSA), Office of Inspector General (OIG) policy, procedures and guidelines regarding GSA-OIG Special Agent(SA) involvement in a critical incident. A critical incident is any event that causes, or has the potential to cause, an unusually intense stress reaction. The distress individuals experience after a critical incident often limits their ability to cope, impairs their ability to adjust and negatively impacts the work environment. These guidelines are applicable to any situation, which has resulted in death, serious bodily injury, or any other type of critical incident. These guidelines are intended to help reduce the chances of GSA-OIG SAs developing post-traumatic stress disorder (PTSD) resulting from a critical incident.

### 904.02 Policy

A number of occupations are at high risk for psychological distress and morbidity. Law enforcement constitutes one such profession. A shooting incident is possibly the most severe occupational stress that an agent is likely to experience during his/her career. The duties of an agent can expose him/her to mentally painful and highly stressful situations, which cannot be resolved through normal stress coping mechanisms.

Unless adequately treated, these situations can create disabling emotional and physical problems. It has been found that agents involved in shootings resulting in death or serious bodily injury may experience such stress disorders. It is the responsibility of the GSA-OIG to provide personnel with information on stress disorders and to guide and assist in its deterrence. It also is the GSA-OIG policy to take immediate action after any incident to safeguard the continued good physical and mental health of all involved personnel.

### 904.02A Definitions

1. Post-Traumatic Stress Disorder (PTSD). An anxiety disorder that can result from exposure to short-term severe stress, or the long-term buildup of repetitive and prolonged milder stress. It may result from exposure to a "traumatic event."
2. SA Involved Shooting Incident. A line-of-duty incident where shooting causes death or serious bodily injury to an agent or other person.
3. Critical Incident. Any situation faced by law enforcement/emergency service personnel that has a stressful impact sufficient enough to overwhelm the usually effective coping skills of either an individual or a group. The event may have the potential to interfere with the ability to function either at the scene or later. If the incident is extreme in nature, it may serve as the starting point for PTSD.

904.03 Responsibilities

904.03A Shooting Incident Procedures for Special Agents

1. A Special Agent should immediately obtain medical aid for injured parties. (b) (7)(E)
2. A SA should immediately notify (b) (7)(E) that a shooting incident has occurred and provide the details.
3. A SA should notify the appropriate (b) (7)(E)
4. A SA should identify individuals (b) (7)(E)  
The SA involved in the shooting (b) (7)(E)
5. A SA will cooperate with the local police by identifying himself/herself and if asked furnish a very brief description of the incident. As applicable, inform the local police that a firearm(s) was discharged while acting in an official capacity, whether medical assistance was requested, and whether a suspect(s) is in custody. (b) (7)(E)  
A SA should advise the police that he/she will furnish further details (oral or written) after the SA has been afforded reasonable time to regain his/her composure, notify supervisory personnel, and consult with the Counsel to the IG. If the discharge results in death or injury, a SA should (b) (7)(E) to the local police or the appropriate law enforcement authority, if requested, and obtain a receipt. (b) (7)(E)  
the weapon and the spent cartridges will be treated as evidence and turned over to the first non-involved GSA-OIG supervisor or SA that arrives on the scene.

904.03B Shooting Incident Procedures for Field Supervisors.

1. The cognizant GSA-OIG supervisor will immediately notify (b) (7)(E) of all critical incidents involving a SA. The GSA-OIG supervisor will consult with the (b) (7)(E) regarding a shooting incident.
2. (b) (7)(E)  
Supportive, (b) (7)(E) communication is very valuable in attempting to alleviate fear of agency reaction. The supervisor does not have to comment on the incident but should show concern and empathy for the agent.

NOTE: The following guidance assumes that a GSA-OIG supervisor will arrive at the scene shortly after an incident. Due to the size of GSA-OIG and the extensive geographic area covered by our personnel, a supervisor may not reach the scene as quickly as desired. In the absence of a GSA-OIG supervisor, SAs should cooperate with local authorities, bearing in mind the guidance provided in this section.

1. The GSA-OIG supervisor shall, if required, assist in making appropriate arrangements for necessary medical treatment for the SA.
2. The handling of a shooting investigation by local authorities may vary greatly.
3. The GSA-OIG supervisor's reactions should adapt accordingly. Support for the SA(s) and cooperation with local authorities must both be considered.
4. If possible, and with the cooperation of authorities investigating the shooting, the GSA-OIG supervisor should arrange for the SA(s) involved in the shooting to leave the area as soon as possible. A counselor or other supportive friend or SA should remain with the SA, but should be encouraged NOT to discuss the details of the incident.
5. If possible, the GSA-OIG supervisor, when meeting with the involved SA(s), should consider the following:

◦Stimulants or depressants should be administered by medical personnel only.

(b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

[Redacted]

(b) (7)(E) [Redacted]

6. SAs involved in a shooting should notify (b) (7)(E) about the incident as soon as practicable. If the involved SA(s) is unable to do so, a (b) (7)(E) personally shall notify (b) (7)(E) to the hospital or other suitable location.

7. At all times, when at the scene of the incident, the (b) (7)(E) should handle the SA and all involved GSA-OIG personnel in a manner that acknowledges the stress caused by the incident.

8. Other SAs at the scene of a shooting also should be screened for emotional reactions and given administrative leave as necessary, on a case-by-case basis.

904.03C GSA-OIG Headquarters Responsibilities

1. The (b) (7)(E) will immediately notify (b) (7)(E) of all available facts.
2. If there is a possible violation of Title 18 USC 111 (Assaulting, resisting, or impeding certain officers or employees) and/or 1114 (Protection of officers and employees of the United States), (b) (7)(E)
3. The (b) (7)(E) will coordinate with (b) (7)(E) regarding any media responses concerning a shooting incident.
4. If the shooting has resulted in the death of an agent, headquarters will notify the (b) (7)(E). That office should coordinate with the (b) (7)(E) and arrange to dispatch (b) (7)(E) to assist the (b) (7)(E).
5. After the (b) (7)(E) is notified of all available facts concerning a shooting incident involving a GSA-OIG law enforcement officer, he/she shall dispatch an investigation team, to be headed by personnel from the OIG (b) (7)(E) and which will report to the director of (b) (7)(E) to conduct a thorough investigation of the incident and prepare a report for the (b) (7)(E) as soon as possible. The investigation team will coordinate its efforts with the law enforcement agency having jurisdiction over the shooting. See also, OIG Manual Section 201.03(d).

904.03D Post Incident Procedures

1. Involved personnel shall be (b) (7)(E)
2. The SA involved in a shooting (b) (7)(E)
- (b) (7)(E)
3. A GSA-OIG supervisor should (b) (7)(E)

4. In conjunction with (b) (7)(E), administrative or other investigations will be completed as expeditiously as possible. The SA involved in the incident will be advised of (b) (7)(E)

5. All GSA-OIG personnel involved in a shooting incident should (b) (7)(E)

6. (b) (7)(E), will address inquiries from the media and will release a statement, if appropriate, pertaining to the incident. The interest of the agent involved will be considered prior to making any media releases. If a (b) (7)(E) is authorized to make a statement to the news media, he/she should (b) (7)(E).

7. A SA(s) directly involved in a shooting incident (b) (7)(E)

#### 904.03E Injured Agent Procedures

If an agent is seriously injured while on duty and is expected to remain hospitalized, the following should be considered:

- Security and privacy of the injured agent;
- Inquiries from GSA-OIG and other law enforcement offices;
- Media/Press inquiries (refer to guidance set forth above);
- Visiting hours with office personnel;
- Blocking hospital telephone calls to the injured agent's room. This will prevent the SA from receiving "crank" calls or inquiries from the media;
- Arranging for the installation of a "liaison telephone" for use by the injured agent and the liaison agent. For short-term use, consider a cellular telephone;
- Ensuring additional items of evidence are properly secured by the hospital (e.g., clothing). When in doubt, treat items as evidence;
- Keeping GSA-OIG management and office personnel apprised of the condition of the injured SA; and
- Assisting the injured agent in coordinating with administrative elements to obtain various benefits, i.e., contacting GSA-OIG Human Resources for assistance with Workers' Compensation Benefits, etc.

#### 904.03F Management Follow-up

- PTSD disorders may not be evident immediately, or the SA may attempt to hide the problem. Each GSA-OIG supervisor is responsible for monitoring the behavior of SA personnel for symptoms of PTSD.
- A GSA-OIG supervisor may require a SA to seek assistance or counseling from a mental health professional or properly trained peer support personnel. This

action may be taken upon a reasonable belief that stress may be disrupting the SA's job performance or ability to carry a firearm.

#### 904.03G Legal Considerations

The same constitutional protections apply to a SA as apply to other individuals since the SA could be subjected to allegations of negligence, wrongful acts, civil rights violations, and criminal violations. Although a SA involved in a shooting incident should cooperate with the investigating authorities, the SA should be cognizant that he/she is still entitled to full constitutional privileges such as due process, the right to counsel, protection against unreasonable search and seizure, and the right not to be compelled to make incriminating statements. Should a SA involved in a shooting incident become subject to civil litigation, the GSA-OIG will, upon request from the SA and a determination by the GSA-OIG that the SA acted within the scope of employment, contact DOJ to seek legal representation for the SA.

Effective Date 12/17/2013

## 905.00 POLICY AND PROCEDURES RELATING TO VICTIM AND WITNESS ASSISTANCE

### 905.01 Purpose

The purpose of these guidelines is to establish procedures to be followed by management officials and Special Agents (SAs), General Services Administration (GSA) Office of Inspector General (OIG) in responding to the needs of crime victims and witnesses. These guidelines combine the requirements of the Victim and Witness Protection Act of 1982 (VWPA), P. L. 97-291 (October 12, 1982), and the Victims' Rights and Restitution Act of 1990, contained in the Crime Control Act of 1990, P.L.101-647 (November 29, 1990) (the Act). Consistent with the like purposes of these statutes, the present Guidelines provide guidance on implementation of the 1990 Act as well as continued guidance on the protection of witnesses under the VWPA, and shall serve as a resource for SAs in the treatment and protection of victims and witnesses of Federal crimes.

### 905.02 Background

The VWPA of 1982 was enacted "to enhance and protect the necessary role of crime victims and witnesses in the criminal justice process; to ensure that the federal government does all that is possible within limits of available resources to assist victims and witnesses of crime without infringing on the constitutional rights of defendants; and to provide a model for legislation for State and local governments."

The Crime Control Act of 1990 mandates that officials of the Department of Justice and other federal agencies, engaged in the detection, investigation, or prosecution of crime, make their best efforts to ensure that victims of crime are treated with fairness and respect for the victim's dignity and privacy.

The 1990 Victims Rights and Restitution Act, 42 U.S.C. §§ 10606-10607, (VRRRA) creates a Federal Victims of Crime Bill of Rights and codifies services that shall be available to victims of federal crime. This Act does not specifically address the treatment of witnesses; however, it reinforces and augments the VWPA in acknowledging the necessary role of witnesses in the criminal justice process and in ensuring their fair treatment by responsible officials.

The 1990 Victims of Child Abuse Act, 42 U.S.C. § 13031, (VCAA) provides a mandatory requirement for certain professionals working on federal land, or in a federally-operated or contracted facility, to report suspected child abuse to an investigative agency with authority to take emergency action to protect the child. The statute also provides criminal sanctions, a Class B misdemeanor, for those professionals who fail to report suspected child abuse.

Special Agents working on federal land or in a federally-operated or contracted facility, in which children are cared for or reside, are required to comply with this statute.

## 905.03 Definitions

For purposes of these guidelines:

1. "Victim" means a person who has suffered direct or threatened physical, emotional, or financial harm as a result of the commission of a crime, including:

- in the case of a victim that is an institutional entity, an authorized representative of the entity; and
- in the case of a victim who is under 18 years of age, incompetent, incapacitated, or deceased, one of the following (in order of preference): a spouse; a legal guardian; a parent; a child; a sibling; another family member; or another person designated by the court.
- Federal departments and state and local agencies, as entities, shall not be considered "victims."

2. "Witness" means a person who has information or evidence concerning a crime, and provides information regarding his/her knowledge to a law enforcement agency. Where the witness is a minor, the term "witness" includes an appropriate family member or legal guardian. The term "witness" does not include a defense witness or an individual involved in the crime as a perpetrator or accomplice.

3. "Serious crime" (as used in the VWPA of 1982), means a criminal offense that involves personal violence, attempted or threatened personal violence, or significant property loss.

4. "Financial harm" is not defined or limited by a dollar amount, thus the degree of assistance, as discussed later in this chapter, must be determined on a case-by-case basis. For example, since victims' means vary, that which constitutes a minimal financial loss for one might represent a devastating loss for another.

5. "Child" means a person who is under the age of 18.

6. "Child abuse" means the physical or mental injury, sexual abuse or exploitation, or negligent treatment of a child. The term "child abuse" does not include, however, discipline administered by a parent or legal guardian to his or her child provided it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty

7. "Negligent treatment" means the failure to provide, for reasons other than poverty, adequate food, clothing, shelter, or medical care so as to seriously endanger the physical health of a child.

## 905.04 Policy

These guidelines apply to those components of the OIG engaged in the detection, investigation, or prosecution of Federal crimes. They are intended to apply in all cases in which individual victims are adversely affected by criminal conduct or in which witnesses provide information regarding criminal activity.

While special attention shall be paid to victims of serious, violent crime, all victims and witnesses of federal crime who have suffered physical, financial, or emotional trauma shall receive the assistance and protection to which they are entitled under the law.

Because of the nature of federal criminal cases it may often be difficult to identify the victims of the offense and, in many cases, there may be multiple victims. Sound judgment may be required to make appropriate decisions as to the range of victim services and assistance given. However, SAs should err on the side of providing assistance rather than withholding it.

1. Bill of Rights of Crime Victims (1990 VRRRA). A crime victim has the following rights:

- The right to be treated with fairness and with respect for his/her dignity and privacy.
- The right to be reasonably protected from the accused offender.
- The right to be notified of court proceedings.
- The right to be present at all public court proceedings related to the offense, unless the court determines that testimony by the victim would be materially affected if the victim heard other testimony at trial.
- The right to confer with the attorney for the government in the case.
- The right to restitution.
- The right to information about the conviction, sentencing, imprisonment, and release of the offender.

2. Child Abuse and/or Negligent Treatment. Special Agents working on federal land or in a federally operated or contracted facility are required to report suspected child abuse and/or negligent treatment. Suspected child abuse should be reported immediately to the local or state investigative agency with authority to take emergency action to protect the child. If appropriate a report should also be made to the United States Attorney's office.

#### 905.05 Procedures

In order to implement the requirements of the Act, there must be at least one individual who shall be designated specifically to carry out victim-witness services in each Regional Field Investigative Office. This Primary Contact Person (PCP) shall be delegated authority by the Special Agent in Charge to carry out the activities described in these Guidelines.

1. Special Agent in Charge for Investigations. With respect to compliance with the VWPA each SAC shall:

- designate, in writing, a PCP and an alternate for providing assistance to victims/witnesses;
- establish internal procedures to ensure the proper oversight of the services to be rendered to victim/witnesses;
- in instances where certain duties and responsibilities overlap, the SAC must take all steps necessary to require coordination and inter-agency cooperation;
- assure that the PCP is notified of any situation in which the provisions of the Act might be invoked;
- submit a copy of the Victim/Witness Log (905-01) to Headquarters, Investigations

(JIB), Attn: Assistant Inspector General for Investigations (JI), when requested.

2. Primary Contact Person. The responsibilities of the PCP shall include ensuring the following actions are taken:

◦ establish contact with Victim Witness Coordinator (VWC) in each U.S. Attorney's office in his/her region to address policy related to:

☒ training;

☒ referral;

☒ information; and

☒ consultation services offered to victims/witnesses.

◦ be the primary contact person with VWCs in U.S. Attorneys' offices;

◦ provide instruction to Special Agents concerning their responsibilities in carrying out the Act;

◦ at the earliest opportunity make reasonable and diligent efforts through the case agent to inform crime victims concerning:

☒ the place where the victim may receive emergency medical and/or social services;

☒ compensation or restitution to which the victim may be entitled under this or any other applicable law, and the manner in which such relief may be obtained; and

☒ the availability of public and private programs which provide counseling, treatment, and other support to the victim.

◦ to the extent deemed necessary and feasible, assist the victim in contacting the specific person or office which will provide the above services;

◦ on an individual case basis, make contacts with VWC in the State and local jurisdictions involved to determine their policy in relation to the particular victim/witness situation or problem;

◦ to the extent possible, avoid disclosure of the addresses of victims/witnesses except to authorized persons;

◦ advise victims and witnesses of serious crimes of steps that may be taken, if warranted, to protect the victim, the victim's family, the witnesses, and the witnesses' families from intimidation and, upon request, the status of the investigation, as appropriate, including any arrest or decision not to prosecute;

◦ maintain property of any victim or witness which is held for evidentiary purposes in good condition and, if possible, promptly return it; if property is not returned promptly, an explanation should be given to the victim or witness as to the property's significance in any criminal prosecution;

◦ upon request by the victim or witness, assist in notifying the employer of the victim or witness if cooperation in the investigation of the crime causes the victim's or witness's absence from work; In interviewing victims or witnesses at their places of employment or other public places, the SA should explain to employers and others the individual's status as a victim or witness and the necessity for conducting the interview at that time.

- upon request by the victim or witness, assist in notifying the creditors of the victims or witness, if the crime or cooperation in the investigation affects the victim's or witnesses' ability to make timely payments;
- provide victim and witness information pamphlets that outline the rights of crime victims under federal law and describe available assistance programs to victims and witnesses as appropriate;
- assist appropriate officials to ensure pertinent information in the SA's possession is included in the victim impact statement;
- in the event of actual intimidation and/or harassment of the victim/witness, take immediate action to:
  - ☑ notify the U.S. Attorney involved in the prosecution of the case;
  - ☑ render whatever interim assistance is necessary to the victim or witness; and
  - ☑ notify the responsible Federal agency, i.e., Federal Bureau of Investigation, U.S. Marshals Service, etc.

### 3. Alternate Contact Person. ACP shall:

- be designated in writing by the SAC; and
- provide assistance to the PCP and the Special Agent in all matters relating to victim/witness assistance program as assigned.

### 4. Special Agent. Special Agent shall:

- at the earliest opportunity (the earliest opportunity means one that will not interfere with an investigation or hamper the Special Agent in the performance of other law enforcement responsibilities) after the detection of a crime, make reasonable and diligent efforts to:
  - ☑ identify the victims of a crime;
  - ☑ inform the victims of their right to receive the services described above and under the law; and
  - ☑ inform each victim of the names, titles, business addresses, and telephone numbers of the responsible officials to whom such a request for services should be addressed.
- prepare and use the Victim/Witness Log (Figure 905-01) as a system for tracking and recording procedures used to provide assistance to victims/witnesses in individual cases. A copy of the Victim/Witness Log will be maintained in the Special Agent's work papers and will be made available to the U.S. Attorney's Office upon request;
- immediately notify the PCP concerning actual instances of intimidation or harassment of any victim or witness;
- notify the PCP of any situation in which the provisions of the Act could be invoked;
- assist the PCP, VWC, and the U.S. Attorney, as necessary, in carrying out the provisions of the Acts;
- ensure that victims/witnesses routinely receive information on the prohibition against victim/witness intimidation or harassment, and the appropriate remedies; and

◦ensure that any information in the case file that is pertinent to the defendant's sentence is brought to the attention of either the U.S. Attorney or the U.S. Probation Office. This information is needed to assist in the preparation of the victim impact statement in the U.S. Probation Office's pre-sentence report to the presiding judge.

Note: All components shall work with appropriate components of other federal agencies that investigate and prosecute violations of Federal law to assist them in providing these services to victims; and shall coordinate their victim-witness service efforts with state and local law enforcement officials, including tribal police officials in Indian Country and victim assistance and compensation service providers.

If available, the OIG will provide printed brochures containing general information and a brief description of rights and available services, to be given to victims as soon as a victim is identified.

Effective Date 3/21/2017

## 906.00 INVESTIGATIVE CASE MANAGEMENT PROCEDURES

### 906.01 Initiating Investigative Cases

On receipt of an allegation, the (b) (7)(E) evaluates the allegation for possible investigative effort, referral, or closure.

Investigative cases are initiated after the OIG receives a complaint or allegation involving possible violations of criminal/civil law or administrative regulations involving either an employee or the programs/operations of GSA. Determinations on complaints/allegations involve one of the five possible courses of action: (1) creating a matters not investigated file (Section 906.01A); (2) creating complaint case file (Section 906.01B); (3) creating a zero case (Section 906.01C); (4) opening an investigative case (Section 906.01D); or (5) opening a pro-active investigation (Section 906.02). The above determinations are only to be made by (b) (7)(E). File numbers are generated in the (b) (7)(E) system after these types of cases initiations are approved by the (b) (7)(E).

#### 906.01A Creating Matters Not Investigated (MNI) Files

MNI files are created to document matters referred to the regional offices, which do not warrant opening an investigation. (b) (7)(E)

#### 906.01B Creating Complaint Files

A case opened as a preliminary investigation into any allegations of a federal crime. A preliminary investigation must be concluded within (b) (7)(E) of its initiation, which may be extended by up to (b) (7)(E) by the SAC. (b) (7)(E)

#### 906.01C Creating Zero Files

A case created to provide a repository of information for future retrieval when the information may not immediately warrant opening an investigation. All allegations involving potential civil or administrative violations which do not result in opening an Investigative (I) case should be documented as a Z case. A Z case can be used as a preliminary investigation into allegations of civil and/or administrative violations.

(b) (7)(E)

(b) (7)(E)

#### 906.01D Opening Investigative Cases

An investigative case is opened when the factual basis of the complaint or allegation warrants such action. Opening an investigative case involves: (1) assessing the importance of the case relative to JI's overall case inventory; (2) initiating a record of the assignment in (b) (7)(E) (3) (b) (7)(E) approves the case initiation in (b) (7)(E) thereby assigning a case number to the file when an incident or closely related incidents involve multiple subjects, generally only a single case will be opened. However, more than one case may be opened if there is a compelling reason to do so. The decision to open multiple cases is made by (b) (7)(E), as appropriate, consistent with Section 906.04.

1. Obtaining Case/Assignment Numbers. The case/assignment number (b) (7)(E).
2. Maintaining Records of Investigative Assignments. All JI offices are responsible for ensuring that case/assignments in the (b) (7)(E) are accurate and up-to-date.
3. Determining Case Classification and Sub-classification Categories. The OIG describes the nature of investigative workload using case classification and sub-classification categories.

(b) (7)(E) and Pre-Employment investigations are special types of investigations.

1. (b) (7)(E)

2. Pre-Employment: Background investigations of OIG job applicants, including auditors, investigators, and OIG support personnel.

#### 906.01E Assigning Investigative Case Priorities

(b) (7)(E)

Under this system, an evaluation of the relative importance of each investigative case is made at the time of case opening. At the field office level, (b) (7)(E) determines the case priority. This priority determination will be adjusted if warranted by new information developed during an investigation.

## 906.02 Proactive Investigative Activities

Proactive investigative activities are an important means of developing investigative cases. OIG SAs engage in two distinct types of proactive investigative activities: (1) proactive activities designed to develop investigative leads and sources; and (2) structured proactive reviews of program areas that are potentially vulnerable to fraud, waste or abuse, which may be initiated by either Central Office or field offices.

In contrast with standard OIG investigations, these proactive investigative activities do not necessarily result from specific allegations of wrongdoing received by the OIG.

### 906.02A Structured Proactive Reviews of Program Areas

OIG SAs also participate in structured proactive reviews of GSA program areas that are vulnerable to fraud, waste, or abuse. SACs are authorized to initiate, develop, and coordinate proactive reviews within their particular GSA regions.

As such, they (1) determine the investigative focus and scope; (2) conduct the investigation subject to existing OIG case management controls; and (3) request (b) (7)(E) [REDACTED] when deemed appropriate.

## 906.03 Case Management and Monitoring

### 906.03A Case Management

In order to ensure timely and appropriate action on investigative cases, the SAC and other supervisory personnel need to be involved, on a continuing basis, in planning and reviewing the investigative work. Supervisory personnel are to ensure adherence to the investigative standards contained in OIG Manual Section 901.04 when planning, directing, and reviewing investigative work.

1. Investigative Plan. An investigative plan, is prepared at the start of every investigation. While the specific format of the plan is determined by (b) (7)(E), all plans must provide at least the following information:

- investigative issues (what is to be resolved); and
- possible violations (statutes and/or regulations); and
- steps necessary to meet investigative objectives

Investigative plans are prepared in (b) (7)(E) and reviewed and approved by the (b) (7)(E).

2. Case Reviews. Every investigative case is subjected to a comprehensive, formal review by (b) (7)(E) generally (b) (7)(E).

a. Review of Cases Worked by SAs. During the Case review, the (b) (7)(E) discuss:

- the results of the investigation to date;
- progress toward objectives stated in the investigative plan;
- need for changes in the investigative plan; and
- sufficiency of administrative requirements, including but not limited to (b) (7)(E) entries and preparation of investigative reports and memoranda.

(b) (7)(E) documents the case review, noting the above discussion points in the Case Review tab (b) (7)(E).

(b) (7)(E) is also responsible for the informal review of each assigned investigation as often as necessary for effective case management.

b. Review of Cases Worked by (b) (7)(E). All investigative cases worked by (b) (7)(E) are subject to review by the (b) (7)(E). Review methodology, frequency of review, and documentation procedures are decided, on a case-by-case basis, by the (b) (7)(E).

A case is assigned to a (b) (7)(E) either by (b) (7)(E). In the latter case, (b) (7)(E) is responsible for bringing this to the attention of (b) (7)(E).

#### 906.03B Referrals To and From Office of Audits (JA)

Subchapter 705 details formal procedures used by JA to advise JI of suspected wrongdoing disclosed as a result of OIG audit work. Subchapter 706 details formal procedures used by JI to advise JA of possible management deficiencies identified during OIG investigative work.

In addition to following these formal reporting procedures, OIG SAs and auditors are expected to share professional information on an informal basis, (b) (7)(E)

#### 906.04 Collateral Investigative Leads

##### 906.04A OIG Policy on Collateral Investigative Leads

Collateral investigative leads are those requiring investigative activity outside the geographic area of responsibility of the field investigations office conducting the investigation. Such leads are normally handled by requesting assistance from the field investigations office with responsibility for the other geographical area.

##### 906.04B Requesting Assistance on Collateral Investigative Leads

(b) (7)(E) responsible for the investigation requests assistance on collateral leads by request to the other (b) (7)(E). The originating office should note the collateral referral in (b) (7)(E) under the Steps. This collateral

request must provide all background and guidance necessary for the assisting office to obtain the desired information/evidence and includes at least the following data:

- title and assignment number;
- background summary of the case;
- location (if known) of records to be examined/obtained;
- names and addresses (if known) of persons to be interviewed;
- pertinent questions that need to be answered;
- copies of any documents the assisting agent will need to complete the collateral request; and
- requested completion date for the investigative work on the collateral leads.

#### 906.04C Responding to Requests for Assistance on Collateral Investigative Leads

Collateral request should be completed within (b) (7)(E) and the assisting office provides a response to (b) (7)(E) to include:

- a brief summary of actions and results; an
- any documents, evidence, and original records of interview acquired during the collateral investigation (as attachments).

In any cases where the assisting (b) (7)(E) is unable to complete the investigative work by the requested date, he/she notifies the requesting office no later than that date, outlining the reasons for the delay and providing an estimated completion date.

#### 906.05 Case Closing

1. Responsibilities for Case Closing. Case closing decisions are made by (b) (7)(E).

2. Procedures for Case Closing. Procedures for case closing are as follows:

- The case agent prepares the Case Closing Authorization in (b) (7)(E) which is electronically submitted to (b) (7)(E).
- (b) (7)(E) approves the case closing; and, where the case is being closed without a referral, justifies the closing in the comments section on the case closing form.

(b) (7)(E) ensures that a case closing memorandum has been included and all necessary (b) (7)(E) entries are made to close the case.

906.05A Retention and Disposition of Investigative Records

Retention and disposition of the OIG's official case files, captured in (b) (7)(E) is the responsibility of JI Headquarters and is performed in accordance with GSA OIG File Plan (GSA OIG Policy 407.03).

Closed Case-Bulk File Storage

In preparation for case closing, (b) (7)(E) for the required retention period. Process for storage can include:

(b) (7)(E)

Effective Date 1/3/2014

## 907.00 HOTLINE POLICIES AND PROCEDURES

### 907.01 OIG Hotline

#### 907.01A Organization, Management, and Scope of the Hotline Function

The OIG hotline function is located within the Investigations Operations Division (JIB). It is operated by the (b) (7)(E) of the GSA Hotline who reports to the Deputy Assistant Inspector General for Investigation (DAIGI), who in turn reports to the Assistant Inspector General for Investigations (AIGI). The hotline will also be staffed by other OIG personnel, henceforth referred to as hotline officers.

The hotline function handles all complaints:

- referred to the OIG by GAO;
- received in the mail that are addressed to the hotline officer;
- received in the mail that are addressed to other Central Office OIG officials, but could best be resolved through the hotline function;
- received by other agency hotlines and referred for GSA/OIG hotline action;
- made in person by walk-in hotline complainants;
- received on the OIG's hotline telephone lines or in its electronic mail; and
- received through the hotline reporting form on the OIG Internet webpage.

#### 907.01B Receiving Hotline Telephone Calls

The hotline officer monitors the hotline telephone lines during duty hours. During non- duty hours, the lines are answered by a recording device that: (1) identifies the GSA- OIG hotline; (2) gives instructions on how to register a complaint; and (3) allows the caller to leave a short message. As his/her first assignment of each workday, the hotline officer reviews all messages left on the recording device after the close of the previous business day. If callers have asked to be contacted, the hotline officer does so as soon as possible.

Every effort will be made to have the hotline phones covered during normal business hours.

1. Hotline Briefing/Coordination Actions. (b) (7)(E) the Hotline keeps the (b) (7)(E) generally apprised of complaints received and immediately briefs the (b) (7)(E) on all matters thought to be of immediate importance, such as complaints regarding a crime in progress, a situation where in life, limb or property is endangered, an allegation regarding a senior GSA management official, an allegation regarding an OIG official, a bribery situation, etc. In the absence of the (b) (7)(E) the hotline officer will directly brief the (b) (7)(E)

on all sensitive or significant situations on an expeditious basis. In the event the (b) (7)(E) is also not available, the (b) (7)(E) will be briefed.

2. Receiving Threats Against the President of the United States, Cabinet Level Members and Members of Congress. Any information received that could be interpreted as a threat against the President, the Vice President, their family members and White House staffers, members of Congress, etc., will be immediately coordinated (b) (7)(E). If the threat/information is on an answering machine, (b) (7)(E) A copy of the message will be released to (b) (7)(E) at their request.

3. Advising Callers on Policies for Protecting the Identity of Hotline Sources. The hotline officer provides advice and information to hotline complainants on the protection of identities as follows:

- When a hotline complainant asks about the degree of protection to be afforded his/her identity, the hotline officer advises that, consistent with Section 7(b) of the IG Act, the identity of a GSA employee complainant is protected from disclosure, unless such disclosure is unavoidable during the course of the investigation. Even though the IG Act addresses only Agency employee complainants, the identity of non-GSA complainants is protected to the fullest extent possible through the same operating procedures as utilized for GSA complainants.

- When a hotline complainant specifically requests confidentiality, the hotline officer provides the same information outlined above, but also explains that confidentiality can never be guaranteed, since disclosure could prove unavoidable during the course of an investigation. Section 907.01D presents additional guidance on the special procedures for protecting the identities of confidential hotline sources.

- When a hotline complainant states that he/she has no objection to being identified as the source of the complaint in any referral to Government officials, the hotline officer advises the complainant in general terms on the course such a referral could take. The purpose of this advice is to minimize any misunderstanding on the possible disclosure of identity.

4. Documenting Hotline Complaints. All telephonic and walk-in complaints will be written up on a Hotline Complaint Form (Figure 907-01). Written complaints will be processed the same as verbal complaints. (NOTE: The Hotline Complaint Form is an internal OIG document (b) (7)(E))

Upon receipt of a hotline call, the hotline officer will ascertain whether the call concerns fraud, waste, abuse or mismanagement, and whether it is GSA related.

- If the call is GSA related, the hotline officer will strive to obtain all possible information from the complainant concerning the allegations being made, i.e., who, what, when, where, why and how. An attempt will be made to obtain the (b) (7)(E)

If the complainant desires confidentiality, the procedures as set forth in Paragraph 3 above will be followed.

•Those complaints that are not GSA related will be referred to the appropriate agency's hotline office, if one exists. If a hotline office does not exist, the complaint should be referred to the agency's appropriate investigative or management authority.

#### 907.01C Initial Screening of Hotline Complaints

All hotline complaints are initially screened by the hotline officer to determine whether they should be subjected to further review/follow-up. Those complaints that lack investigative merit are assigned a file number and closed. Bona fide complaints appearing to relate to any employee, property, or operation of GSA or other Government organization are subjected to further review/follow-up. This initial screening must be completed within <sup>(b) (7)</sup> working days after receipt of the hotline complaint.

#### 907.01D Procedures for Controlling GAO and Hotline Complaints

The hotline officer uses the following procedures to track and control complaints received from GAO, and those GSA hotline complaints meriting further review/follow-up:

1. Assigning Hotline Complaint Numbers. Each opened case is assigned a computer-generated complaint number, created when the hotline officer initiates a record of the complaint in the (b) (7)(E)

2. Preparing the Electronic Hotline Case File. An electronic hotline case file is created for each hotline complaint. All documents pertaining to the complaint will be (b) (7)(E)

3. Completing Hotline Indexing and Indices Checks. The procedures pertaining to the indexing of hotline complaint information (b) (7)(E) and obtaining hotline indices checks are as follows:

•Indexing Actions: All subjects, witnesses, complainants (b) (7)(E) and victims, as well as the names of businesses, will be entered into (b) (7)(E) (Section 902.04F).

•Indices Checks: Prior to any referral action, the hotline officer will (b) (7)(E)

4. Maintaining Hotline Suspense Tickler. If the complaint is to be referred, a suspense report is generated on a (b) (7)(E) basis, indicating those hotline complaints that have not been responded to in (b) (7)(E).

5. Special Procedures for Protecting the Identities of Confidential Hotline Sources. The following special procedures apply when a hotline complainant has requested confidentiality:

•All identifying information concerning the complainant (name, position, residence and work address, home and work telephone, etc.) WILL be recorded in (b) (7)(E) under the (b) (7)(E) and coded (b) (7)(E)

- Referrals made to OIG components will NOT contain complainant's identity. Agents within a JI field office will be able to view the identity of ALL complainants in (b) (7)(E). The complainant's identity is not furnished to any other requestor.
- Referrals made outside the OIG will NOT contain the confidential source's identity, nor will this information be furnished to a non-OIG requestor. The hotline officer also removes any details from the referral that could identify the complainant.

#### 907.01E Referring GAO and Hotline Complaints

For each GAO and hotline complaint that has been assigned a complaint number, the hotline officer in coordination with the DAIGI, determines whether it: (1) has OIG investigative merit; (2) lacks OIG investigative merit, but should be brought to the attention of JA or JC; (3) lacks OIG investigative or audit merit, but should be brought to the attention of GSA management officials; or (4) relates to an agency other than GSA. The complaint is referred in accordance with this determination within JI, to JA or JC, to GSA Management Officials, or to other agencies.

1. Referrals Within JI. Complaints that have investigative merit are referred by the (b) (7)(E) and assigned to the appropriate (b) (7)(E) by the Hotline (b) (7)(E) with a suspense date of (b) (7)(E) calendar days to respond as to action taken.

If the (b) (7)(E) opens an investigation, he/she does so by converting the hotline case to an investigative case in (b) (7)(E) and (b) (7)(E). The Hotline (b) (7)(E) Files on complaints referred by GAO are kept open until all action is complete, at which time the Hotline (b) (7)(E) will forward a summary of the action taken and the final disposition of the case to GAO (Section 907.01F).

If, after receiving the referral from the (b) (7)(E) (b) (7)(E) determines that an investigation is not warranted, the (b) (7)(E) will reassign the hotline case to the Hotline (b) (7)(E). The (b) (7)(E) will explain the reason an investigation is not being opened on the complaint under the "Documents" tab in (b) (7)(E) along with his/her recommendation that the hotline complaint should be referred to JA, JC, or GSA management officials, or that the case should be closed.

2. Referrals to JA and JC. Complaints that lack OIG investigative merit but could be of interest to JA or JC are so referred, with copies of the referral provided to the appropriate SACs (b) (7)(E). The referrals, which are made by the DAIGI to the AIGA or the Counsel to the IG, request response within (b) (7)(E) calendar days. If JA initiates an audit or other project as the result of the complaint, the response to the Hotline includes the assignment number.

Unless the complaint was referred by GAO, the Hotline (b) (7)(E) then closes the hotline case file in (b) (7)(E) cross-referencing it to the JA assignment number. Files on complaints referred by GAO are kept open until all action is complete, at which time JA provides the hotline officer with a summary of the action taken. This summary is forwarded to GAO (Section 907.01D).

If JA does not initiate an audit or other project as the result of the complaint, all material is returned, using the hotline complaint number, to the Hotline (b) (7)(E). The Hotline (b) (7)(E) in conjunction with the AIGI, determines whether or not the complaint should be referred to GSA management officials.

3. Referrals to GSA Management Officials. Complaints that relate solely to management are referred by the AIGI to the appropriate management officials with a suspense date of (b) (7)(E) calendar days to respond. Referrals to a region are directed to (b) (7)(E). Informational copies of all referrals to GSA regional officials are sent to the appropriate (b) (7)(E).

The Hotline (b) (7)(E) in conjunction with the (b) (7)(E) evaluates each management response for completeness and specific coverage of the complaint. A management response that does not fully or directly address the complaint is referred back to the management official. The hotline case is closed only when a fully satisfactory response has been received.

4. Referrals to Other Agencies. Complaints are referred to other agencies in accordance with the following guidelines:

- Complaints received from GAO that do not relate to GSA employees or programs are returned to GAO, with appropriate explanation.
- Hotline complaints that appear to relate entirely to an agency other than GSA are referred to that agency, and the hotline case is closed. The complaint referral letter, transmitted by the (b) (7)(E) asks that the OIG be notified if inquiry into the complaint discloses any GSA-related issue, but does not request a routine response. Copies of such referrals are provided to the appropriate (b) (7)(E).
- The third category of referrals to other agencies consists of GAO and hotline complaints that involve GSA employees or programs, but are within the action responsibility of another agency. In this case, the referral is by cover letter from the (b) (7)(E) which requests notification on the results of the other agency's inquiry. Copies of such referrals are provided to the appropriate (b) (7)(E).

#### 907.01F Following Up on Referrals of GAO and Hotline Complaints

All responses to a hotline complaint are (b) (7)(E) prior to closing the hotline case. When the response to a complaint referral is not received by the specified deadline, the hotline officer telephones the responsible party to determine the status of the response. A request for extension of the due date is generally granted. However, when there is continued failure to meet specified deadlines, the AIGI sends a written request for the current status and the projected completion date.

In the case of complaints referred by GAO, the OIG is required to: (1) notify GAO of initial disposition within (b) (7)(E) days; and (2) notify GAO of final disposition. Case files on GAO complaints are kept open until completion of all action related to the complaints (Section 907.01E). The hotline officer follows up on each such referral every (b) (7)(E) days after the initial response to the referral, until all action on the complaint is completed. These follow-up procedures are modified only when the action office has projected a later completion date.

Effective Date 2/5/2014

## 908.00 RELATIONSHIPS WITH PROSECUTIVE AUTHORITIES, OTHER LAW ENFORCEMENT AGENCIES, AND AGENCY OFFICIALS

### 908.01 Office of Investigations Relationships With Prosecutive Authorities, Other Law Enforcement Agencies and GSA Officials

#### 908.01A JI Relationship with Offices of U.S. Attorneys

The Attorney General's Guidelines for the Office of Inspectors General with Statutory Law Enforcement Authority dated December 8, 2003 (Figure 901-02) establishes procedures for consultations with prosecutors.

Special Agents in Charge (SACs) and Special Agents (SAs) are expected to establish working relationships with U.S. Attorneys' Offices that permit both formal and informal discussion of OIG investigative cases.

Formal presentation of investigative cases to U.S. Attorneys' offices normally occurs after completion of all investigative steps (Subchapter 919). However, SAs are expected to consult with U.S. Attorneys' offices as soon as information is developed that indicates the investigation may corroborate an allegation of a criminal violation. The purpose of this early consultation is to focus investigative effort on cases with prosecutive potential, and to ensure that the investigation fully supports that potential.

When early consultation results in a U.S. Attorney decision to accept the case, decline the case, refer the case to another investigative source, or initiate any grand jury process relating to the case, the SA follows the procedures detailed in Subchapter 919.

When early consultation results in a case being accepted for prosecution, the Report of Investigation should be prepared as appropriate for the AUSA's needs. When early consultation results in the U.S. Attorney requesting additional information or OIG investigative work, the SA documents the early consultation in the case file and proceeds to take the requested actions. Agents should ensure that all investigative activity, both exculpatory and incriminating, is recorded in the official case file. Early consultations that result in requests for additional information or investigative work are noted in the [REDACTED]

2

2 The prior concurrence of a prosecutor also is required for certain situations (b) (7)(E) [REDACTED], as set forth in Chapter 915.

#### 908.01B JI Relationship with the DOJ Antitrust Division

Since 1982, the DOJ Antitrust Division has placed special emphasis on working with the OIG to address anti-competitive practices affecting the Government acquisition process, particularly when those practices are provable violations of anti-trust statutes. In support of this emphasis, OIG investigative cases indicating patterns of collusion, bid-rigging, and other anti-competitive schemes are referred to

the Antitrust Division. The Antitrust Division considers the cases for criminal or civil prosecution and coordinates its activities with Offices of U.S. Attorneys and other DOJ components, as appropriate.

The SAC serves as the OIG's point of contact with the Antitrust Division.

#### 908.01C JI Relationship with the FBI

The Attorney General's Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority dated December 8, 2003 (Figure 901-02) establishes the responsibility for notification of investigation of criminal activity involving General Services Administration (GSA) programs and operations.

The Guidelines establish mutual notification requirements. As the primary investigative arm of the DOJ, the FBI has jurisdiction in all matters involving fraud against the federal government and shares jurisdiction with the OIG in the investigation of fraud against GSA. In such areas of concurrent jurisdiction, the OIG and the FBI must notify each other in writing within (b) (7)(E) calendar days of the initiation of any criminal investigation

Notification is addressed to the FBI in the district in which the investigation is being conducted. Notification by the FBI also is (b) (7)(E) and addressed to the appropriate regional office of the OIG. Notification includes, at a minimum: (a) subject name, date of birth, social security number and any other identifying information including, but not limited to, (b) date the case was opened or the allegation was received, and (c) the allegation on which the case was predicated. In investigations where allegations arise which are beyond the scope of the OIG's jurisdiction, the OIG immediately notifies the appropriate investigative agency of the allegation.

#### 908.01D JI Relationship with Other Law Enforcement Agencies

Upon determining that a complaint or allegation that warrants investigation does not pertain to GSA, the SAC will refer the complaint/allegation to another law enforcement agency. Generally, a complaint or allegation is referred to another law enforcement agency when one or more of the following conditions applies:

- The subject matter is either traditionally or by law investigated by another agency.
- The complaint/allegation does not involve GSA employees, programs, or property.
- The complaint/allegation indirectly involves GSA employees, programs, or property, but it has a major impact on another agency.
- The complaint/allegation involves GSA programs or property, but it can be more effectively pursued by the DHS Federal Protective Service.
- The complaint/allegation involves a threat to the safety of the President or any other protectee or responsibility of the U.S. Secret Service.

1. Standard Procedures for Referrals to Other Law Enforcement Agencies. The standard procedures governing OIG referrals to other law enforcement agencies are as follows:

- The referrals are made by the SAC to the head of the other agency's local office having jurisdiction over the geographical area where the wrongdoing allegedly occurred.
- Except in exigent circumstances, referrals within GSA are by memoranda; and referrals outside GSA are by letters. Referrals may initially be made telephonically or in person, but they should be confirmed in writing for appropriate documentation.
- Referral memoranda/letters contain:
  - a presentation of the complaint/allegation, along with any facts developed by the OIG;
  - a statement that the matter is being referred for informational purposes and any action deemed appropriate;
  - when appropriate, an offer of OIG assistance and support (with the provisions of the OIG/FBI memorandum of understanding used as guidelines for suggested joint investigations); and
  - when the referral involves GSA employees, programs or operations normally a GSA-OIG investigation will be initiated and the case will be investigated jointly with the other agency.

2. Special Procedures for Referral of Matters Involving Threats against Government Officials. The U.S. Secret Service is responsible for protecting the President, Vice- President, President-elect, certain other Government officials, Presidential family members, the Executive Mansion, and foreign diplomatic missions in the Washington, D.C. area. SAs who receive information indicating a potential threat within U.S. Secret Service jurisdiction should immediately report that information to the nearest U.S. Secret Service office or the U.S. Secret Service Intelligence Division, Washington, D.C.

Information indicating threats to Government officials or Presidential and Vice- Presidential candidates not receiving U.S. Secret Service protection should be reported immediately to the nearest FBI office.

#### 908.01E JI Relationship with State and Local Prosecutors

When Federal prosecutors decline OIG referrals (or express no Federal interest during early consultation on an investigative case), SAs should be alert for opportunities to seek prosecution by state and local authorities. Examples of violations encountered in OIG investigations that could be prosecuted in state and local courts are: misuse of Government credit cards; criminal trespass; false utterances (bad checks); and theft of Government property from non-Federal premises.

When state or local prosecutors accept OIG cases, OIG SAs provide assistance and follow the same administrative and reporting procedures as in Federal prosecutions.

## 908.01F JI Relationship with the Office of Special Counsel

JI's relationship with the Office of Special Counsel is defined in Subchapter 603.

## 908.01G JI Relationships with GSA Officials

The OIG's general policy is to keep Heads of Services and Staff Offices (HSSO) and Regional Administrators (RAs) informed of investigative activity by advising these officials of: (1) new investigations, (2) the status of ongoing investigations, and (3) JI action decisions on complaints/allegations forwarded by these management officials. Special Agents in Charge (SACs) are responsible for keeping the RAs informed of their investigative activity; the Assistant Inspector General for Investigations (AIGI) is responsible for keeping the HSSOs apprised of investigative activities. In order to prevent compromising investigations through such disclosure of information – the responsible JI officials are generally expected to exercise judgment, on a case-by-case basis, as to the need for and extent of notification.

1. SAC Notifications to RA. The cognizant SAC notifies the RA as appropriate of investigations in the Administrator's region. The SAC also provides feedback on all referrals/complaints forwarded by the RA, including OIG determinations as to whether an investigation is warranted.

2. AIGI Notifications to HSSOs. (b) (7)(E) whenever: (1) a case is opened involving a GSA Central Office service or staff office, and/or (2) an ongoing case discloses information involving a GSA Central Office service or staff office. Such notification occurs (b) (7)(E)

The (b) (7)(E) briefs the (b) (7)(E) on the investigation as soon as possible after (b) (7)(E) notification. The (b) (7)(E) in turn, briefs the (b) (7)(E), who at his/her discretion may brief HSSO or the GSA Office of the Administrator in accordance with mutually agreed upon methods.

Referrals/complaints by HSSOs for investigative consideration are normally received in the OIG Central Office and processed for investigative determination by the (b) (7)(E). (b) (7)(E) should (b) (7)(E) notify the (b) (7)(E) regarding any referral or complaint received from an HSSO.

The (b) (7)(E) briefs the (b) (7)(E) as to the investigative determinations regarding referrals/complaints by HSSOs. The (b) (7)(E) then notifies the (b) (7)(E) who at his/her discretion may brief the HSSO in accordance with the mutually agreed upon method of notification.

Effective Date 2/5/2014

## 909.00 TRANSMITTING AND SAFEGUARDING CONTROLLED UNCLASSIFIED INFORMATION

### 909.01 Transmitting and Safeguarding Controlled Unclassified Information

Special Agents (SAs) should be familiar with all applicable policies regarding the protection of information. In addition to those policies, SAs should become familiar with the May 9, 2008, Memorandum for the Heads of Executive Departments and Agencies, "Designation and Sharing of Controlled Unclassified Information" (Figure 909-01). For the purposes of sharing Controlled Unclassified Information the designation "For Official Use Only" will be used by the Office of Investigations (JI).

### 909.02 Procedures for Transmitting and Safeguarding "For Official Use Only" Information

The following paragraphs detail: (1) special procedures for transmitting items of evidence, subpoenaed materials, and equally sensitive material; and (2) standard procedures for transmitting "For Official Use Only" information between the Office of Investigations (JI) and field investigations offices; from JI to Regional Administrators (RAs); from field investigations offices to RAs; from JI to GSA Central Office officials; and from JI components to U.S. Attorneys and other agencies.

#### 909.02A Special Procedures for Transmitting Items of Evidence, Subpoenaed Materials, and Equally Sensitive Information

When information is being mailed (b) (7)(E) on an open investigation, the information is sent via authorized (b) (7)(E).

#### 909.02B Standard Procedures for Transmitting "For Official Use Only" Information Between JI and Field Investigations Offices

The following procedures apply when "For Official Use Only" information is being mailed between JI and field investigations offices:

1. The information is sent as described in Section 909.02A.
2. When the information relates to (b) (7)(E) matters (such as (b) (7)(E), it is contained in (b) (7)(E).

#### 909.02C Standard Procedures for Transmitting "For Official Use Only" Information From JI to RAs.

The following procedures apply when JI transmits "For Official Use Only" information to RAs:

1. Correspondence to the RA, National Capital Region, is sent (b) (7)(E) [redacted]  
When reports of investigation are being transmitted, (b) (7)(E) [redacted] (Figure 909-02) is  
attached to the (b) (7)(E) [redacted]

2. Correspondence to RAs outside the National Capital Region that transmits (b) (7)(E) [redacted]  
[redacted] is sent via authorized (b) (7)(E) [redacted]

3. Other "For Official Use Only" correspondence to RAs outside the National Capital Region is sent via  
authorized (b) (7)(E) [redacted]

#### 909.02D Standard Procedures for Transmitting "For Official Use Only" Information From Field Investigations Offices to RAs

The information is either (b) (7)(E) [redacted]. When Reports  
of Investigation are being transmitted, (b) (7)(E) [redacted]  
[redacted]

#### 909.02E Standard Procedures for Transmitting "For Official Use Only" Information From JI to GSA Central Office Officials

Correspondence transmitting (b) (7)(E) [redacted] to officials located in the GSA headquarters  
building is (b) (7)(E) [redacted]. The information is contained in (b) (7)(E) [redacted]  
[redacted]. Correspondence transmitting (b) (7)(E) [redacted] to Central Office officials located  
outside the GSA headquarters building are sent via (b) (7)(E) [redacted]

[redacted] All other correspondence to  
Central Office officials is sent (b) (7)(E) [redacted].

#### 909.02F Standard Procedures for Transmitting "For Official Use Only" Information From JI Offices to U.S. Attorneys or Other Government Agencies

Jl offices either (b) (7)(E) [redacted] "For Official Use Only" information to U.S. Attorneys and other agencies, or  
they send it via authorized (b) (7)(E) [redacted] When (b) (7)(E) [redacted]  
[redacted] are being transmitted, (b) (7)(E) [redacted]  
[redacted]

Effective Date 10/3/2017

## 910.00 POLICY AND PROCEDURES FOR GRAND JURY MATERIALS

### 910.00 Purpose

This subchapter details the special handling requirements for information obtained through the use of the grand jury process.

### 910.01 Scope

Provisions of this section apply to all personnel in the OIG who will have access to grand jury information.

### 910.02 Grand Jury Information

Federal Rules of Criminal Procedure, Fed. R. Crim. P. 6(e), (Figure 910-01) protects from disclosure "matters occurring before the grand jury." There have been many court decisions interpreting this rule; however, many decisions have been piecemeal (i.e. interpreting whether a specific item is afforded protection) and the decisions vary among jurisdictions. For the OIG's purpose, the following materials and information should be treated as "matters occurring before the grand jury" and should not be disclosed to anyone who is not on the applicable grand jury list:

1. Transcripts of witness testimony, statements made by government attorneys before the grand jury, and any other statements made by or before the grand jury.
2. Documents that record or summarize any statement or action taken before or by a grand jury, including summaries of witness statements which identify information witnesses presented before the grand jury. Such documents include prosecutive referrals which contain such information.
3. Documents which are obtained in response to grand jury subpoenas, including lists or summaries of such documents. In addition, as necessary, SAs should ask the AUSA assigned to the case whether jurisdictional court rules or decisions prohibit the SA's access to these materials until after they are presented to the grand jury.
4. Documents or information identifying grand jury witnesses and the targets of grand jury investigations.
5. Grand jury subpoenas are specifically prohibited from disclosure by Rule 6(e)(6).
6. Disclosure of information which the OIG gathers from a source independent of the grand jury proceeding is not restricted by Rule 6(e) simply because the information is subsequently presented to a grand jury or because the related investigation becomes the subject of a grand jury inquiry. However,

the presentation of these materials or statements before the grand jury is considered a matter occurring before the grand jury and must be protected from disclosure.

#### 910.03 Policy

To the extent possible, OIG SAs (b) (7)(E) [REDACTED] This will ensure that the information and evidence obtained during an investigation can be used for appropriate (b) (7)(E) [REDACTED]

#### 910.04 Limitations on Use of Grand Jury Materials

1. Rule 6(e) provides in part that anyone to whom grand jury matters are properly disclosed, "may use that information only to assist an attorney for the government in performing that attorney's duty to enforce federal criminal law."
2. Only OIG employees in receipt of a Rule 6(e) letter from the U.S. Attorney shall have access to grand jury information unless otherwise provided for by exemption.

#### 910.05 Responsibilities

(b) (7)(E) [REDACTED] are responsible for the following:

1. Monitoring the implementation of this section in their respective regional offices.
2. Providing secure storage for any grand jury information located in their respective offices.
3. Ensuring grand jury information is not disclosed to unauthorized personnel unless a Rule 6(e) disclosure court order has been obtained or exemption exists.
4. Instructing (b) (7)(E) [REDACTED] regarding the proper handling of grand jury information.
5. Providing guidance to any OIG employee assigned to assist in a grand jury investigation or who otherwise has access to grand jury material.
6. Ensuring that report(s) issued to agency officials contain no grand jury information.
7. Ensuring that grand jury information is properly disposed of when no longer needed.

(b) (7)(E) [REDACTED] are responsible for the following:

1. Furnishing the U.S. Attorney the identity of those requiring a Rule 6(e) letter.
2. Handling grand jury information so that it is at all times secure from inadvertent or intentional observation by anyone not approved for disclosure.
3. Providing only to those OIG employees in receipt of a Rule 6(e) letter or otherwise exempted, excerpts or summaries of grand jury testimony, information obtained by grand jury subpoena, or information developed through the use of grand jury testimony or subpoena.

4. Maintaining security over all grand jury information and ensuring proper storage.
5. Ensuring all grand jury protected documents/entries in the electronic case management system are properly marked (b) (7)(E) [REDACTED]  
This ensures GJ documents are only accessible by those listed with grand jury rights on the staff tab.

#### 910.06 Procedures

When grand jury assistance is necessary to pursue a criminal investigation, or when the OIG assists in a grand jury investigation, all information from the grand jury shall be safeguarded as required by Rule 6(e), Federal Rules of Criminal Procedure, from unauthorized disclosure. The SA will ask the AUSA to advise on any local rules and procedures which might affect Grand Jury Instructions. When requested, the SA may be asked by the AUSA to provide the names of OIG personnel who require access to such information. In addition, it is common practice to provide the names of OIG management to include the SAC, ASAC, DAIGI, AIGI, DIG, and IG, as these individuals are in the supervisory line and may access case information.

#### 910.07 Safeguards During Use

All grand jury information shall be:

1. When in use, (b) (7)(E) [REDACTED] by an authorized person who is in a position to exercise direct physical control over the material.
2. (b) (7)(E) [REDACTED]  
[REDACTED] from persons who should not have access.
3. Returned to proper secured storage containers as soon as practical after use.
4. Grand jury materials must not be disclosed to unauthorized parties. If grand jury materials must be transmitted, they should ideally be (b) (7)(E) [REDACTED]. (b) (7)(E) [REDACTED]

Grand jury material may also be sent (b) (7)(E) [REDACTED], but the material (b) (7)(E) [REDACTED]

#### 910.08 Storage Requirements

Grand jury evidence must be kept under tight physical security and identified as grand jury material.

Grand jury material may be (b) (7)(E) [REDACTED]

It should be (b) (7)(E) [REDACTED]

Access to grand jury information will only be for authorized individuals in possession of a Rule 6(e) letter for the investigation.

(b) (7)(E) [REDACTED] may require additional safeguards for protection of grand jury information if, in their opinion, the information warrants additional protection.

#### 910.09 Return of Grand Jury Information

All grand jury information will be returned to the U.S. Attorney at the termination of the investigation. If requested by the U.S. Attorney such material may be destroyed by OIG personnel or returned to the supplier/originator.

The ultimate method of disposal will be approved through the U.S. Attorney.

The method and authority used to dispose of grand jury information shall be noted, generally in the Chron Log.

After case closure if retention of the grand jury information is required the grand jury information should be appropriately secured, sealed, and marked GRAND JURY INFORMATION. (Refer to Section 925 of this manual for further information on Grand Jury Material used as evidence.) Unless otherwise instructed, original grand jury information can be destroyed or properly disposed of at case closure.

Effective Date 9/28/2017

## 911.00 MEDICAL STANDARDS FOR OIG SPECIAL AGENTS

### 911.01 General

The duties of a Special Agent (SA), job series GS-1811, in the General Services Administration (GSA) Office of Inspector General (OIG), include federal law enforcement activities, which can be physically demanding and dangerous. The OIG is responsible for ensuring that OIG SAs are physically, mentally and medically qualified for the position they hold. In the interest of fostering the health and well-being of SAs, the OIG permits them, while on duty, to engage in a voluntary physical fitness program (See Section 911.06).

#### 911.01A Purpose

This chapter provides an overview of the policies and procedures concerning medical standards for all levels of OIG Special Agent positions, GS-1811, supervisory and non-supervisory. These terms generally will be used interchangeably in this subchapter.

#### 911.01B Regulatory Requirements

OPM guidance and regulations governing these medical requirements are set forth in (1) OPM Medical Requirements for GS-1811 positions; (2) 5 CFR Part 339 Medical Qualification Determinations; (3) 5 CFR Part 831, Subpart I, Law Enforcement Officers and Firefighters (under the Civil Service Retirement System); and (4) 5 CFR Part 842, Subpart H, Law Enforcement Officers, Firefighters, and Air Traffic Controllers (under the Federal Employees Retirement System).

#### 911.01C Background

OPM has established minimal physical requirements as a part of the qualification standards for SAs, or criminal investigators. OPM determined that the duties of these positions require, among other things, moderate to arduous physical exertion involving walking and standing, use of firearms, and exposure to inclement weather.

These regulatory authorities permit agencies to establish appropriate medical qualification standards for entry and retention as law enforcement officers. These standards are applied in hiring and retaining SAs. The OIG has determined that (b) (7)(E) [REDACTED] The OIG is responsible for ensuring that SAs are physically and medically qualified for these positions.

Consistent with these requirements, the OIG has contracted (b) (7)(E) to provide medical examinations/evaluations and related professional services, including consultation and advisory services. Pertinent medical examinations will be performed by 'examining physicians' and reviewed by a Medical Review Officer (MRO), all of whom are under the purview of (b) (7)(E). The resources of (b) (7)(E) will also be available to OIG managers who observe or are otherwise made aware of potential situations that could affect a SA's physical condition or mental stability.

## 911.02 Coverage

### 911.02A Scope

The medical standards will apply to all GS-1811 series SAs within the OIG. The SA position is both physically demanding and potentially dangerous. The position has substantial productivity demands and a hectic schedule. The accompanying physical requirements and medical standards reflect the nature of this position.

### 911.02B Policy

The OIG requires that all SAs and applicants submit to medical examinations and evaluations as required under this chapter and be certified as medically fit for duty by the MRO prior to or as a condition of continuing duty with the OIG. An SA may elect to submit medical information from his or her own medical practitioner for review and consideration by the MRO, or to consult with his/her personal physician at any time, but this will not replace the required (b) (7)(E) medical examination. (Any such submittal must be accompanied by a Health Insurance Portability and Accountability Act (HIPAA) release; see section 911.05H.)

All applicants for the position of criminal investigator will be required to undergo a post-offer medical examination to determine if the applicant is physically and medically qualified to perform the full duties of the position as defined by the Office of Personnel Management. In addition, incumbent SAs will undergo periodic medical examinations by (b) (7)(E) designated physicians to assess their medical fitness to continue work in an unrestricted manner.

The physical examinations shall be guided by these standards.

1. The examining physician must report on any physical condition identified during the medical examination that could potentially restrict or disqualify a SA from full employment in this position. The MRO shall ensure that detailed medical reasoning is provided to the OIG. Applicants or incumbents will be disqualified if they pose a "direct threat" to the health and safety of themselves or others.
2. Applicants who refuse to submit to a pre appointment medical examination will not be considered for employment. Any incumbent SA who refuses to submit to a required medical examination may be subject to appropriate disciplinary action. OIG managers will treat such cases as potential performance or conduct problems, and coordinate with the Director of Human Resources and Counsel to the IG for further guidance.

3. Throughout the examination process and its aftermath, the employee's right to privacy will be safeguarded through protection of the confidentiality of medical records in accordance with the Privacy Act.

4. All incumbent SAs will be required to take a medical examination (b) (7)(E) to determine their continued medical fitness for duty as an OIG SA. The OIG Physical Exam components for incumbents are:

- general physical exam;

- health history;

(b) (7)(E)

[REDACTED]

[REDACTED]

- resting EKG;

- visual screen (corrected & uncorrected, near & far, each eye & binocular, color, depth and peripheral);

- audiogram; and

- tonometry.

5. The GSA-OIG Physical Exam components for applicants are:

- general physical exam;

- health history;

(b) (7)(E)

[REDACTED]

- resting EKG;

- visual screen (corrected & uncorrected, near & far, each eye & binocular, color depth and peripheral);

- audiogram;

- spirometry (lung test);

- PPD Mantoux (TB test); and

- tonometry.

6. The OIG will bear all costs associated with required medical examinations. Should the SA not meet the medical standards and require additional testing, medical examination, or treatment, the SA will bear the cost associated for any additional testing, examination, or treatment by a private physician.

7. Testing dates for the periodic medical examinations will be generally scheduled on or about (b) (7)(E)

[REDACTED] SAs are to bring with them to the scheduled examination a copy of the OIG Physical Evaluation Form (Figure 911-01) with the shaded portions completed.

8. In between regularly scheduled examinations, if a SAC/ASAC has concerns about a SA's fitness for duty or mental/emotional stability for work, the SAC/ASAC (b) (7)(E) the SAC/ASAC may consult with the MRO and as appropriate direct an SA to be examined/evaluated by (b) (7)(E) personnel. Separate from this medical evaluation, as stated in section 902.07, supervisory personnel or their designees, are authorized (b) (7)(E) from a SA when, in their judgment, such (b) (7)(E) is in the best interest of the SA, OIG, or the safety of others. Supervisory personnel or their designees also are authorized to retrieve a SA's (b) (7)(E) under these same circumstances.

9. OIG SAs are required to inform their immediate supervisor whenever they have reason to believe (b) (7)(E)

### 911.03 Functional Requirements and Environmental Factors

#### 911.03A Functional Requirements

The duties of an OIG SA, require moderate to arduous physical exertion involving walking, standing, use of firearms, operating a vehicle, exposure to all forms of weather, irregular hours, and/or being on 24 hour call. The SA must present investigative findings in both oral and written form, and be able to testify before grand juries, courts, and administrative hearings. The SA must be able to analyze criminal intent, activities, and behavior patterns as well as recommend appropriate action. The SA must be able to drive government vehicles. Surveillance work may require maneuvering and use of ladders, working at heights, using and interpreting various gauges, performing skilled work with hand tools, and entering into confined spaces. Since work is often conducted in "teams," SAs must also be able to work with other OIG SAs and personnel from other agencies.

1. SAs must possess the following general attributes in order to perform the duties of the position of SA satisfactorily:

- arms, hands, legs and feet intact and functioning;
- full range of motion of all joints, limbs and trunk;
- good manual dexterity and eye-hand coordination;
- average strength for age and build;
- acceptable eyesight;
- acceptable hearing (even with background noise);
- normal vocal abilities;
- emotional and mental stability;
- no exceptional fear of confined spaces, heights;
- above average poise and good judgment;

- ability to concentrate intensely;
- ability to work long periods of overtime; and

(b) (7)(E)

2. In general, the SA must have no physical impairments that would prevent the performance of each essential function as described herein. These include running, bending, walking, searching crime scenes for evidence, recording crime scenes using photography or sketches, conducting covert and overt surveillance, interviewing suspects and providing written reports, administering oaths, carrying and potentially using firearms, serving search warrants and subpoenas, performing searches, apprehending suspects, driving, lifting, climbing, and using specialized equipment.

#### 911.03B Environmental Factors

The environmental factors related to the position of the OIG SA include working inside and outside, excessive heat, excessive cold, excessive humidity, excessive dampness or chilling, and dry atmospheric conditions.

#### 911.04 Medical Standards

##### 911.04A Purpose

The purpose of adopting medical standards is to:

1. Have valid, rational, uniform medical guidance regarding the selection of employees for GS-1811 positions.
2. Provide realistic measures to ensure that employees in the GS-1811 position are physically and mentally capable of safely and efficiently performing the essential duties and responsibilities of the position.
3. Orient the MRO to the medical disorders and physical conditions that could render an applicant/employee unable to meet the functional requirements for the position of OIG SA or that could place the employee, coworkers, or the general public at risk.
4. Provide a consistent basis for the MRO to evaluate an applicant's/SA's medical fitness for duty.

##### 911.04B Applicability

These standards establish minimal satisfactory physical and medical standards. All SAs are expected to perform the same tasks and should therefore possess the same minimal physical and mental capacities regardless of age, sex, size, or genetic endowment. These standards are used to ensure consistency and uniformity in the application of the guidelines set forth in 5 CFR Part 339, Medical Qualifications Determinations. Any other disease, condition or impairment, not specifically listed in the medical

standards below, which interferes with the safe, efficient and expected performance of the duties and responsibilities of the position, may also constitute grounds for medical disqualification.

#### 911.04C Medical Conditions

1. The medical conditions listed below will be considered during the review of the applicant's/SA's medical history and the physical examination. They are not intended to be all encompassing. Rather, they are provided to aid the examining physician and to provide guidance in what medical conditions might hinder the SA's ability to satisfactorily perform the essential functions of the job without causing undue risk to themselves or others.

2. Individualized assessments will be made on a case-by-case basis to determine an individual's ability to meet the performance-related requirements of an 1811 position. A final medical determination may require additional medical information and/or testing that is not routinely required.

#### 3. Vision Standard.

a. Any disease or condition which interferes with a person's vision may be considered disqualifying. Cases will be reviewed on a case-by-case basis. Vision standards include:

- Corrected distant visual acuity must be 20/30 or better measured with both eyes viewing;
- Corrected distant visual acuity must be 20/200 or better in the worst eye;
- Complete loss of vision in one eye is disqualifying;

4. Abnormal color vision with severe color deficiency in any color is generally disqualifying. Must be able to pass standard Farnsworth D-15 color vision test. The use of X-Chrom contact lenses or tinted spectacle lenses are not permitted in the testing of color vision; and Visual fields must be full with good peripheral vision. Any history of eye disease or any medical condition likely to cause eye disease, such as retinopathy, glaucoma, retinitis pigmentosa, or retinal detachment will require visual field evaluation by an optometrist or ophthalmologist.

#### 5. Hearing Standard.

a. Any disease or condition which interferes with the ability to hear or interferes with an individual's equilibrium may be considered disqualifying. Cases will be reviewed on a case-by-case basis. The ability to hear is acceptable if the individual meets the following standards:

- In the frequency range from 500-2000 hertz (Hz), the deficit should not exceed 30 decibels in either ear;
- At 3000 Hz, the deficit should not exceed 40 decibels in either ear;
- Hearing in both ears is required. Complete loss of hearing in one ear is disqualifying; and
- The use of any hearing aid to comply with the medical standards is unacceptable.

b. If the pure audiogram standards are not met, additional testing may be performed. The MRO in his/her discretion, before rendering a final medical opinion, may require that either the pure tone

audiogram be repeated after a 14-15 hour noise-free period or additional speech audiometry testing by an audiologist or an Ear, Nose, Throat physician.

6. This speech audiometry testing will consist of:

a. Pure tone air conduction audiogram at the frequencies 250, 500, 1000, 2000, 3000, 4000, 6000 and 8000 Hz.

b. Bone conduction thresholds at 500, 1000, 2000, 3000 and 4000 Hz, with appropriate masking as needed;

c. Tympanometry, including acoustic reflex testing (ipsilateral stimulation at 500,1000, 2000, and 4000 Hz0);

d. Unaided speech reception threshold for each ear under earphones;

e. Unaided speech recognition in quiet for each ear under headphones. Start at +40 dB SL, and present recorded version of NU-6 full list. If client achieves a score of 90% or better, this phase of the test may be terminated and results reported. If a score of less than 90% is obtained, vary presentation level either up or down as appropriate to achieve maximum score. Report %/Intensity function; and

f. Unaided sound field speech recognition in noise. With client facing the speaker, using signal to noise ratio of +10 dB, signal and noise simultaneously emanating from a single speaker, using recorded NU-6 full list in speech noise. Begin at a presentation level of 60 dB HL with 50 dB HL of speech noise. If a score of 50% or better is obtained, test may be terminated. If a score of less than 50% is obtained, vary presentation level up or down to achieve maximum score. Patient may move his/her head to maximize performance. Signal-to-noise ratio of +10 dB must be maintained.

7. Speech audiometry requirements consist of:

a. Pure Tone Audiogram. The average threshold at 500, 1000, 2000, and 3000 Hz, derived by measuring thresholds at these frequencies individually in each ear, adding these values together, and dividing the total by 4, shall not exceed 30 dB HL;

b. Unilateral Hearing Loss. Sensitivity between the two ears must not differ by 25 dB or more at three of the four speech frequencies (500, 1000, 2000, 3000 Hz);

c. Speech Reception Threshold (SRT). The speech reception threshold provides a measure of the quietest or softest speech that an individual can hear and understand under quiet conditions. This measure of detection relates to demands to hear soft whispers and other speech sounds that may alert the SA to danger or the presence of suspects. Since normal hearing is required to hear very faint sounds, and since the ability to hear soft sounds is not dependent on where the sound is coming from (localization ability), the SRT must be 25dB or better in at least one ear;

d. Speech Recognition in Quiet. Because of the critical nature of speech understanding, a stringent cut-off of 90% or better is required for a 50 word-list in quiet conditions; and

e. Speech Recognition in Noise Sound Field. An intelligibility score of 50% in a +10 dB signal-to-noise ratio is required in a non-reverberant environment.

8. Head, Nose, Mouth, Throat and Neck Standard.

a. Any medical condition that significantly interferes with the individual's ability to successfully perform essential law enforcement functions, such as speech or breathing, or that has the potential to render the person suddenly incapacitated will generally be disqualifying. All instances will be reviewed on a case-by-case basis.

#### 9. Cardiovascular System Standard.

a. Any disease or condition that interferes with cardiovascular function and the safe and efficient performance of the job is generally disqualifying. Instances will be reviewed on a case-by-case basis. Examples of impairments are pacemakers or prosthetic valves, coronary artery disease, hypertension, pulmonary embolism, angina pectoris, congestive heart failure, congenital anomalies, chronic venous insufficiency, deep vein thrombosis, aortic aneurysm and history of syncope.

b. Cardiology evaluation and/or maximal, symptom-limited exercise stress EKG may be required to determine whether an individual is capable of safe and efficient job performance. All medications taken for cardiovascular conditions are carefully reviewed to insure that they do not compromise job performance and therefore interfere with safe and efficient job performance. Any history of a cardiovascular condition is evaluated on a case-by-case basis and may require further evaluation.

c. Confirmation of hypertension requires at least three serial readings of blood pressure. Serial readings must include at least three blood pressure readings taken on different days and should include readings in both arms in a standing, sitting, and recumbent position.

#### 10. Chest and Respiratory System Standard.

a. Any disease or condition, which interferes with respiratory function and/or safe and efficient job performance, may be considered disqualifying. Instances will be reviewed on a case-by-case basis. Examples of impairments include asthma, chronic bronchitis, lung abscess, emphysema, pulmonary embolism and tumors of the lung.

b. Pulmonary evaluation, chest x-ray, maximal, symptom-limited exercise stress EKG, and methacholine challenge test (determination of reversible airway disease or asthma) may be required to determine whether an individual is capable of safe and efficient job performance. All medications taken for respiratory conditions are carefully reviewed to insure that they do not compromise job performance and therefore interfere with safe and efficient job performance.

#### 11. Gastrointestinal System Standard.

a. Any disease or condition which interferes with gastrointestinal function and safe and efficient job performance may be considered disqualifying. Instances will be reviewed on a case-by-case basis.

b. Examples of impairments include:

- acute or chronic hepatitis,
- cirrhosis of the liver,
- colostomies and
- dysphagia.

c. All medications taken for gastrointestinal conditions are carefully reviewed to insure that they do not compromise job performance and therefore interfere with safe and efficient job performance. Any condition that is recurrent with significant diarrhea and/or pain, that limits activity, requires pain medication, or that causes anemia, weakness, or significant weight loss may be disqualifying.

#### 12. Genitourinary System Standard.

a. Any disease or condition which interferes with genitourinary function (genital/urinary organs) and safe and efficient job performance may be considered disqualifying. Cases will be reviewed on a case-by-case basis. Examples of impairment include polycystic kidney disease, acute or chronic renal failure, nephrotic syndrome, and neurogenic bladder.

b. All medications taken for genitourinary conditions are carefully reviewed to insure that they do not compromise job performance.

#### 13. Endocrine and Metabolic Systems Standard.

a. Any excess or deficiency in hormonal production can produce metabolic disturbances affecting weight, stress adaptation, energy production and a variety of symptoms or pathology such as elevated blood pressure, weakness, fatigue, and collapse. Examples of impairment include adrenal dysfunction, thyroid disease, pituitary dysfunction, diabetes mellitus, and parathyroid disorders.

b. Any condition affecting normal hormonal or metabolic functioning and response that is likely to adversely affect safe and efficient job performance is generally disqualifying. Instances will be reviewed on a case-by-case basis.

#### 14. Musculoskeletal System Standard.

a. Any condition that adversely impacts an individual's movement, agility, flexibility, strength, dexterity, coordination or the ability to accelerate, decelerate, and change directions and that is likely to adversely affect the safe and efficient performance of essential job functions is generally disqualifying. An orthopedic evaluation, functional capacity evaluation (FCE), imaging, and/or electrophysiologic (EMG) study may be necessary to determine the extent of physical limitations. Instances will be reviewed on a case-by-case basis.

b. Examples of impairment include:

- arthritis,
- amputation of an extremity,
- scoliosis,
- spinal disorders,
- chronic low back pain, and
- knee conditions.

#### 15. Hematology System Standard.

a. Any hematological (blood) condition that adversely affects an individual's exercise capacity or ability to perform aggressive law enforcement functions that is likely to adversely affect the safe and efficient performance of essential job functions is generally disqualifying. A medical evaluation with a maximal, symptom-limited stress EKG may be necessary to determine the extent of physical limitations. Instances will be reviewed on a case-by-case basis.

b. Examples of impairment include:

- anemia,
- bleeding disorders,
- thrombocytopenia,
- hemoglobinopathies,
- multiple myeloma, and
- systemic lupus.

#### 16. Neurological Systems Standard.

a. Any disease or condition that interferes with the central or peripheral nervous system function and that is likely to adversely affect the safe and efficient performance of essential job functions may be considered disqualifying. A medical evaluation by a neurologist and/or neuro-psychologist may be required. Any condition with loss of motor skills, muscle strength, cognitive function, coordination, or gait; sensory loss (limb, hearing, or vision); tremor; pain; or effect on speech may result in disqualification. Instances will be reviewed on a case-by-case basis.

b. Examples of impairment include:

- stroke,
- head trauma,
- migraine,
- epilepsy,
- syncope, and
- cerebral palsy.

#### 17. Psychiatric Disorders Standard.

a. Any disorder that affects judgment, cognitive function, or the safe and efficient performance of essential job functions, is generally disqualifying. A review by a psychologist, neuro-psychologist, neurologist, and/or a psychiatrist may be required. Instances will be reviewed on a case-by-case basis. Examples of impairment include delirium, dementia, major depression, manic-depressive disorder, panic disorder, and schizophrenia.

b. Dermatology Standard. Any disease or condition that may cause the person to be unduly susceptible to injury or disease as a consequence of environmental exposures, including the sun, or which results in

restricted functioning or movement and thereby impairs the safe and efficient performance of essential job functions, may be considered disqualifying. Instances will be reviewed on a case-by-case basis. Examples of impairment include albinism, severe chronic dermatitis, cosmetic disfigurements, scleroderma and severe skin infection.

#### 18. Cancer Standard.

a. Any cancer-related medical condition that impairs the ability to safely and efficiently perform essential job functions will generally be disqualifying. Instances will be reviewed on a case-by-case basis.

b. Further consideration will be given under the following circumstances:

- The cancer has a high cure rate.
- The cancer has stabilized without metastases.
- The oncologist declares the individual to be a complete responder with no evidence of active disease.
- There is no evidence of medication, surgical or radiation side effects present.
- There is no evidence of immune suppression as a result of the treatment.
- The cancer is in remission with low likelihood of recurrence.
- Examples of impairment include pancreatic cancer, renal carcinoma, hepatic carcinoma, adrenal carcinoma, and leukemia/lymphoma.

#### 19. Medication Standard.

a. All prescribed medication, including psychotropic medication, will be evaluated to ensure that safe and efficient job performance will not be adversely affected by use. Instances will be reviewed on a case-by-case basis.

b. The following factors may be considered in making a medical determination:

- Medication type and dosage requirements;
- Potential drug side effects and adverse reactions;
- Potential drug-drug interactions;
- Drug toxicity;
- Medical complications associated with long-term use;
- Drug-environmental interactions;
- Drug-food interactions; and
- History of patient compliance.

## 911.05 Determination of Fitness for Duty

### 911.05A Examining Physician

After examination of the applicant/SA, the examining physician will relate the physical examination and medical history findings to the MRO.

### 911.05B Medical Review Officer

As outlined below, the MRO opines on the medical qualification of the applicant/SA. In making this determination, the MRO should consider all the available information.

This includes:

- a. Whether there is a combination of medical or physical conditions that collectively hinder the individual's functional capacity to perform activities essential to the job, even if no one condition is disqualifying.
- b. Any treatment by a personal physician, including the diagnosis, treatment, and rehabilitation provided by the treating physician. If inconsistencies exist between the MRO and the examining physician's diagnosis, the MRO should make a concerted effort to account for such inconsistencies and to discuss their implications for the person's employability.

A history of a medical condition may be considered disqualifying only if the condition itself is normally disqualifying, a recurrence cannot medically be ruled out, and the duties of the position are such that a recurrence would pose a reasonable probability of substantial harm to the employee or others. For example, while an early history of epilepsy by itself would not ordinarily be disqualifying for any position, a particular history of epilepsy may, depending upon the specific nature of the condition, be disqualifying for certain hazardous positions such as an SA where any loss of consciousness could have serious consequences. Each case must be decided on its own merits. Generally, as long as the candidate is presently able to do the job, he/she is qualified unless the possibility that the condition might recur and would present a substantial health and safety risk.

All correspondence from the MRO is sent to the AIGI.

### 911.05C Report of Medical Review Officer

After the medical examination and receipt and review of laboratory test results, the MRO will complete the Physical Examination Form (Figure 911-01) and forward it, along with appropriate medical examination results, to the AIGI. The Medical Review Form (Figure 911-02) indicates whether the SA, in the opinion of the MRO, is medically fit, medically unfit, or temporarily medically unfit for duty with the OIG. The MRO coordinates the results of all medical examinations with the AIGI. The AIGI notifies the applicants/SAs of the medical findings. The OIG Director of Human Resources retains all MRO reports.

#### 911.05D Medical Review Officer's Statement

The MRO's findings should be recorded on the Medical Review Form (Figure 911-02).

1. For applicants, this form records:

- a. Acceptable; applicant has no medical conditions that will hinder safe performance of essential job functions.
- b. Medical determination cannot be made due to incomplete examination results.
- c. Applicant is not qualified based on available medical information.
- d. Not medically qualified to perform the essential functions of the job.
- e. Acceptable; incumbent has no medical conditions that will hinder safe performance of essential job functions.
- f. Medical determination cannot be made due to incomplete examination results.
- g. Medical determination cannot be made based on available medical information.
- h. Not medically qualified to perform the essential functions of the job.

#### 911.05E Treatment of Applicants

Applicants who are determined medically unfit for duty will be notified of the determination and the specific reasons. If they elect to do so, applicants will have 30 days to present additional information to the MRO for consideration. In no case will an applicant be hired without a finding of medical fitness for duty by the MRO.

#### 911.05F Treatment of Special Agents

SAs who are determined medically fit for duty will be notified by the OIG. In all cases where the SA is found to be medically unfit for duty, or certain job duties should be limited or restricted, OIG managers will take the actions described below.

1. OIG managers will initiate appropriate action deemed necessary to protect life and property, including (b) (7)(E) or access to and rescission of law enforcement authority, if necessary (see Section 902.07).
2. Prepare a memorandum notifying the SA of the MRO's findings/recommendations. If appropriate, the SA will submit as soon as practicable to any additional evaluation/examination deemed necessary by the MRO. In cases where the MRO asserts that the SA is presently medically unfit for duty, he/she will, as appropriate, be temporarily assigned other duties or placed on approved leave pending completion of the required examination/evaluations, which will be reviewed by the MRO. Any duty limitations imposed by the MRO may not be rescinded without written concurrence of the MRO.

3. Consult with the OIG Office of Human Resources and Counsel to the IG to determine appropriate administrative action if the SA refuses to submit to a required medical examination or other evaluation/examination recommended by the MRO, or if the MRO cannot subsequently certify the SA for unrestricted return to duty within a reasonable period of time. Proper attention should be given to consider alternative accommodations in deciding appropriate action in the latter situation, including removal from the SA position.
4. Individuals seeking such accommodations must submit to the medical examination required by the OIG. They may produce additional medical documentation to support their accommodation request.

#### 911.05G Employability Determination

Employment related decisions involving health status are fundamentally management decisions. The AIGI in making an employability determination will consider both medical information and other relevant evidence directly related to the medical information. The AIGI also will ensure the following.

1. The OIG will obtain OPM approval of any agency decision to medically disqualify a certified preference eligible candidate.
2. If the individual submits medical documentation from his/her personal physician, such documentation was reviewed by the MRO.
3. Any decision complies with OPM guidelines for specific medical conditions.

#### 911.05H Reconsideration

The OIG will allow an individual who has a correctable impairment that precludes him/her from retention as an SA to take corrective actions. If the individual can present medical documentation within a reasonable period of time that the impairment has been corrected, the OIG may direct that the individual be re-examined and the MRO will reconsider the medical determination. The OIG will in consultation with the MRO determine what a reasonable time period is.

Applicants who are determined to be qualified upon reconsideration may apply for the next like vacancy. The OIG need not hold a vacancy open during the reconsideration period of a disqualified applicant.

In the event an employee or candidate for employment requests the opportunity to submit medical documentation from his/her personal physician for consideration by the MRO, or wishes the MRO to consider the results of a prior employment-related physical, the employee must complete an authorization for the Release of Health Information Pursuant to HIPAA Form (Figure 911-03). Complete HIPAA Forms will be maintained by OIG Human Resources.

## 911.05I Waivers and Reasonable Accommodation

Failure to meet the established medical standards or physical requirements means that the individual is not medically qualified for the rigorous position of a criminal investigator and normally the individual is disqualified. However, the (b) (7)(E) may waive any medical standards or physical requirement, for a person who is able to demonstrate the capacity to perform safely and efficiently the duties of the rigorous position. All requests for waivers of SA medical standards and/or physical requirements will be forwarded to the (b) (7)(E) who may confer with the MRO. The (b) (7)(E) makes the decision of whether an individual who does not meet the medical standards can nonetheless perform the job safely and efficiently.

If the OIG determines that it cannot waive the medical standards or physical requirements because an SA is unable to demonstrate that he/she can perform the rigorous duties of the position safely and efficiently, the OIG will make reasonable efforts to accommodate the SA by assisting in locating a (b) (7)(E) position for which the person is qualified.

The OIG's decision to separate an employee for reasons of medical disqualification does not control, preempt, or otherwise supersede an OPM determination of entitlement or non-entitlement to disability retirement under 5 USC 8337 or 8451.

## 911.06 Physical Fitness Program

Participation in the physical fitness program is voluntary. The program allows SAs to participate in approved physical fitness activities three hours per week while on-duty. In order to participate in the program, SAs are required to submit a memorandum to their supervisor acknowledging their review of Chapter 911.06 of the GSA OIG policy and describing their proposed activities, location of activities and weekly schedule. See Figure 911-04 for an example of a request to participate in PT authorization memo.

### 911.06A Medical Screening

Since, SA applicants and incumbent SAs undergo comprehensive medical examinations to determine fitness for duty, additional examinations are not required for participation in the physical fitness program.

### 911.06B Physical Fitness Activities

SAs may partake in a total of three hours of exercise, each week, during regularly scheduled workdays, SAs may combine their exercise period with a lunch break for time keeping purposes, the exercise period should generally be in either ½ hour or 1 hour increments or a combination, i.e. ½ hour, 1 hour, 1.5 hours, etc., not to exceed three hours a week.

SAs may participate in the following authorized physical fitness activities: aerobics, bicycling, gymnastics, jogging/running, fitness walking, weight/resistance training, swimming, and rowing. Team or competition sports are not approved physical fitness activities.

#### 911.06C Program Management

The SAC is responsible for implementing the program in their field and resident offices. Participants are personally responsible for any costs associated with the use of a physical fitness facility.

#### 911.06D Injuries

SAs must immediately report to their supervisor any injuries sustained during approved program participation. The supervisor is responsible for immediately reporting these injuries to the (b) (7)(E) in writing.

An employee injured during participation in the program may be eligible for benefits under the Federal Employees' Compensation Act. The OIG Human Resources Office is available to assist in preparing or processing claims and reports for the Department of Labor, Office of Workman's Compensation.

The SAC may place a SA on limited duty status based on the nature and extent of the injury. The SAC may restore a SA to normal duty status when law enforcement duties can be performed without restriction.

Effective Date 4/7/2015

## 912.00 STANDARDS AND PROCEDURES FOR INVESTIGATIVE INTERVIEWS

### 912.01 General Standards and Procedures for Investigative Interviews

#### 912.01A Purposes of Investigative Interviews

The primary purpose for conducting an interview is to discover the facts pertaining to the matter under investigation. The secondary purpose is to evaluate the credibility of the witness and the information furnished. During an interview, the Special Agent (SA) must be mindful of factors that would have a bearing on the potential use of the evidence and the witness in a trial.

#### 912.01B Scope and Conduct of Investigative Interviews

##### 1. Scope of Investigative Interviews. (b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

##### 2. Standards for Conducting Investigative Interviews. Standards for conducting investigative interviews are as follows:

- The person being interviewed generally is entitled to be advised of the general nature of the investigation and whether he/she is a subject of the investigation. (b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(b) (7)(E)

#### 912.01C Arranging Investigative Interviews of GSA Employees

When a General Services Administration (GSA) employee is to be interviewed at an Office of Inspector General (OIG) office, the SA asks the employee's supervisor to direct the employee to report for the interview. If the nature of the investigation makes notification to the immediate supervisor undesirable, the SA notifies a higher level supervisor. The timing and location of the interview is arranged to avoid unnecessary inconvenience to the employee or his/her office.

GSA employees are required by GSA Order OAD P 5410.1 (April 11, 2000) to cooperate with OIG SAs conducting official investigations. (b) (7)(E)

#### 912.01D Scheduling Interviews of Subjects of Investigation

Generally, the facts and circumstances of the particular investigation dictate when the subject of the investigation is interviewed. (b) (7)(E)

#### 912.01E Union Representation at Investigative Interviews

The Federal Service Labor Management Relations Statute, 5 U.S.C. § 7114, gives bargaining unit employees in the federal government that are examined by agency representatives the right to have a union representative present during the examination.

Courts have held OIG SAs are representatives of the agency when they conduct interviews. Therefore, OIG SAs must accommodate an employee's request for union representation in interviews associated with all investigations. Please refer to Figure 912-01 for additional policy and procedures relating to this right, (b) (7)(E)

No attempt should be made to dissuade an employee from requesting union representation at an interview. If the employee requests such representation, the SA -- in conjunction with his/her supervisor -- must decide whether to:

(b) (7)(E)

(b) (7)(E)

In making this decision, the SA and his/her supervisor should consider the purpose to be served by the interview and whether union representation (b) (7)(E). If a decision is made to conduct the interview with a requested representative, the employee is given a reasonable opportunity to arrange for such representation.

A SA has no affirmative duty to advise the employee of his/her right to request a union representative. For additional coverage on the prerequisites to entitlement to a union representative, as well as guidance on an employee's right to designate a particular person as a representative, see Figure 912-01.

### 912.01F Legal and Other Non-Union Representation at Investigative Interviews

1. OIG Policy on Legal and Other Non-Union Representation at Investigative Interviews. Except in the case of custodial interviews, persons being interviewed by OIG SAs do not have a statutory right to legal representation at the interviews. (b) (7)(E)

2. Procedures When Legal Representation is Requested at Non-Custodial Investigative Interviews. (b) (7)(E)

3. Role of Legal Representation at Investigative Interviews. The function of a legal representative is to furnish counsel and advice to the person being interviewed. Accordingly:

(b) (7)(E)

(b) (7)(E)

If a legal representative insists on dominating the interview, or is otherwise disruptive, the SA must decide whether to continue the interview or terminate and reschedule it at a later date.

#### 912.01G Privacy Act Notice Requirements Relating to Investigative Interviews

As detailed in Section 712.05, SAs must provide Privacy Act notices to all persons interviewed during the course (b) (7)(E) The fact that the Privacy Act Notice was provided is noted in the SA's documentation of the interview. See Figure 912-02.

#### 912.01H Confidentiality During Investigative Interviews

Pledges of confidentiality are promises made by SAs to persons being interviewed that their identities will remain confidential and will not be disclosed outside the OIG. The purpose of pledges of confidentiality is to induce otherwise reluctant individuals to cooperate in investigations and provide useful information.

GSA employees who come forward with information to the OIG do not require special pledges of confidentiality. Their right to confidentiality is established by Section 7(b) of the IG Act which prohibits the OIG from disclosing the identity of such an employee without the employee's consent, unless the OIG determines that disclosure is unavoidable during the course of the investigation or certain other conditions are met (as set forth below). (b) (7)(E)

All requests for confidentiality will be properly documented.

When other GSA employees and persons not employed by GSA request confidentiality, the following procedures apply:

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

## 912.01I Waivers of Disciplinary Action During Investigative Interviews

(b) (7)(E)

1. The terms of the agreement (b) (7)(E) contains the following disclaimer:

(b) (7)(E)

## 912.01J Administering Oaths and Affirmations During Investigative Interviews

1. Authority to Administer Oaths. The IG Act gives this authority to the Inspector General (IG), and the IG has re-delegated it to the Assistant Inspector General for Investigations (AIGI), the Deputy Assistant Inspector General for Investigations (DAIGI), and the Special Agents in Charge (SACs) (GSA Order OIG 5450.2E). Designees authorize, in writing, offices and employees in the OIG having investigatory functions to administer oaths.

2. Distinction Between Oaths and Affirmations. Affirmations are used when religious convictions prevent persons from administering or taking oaths. As detailed below, affirmations are synonymous with oaths for all legal purposes.

- If religious convictions prohibit the SA from administering an oath, the SA may request an affirmation to tell the truth. Persons affirming to tell the truth are subject to prosecution for a false statement to the same extent as if their testimony was provided under oath.

- Persons whose religious convictions prohibit their taking an oath also have a constitutional right to instead affirm to tell the truth. Again, persons affirming to tell the truth are subject to prosecution for a false statement to the same extent as if their testimony was provided under oath.

3. Administering Oaths and Affirmations. SAs also administer oaths and affirmations in relation to documents containing statements of the person being interviewed. The SA administers the oath by having (b) (7)(E)

Every document made under oath contains a certificate, known as a Jurat, evidencing that it was properly executed before a duly authorized officer. The proper format for this certificate is: (b) (7)(E)

#### 912.01K Documenting Investigative Interviews: Use of Recording Devices

The OIG follows the May 12, 2014, memorandum from the Deputy Attorney General with the subject line, Policy Concerning Electronic Recording of Statements (attached).

Actions to be taken by OIG Special Agents (SAs) in accordance with that memo include the following:

- The OIG will electronically record custodial interviews after arrest held in an OIG controlled place of detention with suitable recording equipment, unless an exception applies as stated in that memo.
- SAs should make every effort to electronically record custodial interviews after arrest in other places of detention as well.
- While the interview recording may be audio only, video recording equipment should be used when suitable and available.

This policy applies to state as well as federal prosecutions where the defendant is in OIG custody.

(b) (7)(E) SAs who believe electronic recording may be appropriate in a given investigation should discuss the matter with their (b) (7)(E) and secure the approval of the (b) (7)(E) before proceeding. Consensual monitoring is governed by subchapter 913.

#### 1. Control, Inventory and Maintenance of Interview Recording Equipment

The (b) (7)(E) of each regional office (b) (7)(E) is responsible for the custody, security, and maintenance of all interview recording equipment used by that office. For the purpose of controlling and maintaining the OIG's interview recording equipment, the Primary Equipment Custodians and Alternates, as defined in section 913.01G, will be responsible for the following steps.

- Ensure regional interview recording equipment which is not being used shall be accessible to SAs, yet secured to prevent its loss and/or damage; the interview recording equipment shall be stored in an area where security is commensurate with the equipment's value and sensitivity. (b) (7)(E)

•(b) (7)(E)

- Inventory the interview recording equipment in conjunction with the (b) (7)(E) accountable equipment inventory.

- Maintain and repair the interview recording equipment, (b) (7)(E)

2. (b) (7)(E) Securing, and Transcribing Interview Recordings

Upon completion of the interview, the SA makes the original by downloading the interview (b) (7)(E). The SA then adheres to the following procedures:

- The SA (b) (7)(E) thereafter, and the (b) (7)(E)
- The SA ensures the original interview recording is immediately secured as evidence and treated in accordance with Chapter 925.

(b) (7)(E)

If the original interview recording cannot be (b) (7)(E) the SA adheres to the following procedures:

- (b) (7)(E)
- (b) (7)(E)
- The SA retrieves the interview recording device and creates the original interview recording.

(b) (7)(E) the SA proceeds as above with the original interview recording.

When delivering the original interview recording to a prosecutor or other law enforcement authority, the SA uses an (b) (7)(E) (Figure 925-01), to document the other party's receipt.

The SA makes arrangements for the transcription of recorded interviews if a transcription is necessary. Memoranda of recorded interviews are not intended to be a verbatim account and do not memorialize all statements made during an interview. Where communications by the parties were electronically recorded, the recording captures the actual words spoken. (b) (7)(E) and the original interview recording maintained in the evidence locker when stored. The SA shall ensure that both the memorandum of interview and the transcription accurately reflect the contents of the tape.

912.01L Documenting Investigative Interviews: Notes of Interview

Except where recording devices are used (Section 912.01K), SAs make handwritten notes during all investigative interviews. These notes are used to prepare the formal records of interview (Section 912.01M). They may be subject to inspection by a court, and therefore must be retained in the (b) (7)(E) case file. The interview notes will be scanned and electronically attached to (b) (7)(E). (b) (7)(E)

Notes of interview contain (1) case name or numbers; (2) date and place of interview; (3) complete identification of the person interviewed, including identifiers such as driver's license number; (4) names and titles of other persons present at the interview; and (5) an account of the interview.

When a case is closed, the case file and the interview notes are maintained in (b) (7)(E).

#### 912.01M Documenting Investigative Interviews: Formal Records of Interview

1. **OIG Policy on Documenting Investigative Interviews Through Formal Records of Interview.** Based on their interview notes, SAs prepare formal, permanent records of all investigative interviews. These records are prepared in one of the following forms:

- affidavit;
- statement;
- question and answer statement; or
- memorandum of interview/report insert, when the interview is on a witness or subject in a criminal investigation (Figure 918-05).

2. **Documenting Investigative Interviews Through Affidavits.** An affidavit is a written or printed declaration or statement of facts that is: (1) made voluntarily; and (2) confirmed by the oath or affirmation of the party making it before an officer authorized to administer and receive information under such an oath or affirmation. Figure 912-03 presents a sample affidavit format.

As detailed in Section 912.01J, OIG SAs are authorized to administer oaths/affirmations and to receive information under oath/affirmation. In accordance with the Inspector General Act of 1978, SAs conducting official investigations can request GSA employees to furnish signed statements under oath:

- **Establishing Criteria for Use of Affidavits.** For cases with criminal potential, the SA ascertains, during early consultation, (b) (7)(E) on using affidavits to formally record the investigative interviews. When the (b) (7)(E) objects to the use of affidavits, none is taken. However, if such a case is likely to also result in administrative action, the (b) (7)(E) can explore acceptable alternatives to affidavits with JC and the Regional Counsel. In some instances, the SA may have to obtain affidavits in support of administrative action after disposition of the criminal aspects of the case.

- **Situations Where Affidavits Are Normally Used.** Generally, affidavits are used when statements by principals or third parties need to be formalized. The following investigative interview situations normally meet this standard:

- when the person interviewed has made a verbal admission, particularly if the person is the principal or subject of the investigation;
- when the subject or suspect of a criminal investigation agrees to be interviewed;

◦when subject employees and key witnesses are being interviewed in non- prosecution cases (non- prosecution cases are those where investigation has established that an employee committed a violation of law, but the U.S. Attorney/DOJ decided not to prosecute); or

◦when the person being interviewed has information relevant to the investigation, and there is reason to believe that he/she may change or retract his/her oral statement.

•Guidelines for Preparing Affidavits. Affidavits are normally prepared in accordance with the following guidelines:

◦Affidavits are generally not used to record interviews of complainants or informants.

◦Separate affidavits can be prepared when the affiant is relating criminal or administrative violations on the part of more than one individual.

◦The affidavit is in the words of the affiant, not the SA; and it is limited to comments directly bearing on the topic of the investigation. When securing an affidavit in a case that may be referred for prosecution, it is particularly important to avoid inclusion of prejudicial or extraneous comments.

◦The affidavit sets forth any defense, explanation, or other exculpatory statement furnished by a subject of a case.

◦When the affidavit is executed in longhand, it is preferable to have the affiant write it.

◦When the SA writes the affidavit, the affiant must read the full contents of the affidavit before signing it. If the affiant declines to read the affidavit, the SA reads it to him/her. If the affiant is illiterate, the SA: (1) reads the affidavit to him/her in the presence of a witness; and (2) notes this fact on the last page of the affidavit.

◦Before signing the affidavit, the affiant initials the bottom of each page and each correction.

◦The SA completes the Jurat and, if the affiant has signed the affidavit, upon request provides him/her with a copy of it.

3. Documenting Investigative Interviews Through Statements. A statement is an exact and detailed presentation of the comments made by a person interviewed. A statement is used to document an investigative interview when the person has been placed under oath, but refuses to sign an affidavit. The statement is prepared according to the guidelines for affidavits, and is signed and dated by the SA and other persons present at the interview.

4. Documenting Investigative Interviews Through Question and Answer Statements. A question and answer statement is a verbatim transcript of the questions, answers, and statements made by each participant in an investigative interview. A question and answer statement is used when the SA believes that a relatively formal and structured approach to the interview is necessary.

The question and answer statement consists of a transcript that sequentially numbers the questions asked during the interview, and provides the following information:

•time and place where the testimony was given;

•name and titles of all persons present;

- identification, by name and title, of the persons asking and answering questions;
- name and address of the person giving testimony;
- matter to which the testimony relates;
- advice of rights given to the witness or subject;
- administration of oath or affirmation, if appropriate;
- full text of questions asked and answers provided; and
- Jurat completed by the SA, if appropriate.

5. Documenting Investigative Interviews Through Memoranda of Interview/Report Inserts. The memorandum of interview, which is included as an insert to the report of investigation, is the least formal means of permanently documenting an investigative interview. The memorandum of interview:

- is prepared by a SA who attended the interview;
- shows the date, time, and place of the interview, as well as the names of all persons present at the interview;
- presents a straightforward account of information given at the interview that is relevant to the investigative case;
- when appropriate, details the advice given the witness or subject on his/her constitutional rights; and
- is promptly prepared and attached to the (b) (7)(E) case file by the SA who prepared it.

Figure 918-05 presents a sample format for a memorandum of interview/report insert. It should be noted that memoranda of interview may be subject to 18 U.S.C. 3500 (the Jencks Act), which allows defense inspection of any pretrial statement by a witness who has testified, during direct examination in court, on the same subject. When the person being interviewed may subsequently be a Government witness in a criminal trial, particular care needs to be taken to confine the memorandum of interview to a factual accounting of relevant information, and to avoid including opinions, conclusions, and other extraneous material.

#### 912.01N Processing and Use of Formal Records of Interviews

1. Reviewing and Correcting Formal Records of Interviews. The SA carefully reviews every record of interview for accuracy of content and any typographical errors. If the record of interview is examined by the person being interviewed, he/she may correct typographical errors but never alter the record or delete any testimony. The person being interviewed may submit a separate affidavit or question and answer statement or give additional testimony to modify, explain, or expand on the original record of interview.
2. Providing Copies of Records of Interview to Persons Interviewed. Upon request, the SA provides copies of signed affidavits or question and answer statements to the persons interviewed. While such

copies are normally provided as soon as they are available, the (b) (7)(E) may temporarily withhold them, if necessary, to avoid prejudice to the investigation.

3. Use of Records of Interviews in Trials. Except when they contain confessions or admissions against interest, records of interviews are generally not admissible as evidence in trials. However, records of interviews can be used:

- to refresh the recollection of a witness or discourage a witness from changing his/her testimony;
- to impeach a witness on the stand when his/her testimony in court is materially inconsistent with the previous statements; and
- as the basis for prosecution of a witness who testifies falsely at a trial.

## 912.02 Warnings and Assurances During Criminal Investigation Interviews

### 912.02A Providing Information on Targets and Subjects of Criminal Investigations

DOJ guidelines define targets and subjects of investigation as follows:

- a target of an investigation is a person whom the prosecutor believes to be a putative defendant, i.e., likely to be indicted by the grand jury.
- a subject of an investigation is any person whose conduct is within the scope of the investigation.

If a person being interviewed demands to know if he/she is a target or subject of the investigation and the case has not been referred to a U.S. Attorney/DOJ, the SA:

(b) (7)(E)

If the criminal aspects of the person's conduct have already been referred to a U.S. Attorney/DOJ for prosecution, the SA must inform the person of this. Such a situation could arise when, subsequent to criminal referral and prosecutorial agreement, the OIG is further investigating the civil and/or administrative aspects of a case.

### 912.02B Specific Warnings and Assurances During Custodial Criminal Investigation Interviews

A custodial interview occurs when the person being interviewed has been taken into custody or otherwise legally deprived of freedom of action in any significant way. The SA gives a full Miranda warning in all custodial interviews, even if the arrest or incarceration resulted from a matter totally unrelated to the investigation.

In addition to the standard Miranda language, the Miranda warning for federal employees contains the additional statement that "If you refuse to answer the questions posed to you on the ground that the answers may tend to incriminate you, you cannot be disciplined or discharged solely for remaining

silent.” As is discussed more fully below in section 912.02E, this language serves to negate the possible coercive effect of the prospect of job forfeiture on a Federal employee for failing to cooperate.

Procedures for giving the Miranda warning during custodial interviews are as follows:

- The SA reads the Miranda rights, from the Waiver of Rights form (Figure 912-04 and Figure 912-05), to the person being interviewed. The form used depends on whether or not the person being interviewed is a Federal employee.
- The SA asks the person whether he/she understands the Miranda rights and wishes to waive them.

Depending on the person's response, the SA proceeds as follows:

(b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

#### 912.02C Specific Warnings and Assurances During Non-Custodial Criminal Investigation Interviews

Warnings are not required in non-custodial criminal investigation interviews unless: (1) the warning is directed by a grand jury or a prosecutor to whom the investigation has been referred for prosecutive consideration; and/or (2) the interview involves a federal government employee. Warnings are not, however, given to witnesses. NOTE: There may be other unique situations in which the subject of an investigation (but not a witness) could argue that he or she was subject to coercion. SAs should be sensitive to this possibility and discuss with management the need to give a warning in these circumstances before proceeding with an interview.

If a subject or his/her attorney asks whether cooperation is mandatory, (b) (7)(E) [REDACTED]  
[REDACTED] If the subject or his/her attorney asks whether the investigation is a criminal one, the SA responds that it (b) (7)(E) [REDACTED].

1. Warnings Directed by a Grand Jury or a Prosecutor During Non-Custodial Criminal Investigation Interviews. Section 912.02D provides guidance on warnings directed by a grand jury or prosecutor.

2. Warnings to Federal Government Employees During Non-Custodial Criminal Investigation Interviews. Section 912.02E provides guidance on warnings to be given Federal employees in criminal investigation interviews.

#### 912.02D Specific Warnings and Assurances During Criminal Investigation Interviews of Non-Federal Employees Directed by a Prosecutor or During Grand Jury Investigations

Interviews conducted by SAs assisting prosecutors (either during grand jury investigations or after a case has been accepted for prosecution) must conform with any applicable grand jury rules and Federal Rules of Criminal Procedure, whether or not in accordance with the guidelines in this Subchapter. Clarification on advice or other warnings appropriate to a particular situation should be sought, as necessary, from the government attorney; and the proper form of the warning is as directed by the prosecutor.

(b) (7)(E)



#### 912.02E Warnings and Assurances to Federal Employees During Non-Custodial Interviews in a Criminal Investigation

GSA Order OAD P 5410.1 (April 11, 2000) requires GSA employees to cooperate fully with OIG investigative special agents. (b) (7)(E)



In accordance with Attorney General Guidelines, the OIG has developed two warnings to be given federal employees with potential criminal exposure when interviewed in a criminal investigation. These warnings are designed to ensure that information obtained during such interviews is admissible in subsequent criminal proceedings. The first warning is for federal employees interviewed in custody during a criminal investigation and is discussed above in section 912.02B. The second warning, titled “Non-Custodial Warning and Assurance to Employees: This Statement is Voluntary and May be Used Against You in a Criminal Proceeding,” (the so-called Garrity warning) is found at Figure 912-06. The critical elements to this warning are that a federal employee is being interviewed; criminal prosecution of this person is a possibility; and the interview is voluntary. To ensure voluntariness, the warning states that the employee has a right to remain silent or can stop answering questions at any time and that this right overrides the duty to cooperate.

The form used should be signed and dated by the person being interviewed, the SA, and any witness at the initiation of the interview. A refusal to sign the form should be noted on the form.

### 912.03 Warnings and Assurances During Administrative Misconduct Interviews

The OIG has also developed a warning to be used when interviewing federal employees in administrative misconduct cases in which there do not appear to be potential crime. Warnings are generally given to employees who face a risk of any kind of disciplinary action. The form, which is presented at Figure 912-07, provides warning to employees being interviewed that they are subject to discipline or discharge for not answering questions and that their statement cannot be used against them in a criminal proceeding (the so-called Kalkines warning).

(b) (7)(E)

Such situations include:

- interviews relating to allegations that, if true, would not have potential for criminal prosecution; and
- interviews relating to allegations that, if true, have potential only for non-Federal criminal prosecution, and a decision has nevertheless been made to compel full answers from the employee.

(b) (7)(E)

As with the other warnings, this form must be signed and dated by the person being interviewed, the SA, and any witness at the initiation of the interview.

Effective 10/3/2017

## 913.00 CONSENSUAL MONITORING

### 913.01 Policy

This chapter establishes policies and procedures for consensual monitoring activities conducted by JI involving face-to-face, wire (telephone), and radio communications.

### 913.02 References

This chapter is issued under the authority of the IG and the AIGI to establish and ensure compliance with Attorney General and quality standards for consensual monitoring activities conducted by JI. The guidelines and standards can be found in:

1. Title 18 USC 2511(2)(c)
2. US Attorney's Manual Chapter 9-7.301-302
3. AG Memo dated May 30, 2002 – Procedures for Lawful, Warrantless Monitoring of Verbal Communications (Figure 913-01)
4. AG Memo dated December 8, 2003 – Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority (Figure 913-02)

### 913.03 Scope

The provisions of this chapter apply to all employees of JI.

### 913.04 Consensual Monitoring Guidelines

1. Consensual monitoring is used only (b) (7)(E) .
2. Consensual monitoring will only be initiated after obtaining permission of consenting party or parties, and obtaining proper agency authorization. This includes SAs who record their own investigative conversations with another party, pursuant to an investigation.
3. Consensual monitoring activities including approvals, authorizations and techniques will be documented in the electronic case management system.
4. SAs must be cognizant and able to distinguish between those situations requiring supervisory approval, IG Approval, DOJ verbal advice, and DOJ written approval.

### 913.05 General Consensual Monitoring Considerations

1. Consensual monitoring is the use of electronic devices to intercept, transmit, or record private conversations, when one or more (but not all) parties to a conversation have consented to its interception, transmission, or recording. Consensual monitoring policies and procedures apply to wire, radio, and face-to-face communications.

a. Wire communications include telephone;

b. Radio communications include wireless communications (cellular phone).

c. Face-to-face communications are verbal (oral) non-wire communications. Face to face communication is commonly referred to as non-wire, because it is not being recorded through a wired telephone or wireless cellular phone. However, face-to face communication is captured using either a body worn audio device, or through a device in a fixed location, or in personal effects.

2. Consensual monitoring does not apply to interviews, question and answer sessions, or similar situations where room recording devices are used, e.g. recorded interview with the full knowledge and consent of all participants.

3. In consensual monitoring situations, because the consenting party is cooperating with the government and would relate the substance of the conversation to the government anyway, the government is obtaining no information it would not otherwise obtain; it simply obtains it faster and in a more probative form (see *United States v. White*, 401 U.S. 745 [1971]).

4. Consensual monitoring is markedly different from wiretapping and other forms of interception, which require a judicial warrant.

5. AG Memo dated May 30, 2002 (Figure 913-01) covers the investigative use of devices which intercept and record certain consensual verbal conversations where a body transmitter or recorder or a fixed location transmitter or recorder is used during a face-to-face conversation. AG Memo dated December 8, 2003 (Figure 913-02) reiterates these requirements.

### 913.06 Obtaining Consenting Parties' Permission for Consensual Monitoring

1. Written Consent. (b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

2. Verbal Consent. (b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

3. (b) (7)(E) [Redacted]

### 913.07 Authorization

Requestor shall submit a request for authorization and receive approval before conducting any monitoring activity.

#### 1. Required information

a. (b) (7)(E) [Redacted] A Request for Authorization to Use Electronic Equipment for Consensual Monitoring form (Figure 913-04) should be used for this purpose. (b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E) [Redacted]

2. Wire (telephone) and Radio ONLY situations

(b) (7)(E)

3. Non-sensitive face-to-face situations, which are all other situations not covered in section 913.07D

a. Where face-to-face communications will be monitored, (b) (7)(E)

d. Emergency Procedures for Obtaining Approval of Verbal (b) (7)(E) Consensual Monitoring, Not Requiring Prior Written DOJ Authorization. Every effort is made to submit written requests for, and obtain (b) (7)(E) approval, of verbal (b) (7)(E) consensual monitoring activities. However, in emergency situations where this is not feasible, the (b) (7)(E) make the request to the (b) (7)(E) and/or the (b) (7)(E) may give his/her (b) (7)(E) approval. In such situations:

- The request to the (b) (7)(E) includes all information required on the Request for Authorization to use Electronic Equipment for Consensual Monitoring form.
- The request to the (b) (7)(E) includes explicit assurance that the proposed consensual monitoring has been discussed with the appropriate (b) (7)(E) and contains the advice given, and in concurrent investigations, that the participating agencies were notified and concurred or not.
- The (b) (7)(E) fully documents the (b) (7)(E) request and/or the (b) (7)(E) approval, as well as the emergency circumstances, as soon as possible after the (b) (7)(E) emergency final authorization.

4. Sensitive Face-to-Face Situations

a. In Six Specified Sensitive Situations where face-to-face conversations will be monitored (Figure 913-01, Section II (A)), and written DOJ/Office of Enforcement Operations authorization is necessary (Figure 913-04). (Note: The Consent Request form will be from the IG to DOJ/Office of Enforcement Operations.) The six situations requiring prior DOJ written approval:

- The interception relates to an investigation of a member of Congress, a Federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous 2 years.

- The interception relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any State or Territory, or a judge or justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his/her official duties.
- The consenting or non-consenting person is a member of the diplomatic corps of a foreign country.
- The consenting or non-consenting person is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.
- The consenting or non-consenting person is in the custody of BOP or the United States Marshals Service.
- The Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General for the Criminal Division, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent for making a consensual interception in a specific investigation.

b. Wire and Radio Communication Exception. The Attorney General's Memorandum on Procedures for Lawful, Warrantless Monitoring of Verbal Communications dated May 30, 2002, sets forth the government-wide requirements relating to consensual monitoring of face to face communications and specifies that it does not apply to interception of telephone and radio communications even if the interception falls within one of the above six DOJ sensitive categories (Figure 913-01 Section II (B)(5) and (6)).

c. Standard Procedures for face-to-face DOJ Sensitive Situations

- The completed request (Figure 913-04), addressed to DOJ Office of Enforcement Operations, will be reviewed by (b) (7)(E) and forwarded to (b) (7)(E)
- The request should be sent at least (b) (7)(E), whenever possible, prior to the requested monitoring, to allow JI sufficient time for review. The (b) (7)(E) will review and provide to the (b) (7)(E)
- Transmitted to the (b) (7)(E) for approval, by the (b) (7)(E) if the (b) (7)(E) agrees with the request for consensual monitoring.
- Approved / disapproved by the (b) (7)(E) where the (b) (7)(E) signs and dates the form and returns it to the (b) (7)(E)
- Transmitted to DOJ's Office of Enforcement Operations by the (b) (7)(E), whenever possible, in advance of the proposed monitoring (b) (7)(E). Where the request is of an emergency nature, an asterisk should be placed adjacent to the deadline date.
- Approved / disapproved by DOJ's Office of Enforcement Operations with approval / disapproval documented on the request and the original request will be returned to the OIG.

d. EMERGENCY Criteria and Procedures for DOJ Sensitive Situations:

a. Emergency situations are those where:

- Waiting for the physical receipt of the written DOJ approval may not be feasible.

- There is imminent loss of essential evidence.
- There is a threat to the immediate safety of a SA, informant, or consenting third party.
- There are reasonable grounds to believe that written DOJ approval cannot be received in time to conduct the consensual monitoring.

b. Emergency Procedures for Obtaining Approval of Face-to-face Consensual Monitoring that Normally Require Prior, written DOJ Authorization for Sensitive Situations:

- The (b) (7)(E) provides the (b) (7)(E) with all the information required on the form, and obtains the (b) (7)(E) approval. Where possible, the information is provided to the (b) (7)(E) approval is obtained. When this is not possible, the (b) (7)(E) documents the verbal request and/or approval as soon as possible and provides this documentation to the (b) (7)(E) explanation of the emergency circumstances.
- Where possible, the (b) (7)(E) the Director or Associate Director of DOJ's Office of Enforcement Operations and requests verbal authorization for the consensual monitoring.
- When the decision for consensual monitoring must be made during non-working hours at DOJ: (1) the consensual monitoring is undertaken based on the (b) (7)(E) approval and (2) the OIG provides full notification and explanation to the DOJ's Office of Enforcement Operations within (b) (7)(E) working days after the (b) (7)(E) emergency authorization.

#### 913.08 Duplicating, Securing, and Transcribing Recordings

Evidence recordings are handled in accordance with Chapter 925. For procedures on handling digital evidence, see Section 925.03F (Handling Digital Evidence).

The SA makes arrangements for the transcription of recordings only if a transcription is necessary.

Where communications by the parties were electronically recorded, the recording captures the actual words spoken. It is not necessary for agents to write a verbatim account/all statements of the dialog exchanged during a consensual call, but all relevant excerpts of the consensual conversation should be captured, generally on a Memorandum of Activity form for easy reference. The SA shall ensure that both the Memorandum of Activity and the transcription accurately reflect the contents of the recording.

#### 913.09 Control, Inventory and Maintenance of Consensual Monitoring Equipment

Consensual monitoring equipment consists of those resources whose principal function is to record verbal conversations with at least one of the parties' consent.

1. Responsibilities of (b) (7)(E) . (b) (7)(E) is responsible for managing the custody, security, and maintenance of all consensual monitoring equipment used by their office. For the purpose of controlling and maintaining the OIG's consensual monitoring equipment, (b) (7)(E) in each investigative office designates: SAs to act as primary equipment custodian;

alternate equipment custodian for branch and the regional office; and, when applicable, a SA to act as equipment custodian in subordinate offices. These designations are made (b) (7)(E)

2. Each equipment custodian and his/her alternate is responsible for the custody, issuance, security, inventory, and maintenance of all consensual monitoring equipment within the jurisdiction of the office.

3. Controlling Consensual Monitoring Equipment. OIG uses special procedures to prevent loss and/or damage to consensual monitoring equipment. These special procedures govern the storage, inventorying, and tracking of all consensual monitoring equipment. All consensual monitoring equipment must be tracked in the (b) (7)(E) Technical Inventory. When this equipment is used for investigations, it must be assigned to an agent and properly noted in (b) (7)(E). Upon receipt, agents must accept the equipment and when no longer needed the agent must return the equipment. When this equipment is loaned/transferred to another office, it must be properly tracked and accounted for in (b) (7)(E).

4. Storage of Consensual Monitoring Equipment.

a. JI's consensual monitoring equipment is permanently assigned to the (b) (7)(E) or regional offices. The (b) (7)(E) or regional office, (b) (7)(E)

b. (b) (7)(E) office, should be (b) (7)(E) when not in use. If this type of (b) (7)(E) is not available, the equipment is (b) (7)(E). Access to the stored equipment is limited to the (b) (7)(E).

5. Inventory Records and Reports on Consensual Monitoring Equipment.

a. The (b) (7)(E) ensures consensual monitoring equipment is properly documented in (b) (7)(E)

b. The (b) (7)(E) conducts an accountable equipment inventory to include all consensual monitoring devices (b) (7)(E) This inventory contains: (b) (7)(E)

6. Maintaining and Repairing Consensual Monitoring Equipment.

a. To facilitate the government showing fidelity of all recording equipment in trial, the (b) (7)(E) are responsible for all maintenance and repairs of the consensual monitoring equipment, which must be documented in the item's record in (b) (7)(E)

## 7. Loan of Consensual Monitoring Equipment.

a. Consensual monitoring equipment may be loaned to other law enforcement agencies under the authority created by the Economy Act, 31 U.S.C. SS 1535, with the following information documented:

- Agreement for Temporary Interagency Loan of Equipment (Form 913-06) may be utilized.
- Receiving Agency name.
- Loan is temporary and will not create actual costs for GSA OIG and therefore reimbursement is not necessary unless equipment is lost, damaged, or destroyed.
- Description of item(s) loaned.
- Dates of loan.
- Receiving agency will compensate the GSA OIG for any costs the GSA OIG incurs for repair or replacement of equipment lost, damaged, or stolen.
- Name, title, signature and date of GSA OIG representative and receiving agency representative.

Effective Date 2/10/2014

#### 914.00 POLICY FOR UNDERCOVER OPERATIONS

Undercover operations may be used to gather information and evidence of criminal, civil and administrative violations within the investigative jurisdiction of the GSA OIG. However, (b) (7)(E)

[REDACTED]

Therefore, undercover techniques will be carefully considered and monitored. (b) (7)(E)

[REDACTED]

#### 914.01 Definitions

(b) (7)(E)

[REDACTED]

#### 914.02 External Guidelines Affecting GSA OIG Undercover Operations

All undercover activities led by the GSA OIG shall be conducted in accordance with the Attorney General's Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority (Figure 901-02).

Additionally, GSA OIG undercover operations shall be subject to the Attorney General's Guidelines for Federal Bureau of Investigation (FBI) Undercover Operations ("Undercover Guidelines" (<http://www.justice.gov/ag/readingroom/undercover.htm>) and the Council of Inspector Generals for Integrity and Efficiency (CIGIE) "Guidelines for Undercover Activity," published in June 2013 (Figure 914-01).

All special agents contemplating using or involved in undercover activity shall familiarize themselves with these guidelines.

914.03 Types of Undercover Operations

A. Group I – “Undercover Operations Involving (b) (7)(E) ” - where there is a reasonable expectation that the undercover operation will involve one or more of the following (b) (7)(E)

(b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

B. Group II – “Undercover Operations Involving Certain (b) (7)(E) [Redacted]” – where there is a reasonable expectation that the undercover operation will involve any of the following (b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

C. Group III - (b) (7)(E) [Redacted] - any investigative activity not defined above which involves (b) (7)(E) [Redacted] by a special agent of the GSA OIG or another federal, state, or local law enforcement organization working with an OIG, and which is not expected to exceed (b) (7)(E) [Redacted]

#### 914.04 Considerations

Before commencing or seeking the approval to conduct any undercover activity, SAs and supervisors shall consider the following: (b) (7)(E) [Redacted]

[Redacted]

(b) (7)(E)

If any of the aforementioned conditions pose a significant risk, the use of other investigative techniques should be considered.

#### 914.05 Application and Authorization to Conduct Undercover Activities

(b) (7)(E)

[Redacted text block containing multiple paragraphs of information under section 914.05]

(b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

914.06 Approval for Undercover Operations Under Exigent Circumstances

(b) (7)(E)

[Redacted]

914.07 Duration of Authorization

(b) (7)(E)

[Redacted text block]

914.08 Requirement to Notify the Federal Bureau of Investigation

(b) (7)(E)

[Redacted text block]

914.09 Record Keeping and Reporting Requirements

(b) (7)(E)

[Redacted text block]

914.10 Oversight and Review of Group I and Group II Undercover Operations

(b) (7)(E)

[Redacted text block]

(b) (7)(E) [Redacted]

#### 914.11 Termination and Closure of Undercover Operations

When the objectives of any undercover operation have been accomplished or (b) (7)(E) [Redacted], the (b) (7)(E) [Redacted] should terminate the operation and notify the (b) (7)(E) [Redacted] that the operation will be closed.

Within (b) (7) [Redacted] days of termination of an undercover operation, the (b) (7)(E) [Redacted] which shall include the following information:

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E) [Redacted]

914.12 Cover Agents

(b) (7)(E) [Redacted]

914.13 Undercover Agents

The recruitment, selection, and training of special agents to become undercover agents are critical to the success of the GSA OIG undercover program. (b) (7)(E)

[Redacted]

(b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

914.14 Duties and Responsibilities of Undercover Agents

(b) (7)(E)

[Redacted]

(b) (7)(E)

[Redacted]

[Redacted]

914.15 Participation in Unethical or Illegal Activity by Undercover Agents

(b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E)

914.16 Participation in Undercover Activities Led by Other Law Enforcement Agencies

(b) (7)(E)

914.17 Coordination of Undercover Operations with Prosecutor

(b) (7)(E)

Effective Date 2/11/2014

## 915.00 POLICY FOR SOURCES OF INFORMATION AND USE OF CONFIDENTIAL FUNDS IN SUPPORT OF INVESTIGATIONS

### 915.01 Use of Sources of Information

In accordance with the Attorney General's Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority dated December 8, 2003, the Office of Inspector General (OIG) shall follow the Attorney General's Guidelines Regarding the Use of Confidential Informants dated May 30, 2003 (Figure 915-01) (hereinafter referred to as "the Attorney General's Guidelines").

Nothing contained in this chapter or any other chapter of this manual is intended to create or does create an enforceable legal right or private right of action by a cooperating person or any other person.

### 915.02 Types of Sources of Information

In the conduct of investigations of criminal, civil, administrative or employee misconduct violations, SAs shall use the following definitions established by the Attorney General's Guidelines:

1. Confidential Informant or "CI" - Any individual who provides useful and credible information to the OIG regarding criminal activities and from whom the OIG expects or intends to obtain additional useful and credible information regarding such activities in the future.
2. Cooperating Defendant/Witness - Any individual who: a) meets the definition of a CI; b) has agreed to testify in a proceeding as a result of having provided information to the OIG; and c) is a defendant or potential witness who has a written agreement with a federal prosecuting office, pursuant to which the individual has an expectation of future judicial or prosecutive consideration or assistance as a result of having provided information to the OIG, or is a potential witness who has had a federal prosecuting office concur in all material aspects of his or her use by the OIG.
3. Source of Information - Any individual who:
  - a) meets the definition of a CI;
  - b) provides information to the OIG solely as a result of legitimate routine access to information or records, such as an employee of the military, a law enforcement agency, or a legitimate business (e.g., phone company, banks, airlines), and not as a result of criminal association with persons of investigative interest to the OIG; and
  - c) provides such information in a manner consistent with applicable law.

In addition, the Inspector General Act in effect creates another category, confidential sources of information, stating that the Inspector General "shall not, after receipt of a complaint or information

from an employee, disclose the identity of the employee without the consent of the employee, unless the Inspector General determines such disclosure is unavoidable during the course of the investigation.”

Unless otherwise specified, the provisions in this chapter apply to only CIs. The term “cooperating person” as used in this chapter shall apply to other sources of information as discussed above.

### 915.03 Determination of Suitability and Documentation of CIs

Before documenting a CI, (b) (7)(E) [redacted]

In accordance with the Attorney General’s Guidelines, CIs shall be documented on a Source Suitability Report and Recommendation (Figure 915-02). (b) (7)(E) [redacted]

[redacted]

(Figure 915-02) (b) (7)(E) [redacted]

[redacted] (see Figure 915-03).

### 915.03A Conditions Requiring Review of the Confidential Informant Review Committee

(b) (7)(E) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

(b) (7)(E) [Redacted]

915.03B Conditions Requiring Permission from Federal Prosecutor Before Use

(b) (7)(E) [Redacted]

915.04 Registration of CIs

(b) (7)(E) [Redacted]

915.05 Prohibition on Commitments of Immunity

(b) (7)(E) [Redacted]

915.06 Protecting the Identities of CIs and Cooperating Persons

(b) (7)(E) [Redacted]

(b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

915.07 Interaction with CIs and Cooperating Persons

(b) (7)(E)

[Redacted]

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

915.08 Illegal Activity by CIs

(b) (7)(E) [Redacted]

915.09 Headquarters and Field Responsibilities

In keeping with the Attorney General's Guidelines, the (b) (7)(E) [Redacted] is designated to oversee the management of all aspects of the confidential informant program. (b) (7)(E) [Redacted] shall (b) (7)(E) [Redacted] review this chapter with the (b) (7)(E) [Redacted] and ensure they receive sufficient initial and in-service training, and shall consider their compliance with this chapter (b) (7)(E) [Redacted]

915.10 OIG Confidential Fund

(b) (7)(E) [Redacted]

[Redacted]

(b) (7)(E) [Redacted]

915.11 Use of Confidential Funds

The OIG confidential fund is to be used solely to facilitate the collection of evidence and information concerning civil and criminal violations related to the programs and operations of the General Services Administration.

(b) (7)(E) [Redacted]

[Redacted]

The following types of expenditures may be financed by the confidential fund:

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



(b) (7)(E) [Redacted]

[Redacted]

915.13 Disbursements of Confidential Funds from (b) (7)(E)

Confidential funds may be disbursed through any reasonably secure method as outlined below.

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

915.14 Security of Confidential Funds

All confidential funds (cash) must be maintained by the recipient (b) (7)(E) [Redacted]

[Redacted]

[Redacted]

915.15 Payment of Confidential Funds

Payment of confidential funds to CIs shall be made in accordance with the Attorney General's Guidelines (Figure 915-01, pp. 18-19).

(b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

#### 915.16 Accounting for Confidential Funds

SAs must be cognizant that confidential funds may be subject to theft by CIs, cooperating persons, the subject of their investigation or others. (b) (7)(E)

[Redacted]

Confidential funds maintained at (b) (7)(E) shall be audited by the (b) (7)(E) no later than (b) (7)(E).

(b) (7)(E) must prepare a (b) (7)(E) report of the use and current balance of confidential funds in their possession. The report shall be submitted to the (b) (7)(E) no later than the (b) (7)(E) (b) (7)(E) Figure 915-05. The failure to account for confidential funds shall serve as the basis to revoke an authorization and require the immediate return of all remaining funds to (b) (7)(E)

The (b) (7)(E) shall maintain and make available to the (b) (7)(E) the accounting of all confidential funds (Headquarters and field).

#### 915.17 Loss of Confidential Funds

In the event confidential funds are lost or stolen, the following shall be performed:

(b) (7)(E)

2) The (b) (7)(E) within (b) (7)(E) will prepare a memorandum to the (b) (7)(E)

[Redacted]

3) If the loss resulted from the apparent negligence of the responsible SA, (b) (7)(E)

[Redacted]

#### 915.18 Return of Confidential Funds to Headquarters

(b) (7)(E)

[Redacted]

[Redacted]

Effective Date 2/12/2014

## 916.00 SUSPENSION/DEBARMENT INVESTIGATIONS AND REFERRALS

### 916.01 Definition and Regulatory Basis of Suspensions/Debarments

Suspension and debarment are measures taken by the government to disqualify entities from participation in government contracting or subcontracting. Suspension temporarily disqualifies the entity; debarment disqualifies the entity for a fixed period. Suspension and debarment are used for the purpose of protecting the interests of the government, not for punishment.

The regulatory basis for General Services Administration (GSA) suspension and debarment actions are:

- the Federal Acquisition Regulations Subpart 9.4 (48 Code of Federal Regulations 1-9.4); and
- Subpart 509.4 of the GSA Acquisition Regulations Manual; Debarment, Suspension, and Ineligibility.

### 916.02 Causes for Suspensions/Debarments

The following paragraphs summarize causes specified in the Federal Acquisition Regulations for entity suspensions and debarments.

1. Causes for Suspensions. The Suspension and Debarment Official (SDO) may suspend an entity:

- when the entity is suspected, upon adequate evidence, of:
  - commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public contract or subcontract;
  - violation of Federal or state antitrust statutes relating to the submission of bids or proposals;
  - commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property; or
  - commission of any other offense indicating a lack of business integrity or business honesty that seriously and directly affects the present responsibility of a government contractor or subcontractor;
- when the entity is indicted for any of the causes listed above;
- for any other cause of so serious or compelling a nature that it affects the present responsibility of a government entity; or
- for any of the above causes based on a suspension by another agency where the original suspension does not have Government-wide effect.

2. Causes for Debarments. The SDO may debar an entity for any of the following causes:

- conviction of, or civil judgment for:

- commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public contract or subcontract;
- violation of Federal or state antitrust statutes relating to the submission of bids or proposals;
- commission of any embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property; or
- commission of any other offense indicating lack of business integrity or business honesty that seriously and directly affects the present responsibility of a Government contractor or subcontractor;
- violation of the terms of a government contract or subcontract so serious as to justify debarment, such as:
  - willful failure to perform in accordance with the terms of one or more contracts; or
  - a history of failure to perform, or unsatisfactory performance of one or more contracts;
  - any other cause of so serious or compelling a nature that it affects the present responsibility of a government contractor or subcontractor; or
  - debarment for any of the above causes by another agency where the original debarment did not have Government-wide effect.

#### 916.03 OIG Policy on Suspension/Debarment Investigations and Referrals

**(b) (7)(E)** [REDACTED] authorizes investigations to gather evidence for referral to the Suspension and Debarment Official (SDO) for their consideration in the suspension or debarment of entities. Office of Inspector General (OIG) policies relative to these investigations and referrals are presented in the following paragraphs.

When an audit of a contract or contractor indicates that suspension or debarment is appropriate as a result of a suspected wrong-doing, the matter is referred for investigation in accordance with standard Suspicion of Irregularity procedures (Subchapter 705).

**(b) (7)(E)** [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

If the OIG has information indicating grounds for suspension/debarment, but the entity's business is with a government agency other than GSA, the information is referred to that agency for consideration of suspension/debarment action. (b) (7)(E)

2. OIG Policy on Recommending Suspension/Debarment Referrals During Ongoing Criminal Investigations. (b) (7)(E)

Recommendations for suspension/debarment are made by the SACs to the GSA SDO.

3. OIG Policy on Making Suspension/Debarment Referrals to the GSA SDO. (b) (7)(E)

In support of this policy, (b) (7)(E) should make a referral as soon as an investigation reveals reasonable grounds for suspension/debarment, including when:

- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)

The (b) (7)(E) is responsible for making all suspension/debarment referrals for his/her region.

4. OIG Policy on Tracking and Reporting Suspension/Debarment Investigations (b) (7)(E)

(b) (7)(E)

#### 916.04 Documentation, Format, and Contents of Referrals for Suspensions

Figure 916-01 describes: (1) the information and documentation required for suspension referrals; and (2) the format and contents of the suspension referral memorandum from the SAC to the SDO.

#### 916.05 Documentation, Format, Contents, and Timing of Referrals for Debarment

Figure 916-02 describes: (1) the information and documentation required for debarment referrals; (2) the format and contents of the debarment referral memorandum from the SAC to the SDO; and (3) the importance of making debarment referrals on a timely basis.

Effective Date 2/12/2014

## 917.00 SEARCH AND SEIZURE

### 917.01 Search and Seizure

#### 917.01A Office of Inspector General Policy on Search and Seizure

Office of Inspector General (OIG) Special Agents (SAs) are authorized to request search warrants through U.S. Attorneys or DOJ, and to execute such warrants. SAs are also authorized to execute warrantless searches within the guidelines set forth. Unless precluded by State law, SAs may request search warrants from state or local judicial officials, (b) (7)(E).

(b) (7)(E)

is notified prior to and immediately after each contemplated or effected search.

#### 917.01B OIG Policy on Obtaining Search Warrants

(b) (7)(E)

#### 917.01C Special Agents Authority to Serve and Execute Search Warrants

SAs' authority to seek, serve and execute search warrants derives from the following:

- The IG Act, 5 U.S.C. App. 3, section 6(e)(1)(c), which authorizes OIG special agents to seek and execute warrants to search a premises or seize evidence upon probable cause.
- Rule 41 of the Federal Rules of Criminal Procedure, which provides, in part, that a search warrant may be issued upon request of a "federal law enforcement officer....who is engaged in enforcing criminal

laws and is within any category of officers authorized by the Attorney General to request issuance of a search warrant”; and

- 18 U.S.C. 3105, which provides, in part, that “A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution.”

#### 917.01D Executing Search Warrants

(b) (7)(E)

(Figure 917-01) (b) (7)(E)

(b) (7)(E)

#### 917.01E Searches Under Search Warrants

The following standards and procedures apply to searches conducted under search warrants.

1. Timing. Search warrants are executed in accordance with the restrictions imposed by the Court and Rule 41, Federal Rules of Criminal Procedure.
2. Announcement. Title 18 U.S.C. §3109, requires the SA to announce his/her identity, authority, and purpose before entry to execute a search warrant. The announcement need not be lengthy or elaborate, but should be conveyed in a manner to make it unmistakable that the person behind the door knows what is taking place.
3. Exception to Announcement Requirements. The announcement requirement of Title 18 U.S.C. §3109 does not apply under the following circumstances:
  - when the SA executing the warrant reasonably believes that by the announcement he/she places himself/herself or other persons within premises in imminent peril of bodily harm;
  - when the SA is virtually certain that persons within the place to be searched already know of the SA's identity, authority, and purpose (the “useless gesture” exception); or
  - when the SA has reason to believe the evidence sought under the warrant is in the process of destruction or removal.

4. Number of Special Agents (b) (7)(E)

5. Entry. (b) (7)(E)

6. Plain View Doctrine. Where SAs are lawfully present on premises, as during the execution of a warrant, and they observe evidence (e.g., fruits or instrumentalities of crime, contraband, illegal substances, etc.) in plain view, such evidence may be seized even though it is not described in the warrant and not relevant to the offense under investigation. The incriminating character of the item must be immediately apparent and the agent must be lawfully located in a place from which he can both plainly see and lawfully access it.

(b) (7)(E)

7. Resistance or Interference. Title 18 U.S.C. §2231 makes it a felony to assault, resist, oppose, prevent, impede, intimidate, or interfere with a SA attempting to execute a search warrant. Hence, a person may not obstruct the execution of a warrant and can be immediately arrested for doing so. A violation may be shown even though the person resisting does not use force or violence.

(b) (7)(E)

Destruction or removal of evidence sought under warrant is a separate criminal violation (Title 18 U.S.C. §2232), as is any forcible attempt to rescue property already seized by the searching agent (Title 18 U.S.C. §2233).

8. (b) (7)(E)

9. (b) (7)(E)

(Figure 925-01 (b) (7)(E)

(b) (7)(E)

If the person from whose possession evidence is seized is not present, a copy of the warrant and the (b) (7)(E) are left in a conspicuous place at the location of the search.

10. Return. The return of a search warrant is the report to the issuing magistrate that the warrant was executed. (b) (7)(E)

(b) (7)(E)

#### 917.01F Searches Incidental to Arrest

Few rules are as firmly embedded in search and seizure law as that which permits a search incidental to arrest with or without arrest warrant. The authority to search following a custodial arrest is an exception to the warrant requirement and allows a full and complete search for weapons or implements of escape and for evidence connected with the crime for which the person has been arrested.

The purpose of the search is to protect the arresting SA and prevent escape. The right to search flows from the fact of arrest. The nature of the crime, whether felony or misdemeanor, violent or nonviolent, has no bearing on the right to search. The imposition of physical custody is the key to any such search.

Any search incidental to arrest is made (b) (7)(E) unless the arrest is made under emergency or exigent circumstances. The following standards and procedures apply to searches incidental to arrest.

1. Scope of Search. Following a lawful arrest, a SA is entitled in all cases to search the person of the arrestee and the area within his/her immediate control at the time of arrest. (b) (7)(E)

2. Protective Sweep. Following a lawful arrest made within premises, SAs may properly conduct a cursory search of the premises if they have a reasonable suspicion that confederates, accomplices, or

others are present and may jeopardize the safety of the arresting agents or the arrestee. Reasonable suspicion must be based upon facts known to the SAs, such as noises in an attic or the at-large status of a dangerous confederate.

The cursory search is not justified solely by the arrest. Rather, it is an independent search authority aimed at protection of the arresting SAs. (b) (7)(E)

(b) (7)(E) If a SA, while conducting a protective sweep, observes evidence in plain view, it may be seized under that doctrine.

3. Receipt and Certificate. A receipt for any property taken in a search incidental to arrest is given to the person from whom the property is taken. (Figure 925-02 or equivalent). (b) (7)(E)

(b) (7)(E)

4. (b) (7)(E)

(b) (7)(E)

#### 917.01G Searches by Consent

A consent is a relinquishment of Fourth Amendment rights by the consenting party, and thus is reasonable even in the absence of probable cause and where searching agents cannot particularly describe the materials being sought.

The essential elements of a search by consent are detailed below.

1. Authority to Consent. SAs seeking permission to search without a warrant must obtain consent from a person authorized to give it. Only a person with actual or apparent authority over the place to be searched may give consent.

This is ordinarily the person who currently possesses the premises or personal property.

Ownership is not the equivalent of actual or apparent authority where the owner has temporarily yielded his/her right to possess, as in the case of landlord and tenant, or innkeeper and guest. Nor is lawful presence the same as actual or apparent authority. A guest or invitee, lawfully on premises, is generally not authorized to give up rights possessed by his/her host.

SAs are to obtain consent from a person with authority. (b) (7)(E)

(b) (7)(E) (Figure 917-02).

(b) (7)(E)

SAs should carefully question any person present who might be of help in deciding who is authorized to consent.

2. Voluntariness. The critical issue in any consent search is whether the consent is voluntary; that is, whether it is the result of a free and unconstrained choice. It is the Government's burden to prove the consent is not coerced. SAs, therefore, avoid any actions or statements likely to elicit submission to their authority rather than a free choice.

No single criterion is used to determine voluntariness, but rather the sum total of surrounding circumstances--such considerations as the number of SAs present, the time of search, the manner of request, the display of weapons, and the physical or mental condition of the consenter. (b) (7)(E)

[REDACTED]

[REDACTED]

However, a consent to enter, obtained by such means in an undercover operation, is proper.

3. Warning of Rights. In establishing voluntary consent, the Government is not required to prove a warning of Fourth Amendment rights was administered before the consent. While knowledge of a right to refuse consent is a factor to be taken into account, the SA need not prove that the one giving permission to search knew that he had a right to withhold his/her consent.

4. Limitation of Consent. (b) (7)(E)

5. Implied Consent. (b) (7)(E)

6. Receipt and Certificate. A receipt is prepared and given to the consenting party for any property seized during a consent search. (Figure 925-02 (b) (7)(E)

#### 917.01H Emergency Searches

The delay to procure a search warrant may sometimes place the safety of people in jeopardy or defeat the purpose of the warrant by permitting disposal of evidence. The law therefore recognizes that, under certain emergency circumstances, the requirement of a search warrant is waived, and a SA may properly make a warrantless entry and search of a place otherwise protected by the Fourth Amendment.

A SA may enter immediately to protect life or safety, to seek out a fugitive while in hot pursuit, and to preserve evidence which is in the process of destruction or removal. Such entries and searches can be made only under extraordinary circumstances. SAs should be prepared to justify their conduct by facts supporting a reasonable belief that such an emergency existed.

## 917.01I Searches for Work-Related Evidence

A government employee's reasonable expectation of privacy can be validly negated by government regulation, consent to search as a condition of employment or entry, longstanding customs and practices, and when work-related items (e.g., vouchers, log books, memoranda, etc.) are the object of the search.

GSA does not presently have regulations governing warrantless searches of employee work areas. Each case, however, must be evaluated on a case-by-case basis. (b) (7)(E)

## 917.02 Inventory Policy

### 917.02A Purpose

This directive establishes the U.S. General Services Administration, Office of Inspector General (GSA-OIG) policy and procedures concerning the inventory of property lawfully taken into custody by Special Agents (SAs) of the GSA-OIG.

### 917.02B Definition

An inventory is an administrative measure designed to protect property while in agency custody; to protect the agency against claims of lost, stolen or damaged property; and to protect agency personnel and the public against injury or damaged property due to hazardous materials or substances that may be located within property taken into custody.

### 917.02C Policy

A complete inventory shall be made of all property that is taken into custody by the GSA- OIG. Inventories need not be made contemporaneously with the time property is taken into custody, but must be made as soon as practicable after the property to be inventoried has been transported to the location where it is to be stored. (b) (7)(E)

(Figure 917-03).

### 917.02D Inventories of Vehicles

This section of the directive provides additional guidelines concerning inventories of vehicles. For purposes of this section, the term vehicle shall include all mobile conveyances, to include water vessels and aircraft.

Special Agents may conduct an inventory of a vehicle without a warrant or probable cause when the vehicle has been taken into custody by the GSA-OIG.

(b) (7)(E)

#### 917.02E Scope of Inventory

The contents of all vehicles that are taken into custody by the GSA-OIG shall be subject to inventory in accordance with the provisions of this policy.

- An inventory should be conducted (b) (7)(E). If so, the vehicle may be (b) (7)(E) when (b) (7)(E) is able to conduct the inventory.
- A vehicle inventory shall extend to all areas of the vehicle in which personal property or hazardous materials may reasonably be found including, but not limited to, the passenger compartment, the glove compartment, the engine compartment, the trunk, and other storage compartments located on or in the vehicle.
- All closed containers, whether locked or unlocked, found on or within a vehicle shall be opened for purposes of the inventory.
- All contents of the vehicle found during the inventory shall be documented on the GSA-OIG inventory form (Figure 917-03). In addition to listing the items found during the inventory, Special Agents should document any pre-existing damage to the vehicle or its contents on the inventory form. Damage caused to the vehicle during the inventory should be noted as such on the inventory form.

#### 917.02F Property Control

After the vehicle is inventoried, the vehicle should be moved to a secure facility for safekeeping unless movement of the vehicle is limited by reasons of safety or practicality.

If the vehicle is unable to be moved, measures shall be taken to safeguard the vehicle and its contents.

When property of extraordinary value is located during an inventory, that property should be properly documented on the inventory form and then moved to secure storage.

If hazardous materials are located during the inventory, those items shall be handled and secured appropriately.

Although an inventory is not a search for evidence, any property that is discovered during the inventory that is contraband or evidence of a crime will be subject to seizure.

(b) (7)(E)

Special Agents will take appropriate measures to return property that is not subject to seizure to the lawful owner as soon as practical. The return of any property shall be (b) (7)(E) as soon as practicable after the property is returned.

Effective Date 2/12/2014

## 918.00 REPORTS OF INVESTIGATION AND LETTERHEAD REPORTS

### 918.01 OIG Policy on Reports of Investigation and Letterhead Reports

Office of Investigations (OI) investigative reports are issued in accordance with the general and qualitative standards that have been adopted by the Council of Inspectors General on Integrity and Efficiency (CIGIE) (Figure 901-06).

#### 918.01A Communicating Investigative Findings in Reports of Investigation versus Letterhead Reports

OIG Special Agents (SAs) communicate the results of investigations either in Reports of Investigations or in Letterhead Reports, when appropriate. A Report of Investigation is the standard method for communicating investigative findings to persons responsible for taking action on those findings. A Letterhead Report is used when:

- An investigation established that the complaint or allegation did not establish sufficient factual basis for further investigation, but a report to an official of GSA or another Government agency is appropriate.
- The investigation was for personnel security purposes, and involved arrest checks, other record checks, and/or pre-employment suitability inquiries on a prospective GSA employee.

#### 918.01B Standards for Reports of Investigation and Letterhead Reports

The following standards apply to all OIG investigative reports, whether in the Report of Investigation (ROI), or the Letterhead Report format.

- Investigative reports present factual data fully, accurately, and objectively.
- Factual investigative findings are substantiated by supportive evidence to demonstrate their accuracy and reasonableness.
- Investigative reports present information and factual investigative findings that are sufficiently comprehensive to allow the reader to reach a conclusion on the allegation/violation and the action that should be taken.

- (b) (7)(E) [REDACTED]

- Investigative reports are written clearly and concisely.

- (b) (7)(E) [REDACTED]

- Investigative reports are prepared by the case agent as soon as practical after conclusion of investigative activity. Investigative reports are then issued within (b) (7)(E) thereafter.
  - To prevent unauthorized dissemination and use, investigative reports are designated "For Official Use Only" and controlled accordingly. The "For Official Use Only" designation appears at the top and bottom of each page of the report.
  - Investigative reports are distributed to officials having the authority to act on the report contents.
- Exculpatory evidence and relevant mitigating information when discovered during an administrative proceeding should be contained in the ROI. Exculpatory evidence in a criminal or civil investigation must be brought to the attention of the prosecutor.

#### 918.02 Presentation Guidelines for Reports of Investigation and Letterhead Reports

Presentation guidelines applicable to Reports of Investigation and Letterhead Reports are as follows:

- **Order of Presentation of Information.** Information in the report should be organized in a logical and easy to understand fashion; information need not be presented based on the chronological sequence of the investigation or the events. When writing reports on complex or voluminous cases, the SA should consider organizing the report by subheadings. For example:
  - In a Standards of Conduct case involving several allegations, the report could be organized by the individual allegations.
  - In a case involving investigation of a number of contractors, the report could be organized by the individual contractors.
- **Capitalization.**
  - The last name of each person who is a subject of an investigation is typed in capital letters, as are all pronoun references to that person.
  - The full name of each corporation, company, or other business concern that is the subject of an investigation is typed in capital letters.
  - The names of federal, state, and local agencies/departments are typed in accordance with standard capitalization rules (upper and lower case letters).
- **Use of Personal Pronouns.** Investigative reports are normally written in the third person; however, first person personal pronouns are permissible as the situation dictates.
- **Quotations.** Quotations from laws, regulations, or other publications are not included in either the Details of Investigation section or report inserts if they exceed one-half page in length. When quotations exceed that standard, they can be attached as exhibits and summarized in either the Details of Investigation section or report inserts.

• (b) (7)(E)

(b) (7)(E) Reports are not intended to report investigative measures or techniques.

- Information from Official Personnel Folders. When writing reports on cases involving government employees, care must be taken not to include extraneous personal information from the employees' Official Personnel Folders. All Official Personnel Folder information reported must closely pertain to the matter under investigation.

- Information from Law Enforcement Agencies. SAs are cautioned to clearly notify police officials when they request arrest records for a personnel security investigation. (b) (7)(E)

- (b) (7)(E) is not normally included in Reports of Investigation or Letter Reports.

- (b) (7)(E) are not normally exhibited in Reports of Investigation. The (b) (7)(E) may be summarized in either the Basis for Investigation or Synopsis section.

### 918.03 Format and Contents of Reports of Investigation

The following paragraphs describe the general format of Reports of Investigations, and provide detailed guidance on the format and contents of each section in a Report of Investigation. A sample Report of Investigation appears in Figure 918-01.

#### 918.03A General Format of Reports of Investigations

General format requirements applicable to all Reports of Investigations are as follows:

- The Report of Investigation must contain the following sections: (1) Administrative Data Page(s); (2) Table of Contents; (3) Basis for Investigation; (4) Synopsis; (5) Details of Investigation; and (6) List of Exhibits.

- Additional sections may include, among others, Subjects and Defense Counsel, Potential Offenses, and List of Witnesses. Recognizing that special information is required, SACs may choose to include sections such as Venue, Statute of Limitations, Assets, Agency Program Background, Entity or Organization Background, etc. The prime objective is to prepare a Report that effectively communicates investigative findings to appropriate readers.

- Each section of the report starts on a new page, and the report pages are numbered consecutively beginning with the first page of the Basis for Investigation section. (The Administrative Data Page(s) and Table of Contents are not numbered).

- The Report of Investigation is contained within official OIG front and back report covers.

- (b) (7)(E)

•Each section of the Report is headed by the nomenclature of that section, typed in UPPER CASE LETTERS, underlined, and centered at the top of the first page of that section.

#### 918.03B Format and Contents of Administrative Data Page(s)

The Administrative Data Page is a mandatory section.

The first Administrative Data Page is headed by the words ADMINISTRATIVE DATA PAGE. If additional pages are necessary, no such heading is required on them. The following captions are presented beneath this heading, at the left hand margin:

•Character of Case: Cite case category (Examples: Fraud against the Government; Theft of Government Property). It is acceptable to use more than one case category, if appropriate.

•Subjects: Complete subject identity. Identifying data on each subject includes: (1) full name, including middle name if known; (2) position; (3) all known aliases or "doing business as" names; and (4) address.

When subjects are contractors, the following identification standards apply:

In cases involving multiple contractor subjects, the Subject section: (1) shows the full name and address of each contractor; and (2) lists the prime contractor first, with the designation "Prime Contractor" after that contractor's name.

If the investigation has developed an official of the contracting firm as a subject, his/her name, position and residence address are shown after the name and address of the contracting firm. An example of this type of Subject section is shown in Figure 918-01.

When the subject of an investigation is not known, the Subject section states UNKNOWN SUBJECT in capital letters.

•Case File Number: The OIG case number (b) (7)(E) .

•Related Case File Number: Cross-referenced cases.

•Date of Report: The date the Report of Investigation is signed by the (b) (7)(E)

•Prepared by: Signature of the responsible SA, with his/her name and title typed beneath the signature.

•Reviewed by: When appropriate, signature of the (b) (7)(E) reviewing the Report, with his/her name and title typed beneath the signature.

•Approved by: (b) (7)(E)

The following words are centered at the bottom of the Administrative Data Page(s) and printed on individual lines in upper case letters:

OFFICE OF INVESTIGATIONS OFFICE OF INSPECTOR GENERAL U.S. GENERAL SERVICES ADMINISTRATION

### 918.03C Format and Contents of Table of Contents

The Table of Contents is a mandatory section.

Unless subheadings are included in the Details of Investigation, the Table of Contents lists only the major report sections. When subheadings are used in the Details of Investigation, they are included in the Table of Contents.

### 918.03D Format and Contents of Basis for Investigation

The Basis for Investigation is a mandatory section.

This section cites the source(s) of information and describes the allegations. See Figure 918-01 and Figure 918-02 for examples.

When a case involves confidential witnesses or complainants the following legend is typed in upper case letters at the bottom of the section:

“THIS REPORT CONTAINS INFORMATION FURNISHED BY PERSON(S) WHOSE IDENTITIES MAY NOT BE DISCLOSED EXCEPT AS PROVIDED BY THE INSPECTOR GENERAL ACT OR CIVIL SERVICE REFORM ACT OF 1978. IMPROPER DISCLOSURE MAY RESULT IN PUNITIVE ACTION.”

### 918.03E Format and Contents of Synopsis

The Synopsis is a mandatory section.

Standards relative to the contents of the Synopsis are as follows:

- The Synopsis must be fully substantiated by one or more exhibits to the Report of Investigation.
- The Synopsis must provide sufficient information for the reader to conclude that the matter merits action.
- The Synopsis must not include opinions or conclusions of the SA. Instead, the Synopsis identifies and summarizes information from which the reader can formulate an independent conclusion.

This section should provide the reader with a summary of the investigative findings, nature of the fraud scheme or other wrongdoing, significant or unique issues involved, and other information to convey an overall understanding of the case.

This section is not intended to include every investigative detail, cite every witness or each document reference, or include specifics that are not necessary to provide an overview. A detailed chronological presentation of the investigative steps is not desired; rather, the results are to be stated in a logical sequence for the benefit of the reader.

Details, such as dates of investigation or lengthy titles documented elsewhere in the Report, are not to be included in the narrative unless necessary.

### 918.03F Format and Contents of Details of Investigation

Details of the Investigation is a mandatory section.

The purpose of the Details of Investigation is to bring the investigation into proper focus for the reader, by presenting clearly, concisely, logically, and factually the pertinent information contained in the exhibits to the report. Sub-headings may be used to enhance the organization of the Details of Investigation (See Sections 918.02 and 918.03).

Exhibits are an essential part of a Report of Investigation. The Details of Investigation section must contain adequate references to exhibits, and page numbers of exhibits may be added when appropriate.

The witnesses must be identified and their testimony presented in a logical order. If sub-headings are used, they are positioned and styled so as not to be confused with major section headings.

### 918.03G Format and Contents of Potential Offenses

Potential Offenses is an optional section.

This section cites statute(s) that may have been violated by particular subjects. See Figure 918-02.

### 918.03H Format and Contents of Subjects and Defense Counsel

Subjects and Defense Counsel is an optional section.

This section contains a listing or discussion of all subjects of the investigation, including both individuals and business entities. The identifying information, including full name, aliases, home and business addresses of subjects, telephone numbers, social security or employer identification number, etc., is included for each individual and entity listed as a subject. This section also sets forth names, business addresses and telephone numbers of representatives (such as attorneys) of subjects. See Figure 918-02.

### 918.03I Format and Contents of List of Witnesses

List of Witnesses is an optional section.

This section lists witnesses whose testimony would be necessary to prove the case. The addresses and telephone numbers are shown after each witness' name, and, if appropriate, job title. For example, see Figure 918-02.

### 918.03J Format and Contents of List of Exhibits

List of Exhibits is a mandatory section that may take one of two forms, either listing the witnesses and exhibits together (Figure 918-01) or separately (Figure 918-02).

If listing the witnesses and exhibits together in the ROI, this section contains three columns: (1) Witness; (2) Exhibit Number; and (3) Description.

- The witness' full name, job title (if appropriate), address and telephone number are listed in the left-most column after a sequential witness number preceded by a W (e.g. W1, W2, etc.).
- The Exhibit Number is a sequential number for each exhibit associated with a given witness. For example, witness W2 may have two or more exhibits attributed to or associated with him/her.
- The third column contains a description of the exhibit.

If a List of Witnesses section is included, the List of Exhibits Section shall contain only the Exhibit Number and Description, and shall not contain a witness number. (Figure 918-02).

Exhibits may consist of copies of statements and documents, such as affidavits, memoranda of interview/activity, canceled checks, invoices, bank records, books of account, related work papers, etc. The Report must contain adequate references to any exhibits, and shall describe the relevance of any and all exhibits. Accordingly, exhibits are separately and sequentially numbered, in the order they are originally mentioned in the Report, to facilitate reference and avoid confusion. When the Report is completed, exhibits are arranged (tabbed and bound, if appropriate) in their numerical order.

#### 918.03K Report Inserts

Report inserts are memoranda documenting investigative interviews and activities. They are routinely prepared as soon as practical after the interview/activity, and may be included as exhibits to the ROI.

There are two types of memoranda report inserts: the Memorandum of Interview (Figure 918-05) and the Memorandum of Activity (Figure 918-06).

1. Memorandum of Interview. Each investigative interview is documented in a Memorandum of Interview, (b) (7)(E)

[REDACTED]

2. Memorandum of Activity. A Memorandum of Activity is prepared for each pertinent investigative activity and each pertinent record/document review. (b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

(b) (7)(E) Therefore, a Memorandum of Activity is used to summarize information contained in these types of records.

Memoranda of Activity and Memoranda of Interview are also used to document investigative results occurring subsequent to issuance of the Report of Investigation. Such memoranda can be incorporated into a supplemental Report of Investigation, or, if appropriate, forwarded to the action official by Transmittal Memorandum.

#### 918.04 Format and Contents of Letterhead Reports

Letterhead Reports are not required to adhere to a prescribed format, but they must contain the following information:

- investigative activity performed;
- a summary of significant findings or disclosures; and
- a summary of specific legal, criminal or administrative determinations and actions taken.

Letterhead Reports to GSA management officials must be prepared as a memorandum in accordance with GSA Order OAD 1804.12, Part 3, Section 1, Paragraphs 22 and 23, and Section 2 (Section 919.03B). When the Letter Report will be provided to GSA management officials, the following additional data must be added:

- identification of the system of records; and
- the name and office telephone number of a Regional Investigations Office contact. Sample Letterhead Report Issued for Information Only appears in Figure 918-03. Sample

Letterhead Report for Action Consideration appears in Figure 918-04.

Letterhead Reports are contained within official OIG front and back report covers.

#### 918.04A Preparing Referrals for Criminal Prosecutive Consideration

When an investigation shows potential for criminal prosecution, a formal referral to the appropriate prosecutorial office may be made. Depending on the circumstances, and the desires of the prosecuting official, the referral can be made by issuing a Report of Investigation or other documentation as requested by the prosecutor.

All formal referrals should concisely identify the subjects, subject matter of the investigation, and potential violation(s).

A letter from (b) (7)(E) shall be used to transmit all formal referrals. Transmittal letters should concisely identify the subjects, subject matter of the investigation, and potential violation(s). When appropriate, the transmittal letter acknowledges acceptance of the case during early consultation.

Effective Date 2/12/2014

#### 919.00 REFERRALS AND POST-INVESTIGATIVE ACTIVITY

Reports of Investigation and Letterhead Reports are referred outside the OIG for:

- criminal prosecutive consideration;
- civil action;
- GSA management officials' administrative action or information; or
- other agencies' action or information.

All Reports of Investigation and Letterhead Reports must be transmitted in accordance with the OIG procedures for safeguarding "For Official Use Only" information.

Reports of Investigation and Letterhead Reports with its corresponding exhibits should be uploaded in the (b) (7)(E) with a hard copy being transmitted to the action officials along with an original transmittal letter or memorandum.

#### 919.01 Referrals for Criminal Prosecutive Consideration

##### 919.01A Reporting and Following Up on Referrals for Criminal Prosecutorial Consideration

Pending prosecutorial determination, the responsible Special Agent (SA) and manager should monitor the time elapsed after each referral to ensure a timely resolution to the referral.

When a case is declined for criminal prosecution but the prosecuting authority has not provided written documentation of that decision, the SA prepares a confirmation letter giving an overview of the referral and the reason(s) for declination.

When a case is declined for criminal prosecution by DOJ/the U.S. Attorney's Office, the SA should be alert to the case's potential for referral: (1) to state or local prosecutors; (2) for civil action (Section 708.02); and (3) for administrative action by management officials.

#### 919.02 Referrals to GSA Management Officials for Administrative Action or Information

##### 919.02A Purposes of Administrative/Information Referrals to GSA Management Officials

Investigative results are forwarded to GSA management officials for:

- consideration of administrative action; or
- information purposes, when the Special Agent in Charge (SAC) or Assistant Inspector General for Investigations (AIGI) deems it appropriate.

## 919.02B Making Administrative/Information Referrals to GSA Management Officials

1. General Standards and Procedures for Making Administrative/Information Referrals. General standards and procedures for making administrative/information referrals are as follows:

- Referrals are made either by memoranda that transmit Reports of Investigation or by Letterhead Reports. Section 907.01A details OIG policy on using Reports of Investigation versus Letterhead Reports. Letterhead Reports and memoranda that transmit Reports of Investigation should be prepared in accordance with GSA Order OAD P 1804.12, GSA Correspondence Management, Part 3, Section 1, Paragraphs 22 and 23, and Section 2. A sample memorandum used for this purpose is presented at Figure 919-01.
- Referrals are addressed to the Administrator, Heads of Services and Staff Offices, Regional Administrators, or other program officials who have line authority over the program areas/employees.
- All referrals for consideration of administrative action: (1) reference an attached Disposition Report (Figure 919-02); and (2) ask that the management officials use this form to reply to the OIG on the administrative action taken or to be taken.
- Signatory authority for administrative/information referrals is as follows: (b) (7)(E)

2. Standards and Procedures for Making Specific Types of Administrative/Information Referrals. Standards and procedures for making specific types of administrative/information referrals are as follows:

- Referrals for consideration of suspension/debarment action are made in accordance with the specific standards and procedures set forth in Subchapter 916.
- Referrals for consideration of administrative action other than suspension and debarment are made by GSA memorandum that: (1) transmits the Report of Investigation; and (2) includes the following information:
  - an introductory statement which sets forth: (1) the purpose of the referral (i.e., that the investigation has been completed and the Report of Investigation is being referred for consideration of administrative action); (2) the identification of the subject(s); (3) the allegation(s) or complaint(s) developed or received; (4) the copy number of the Report of Investigation; and (5) a statement that the facts developed may be proscribed by a specifically cited section or sections of the GSA Standards of Conduct (ADM 7900.9);
  - if applicable, a statement that the case was referred for prosecutive consideration, and a report on the status of that referral;
  - statements that identify the system of records and the routine use under the Privacy Act of 1974;
  - a statement prohibiting duplication of the Report of Investigation, with the caveat that the Director of Human Resources may duplicate parts or all of it when: (1) the referral is used as a basis for adverse action against a GSA employee; and (2) immediate notification is made to the signatory of the referral;

- a statement asking that the addressee complete and return the Disposition Report form to the referral signatory within (b) (7)(E); and
  - a request that the addressee return the Report of Investigation after it has served his/her purpose.
- Referrals for information purposes are made in accordance with the specific standards and procedures for Letterhead Reports set forth in Section 918.04.

#### 919.02C Following Up on Administrative Referrals to GSA Management Officials

If the office to which the administrative matter was referred has not responded to the referral or submitted a completed Disposition Report within the timeframe specified in the referral (Section 919.02B), the SAC or delegate should contact the management official, inquire as to the action taken or to be taken, and an anticipated date that final action will be taken. (b) (7)(E) shall take any further follow-up action as deemed necessary and appropriate to ensure resolution of the referral. These contacts should be documented in the case file. In the event of continued non-responsiveness by the management official, the matter is referred for follow-up by (b) (7)(E). In the case of referrals signed by (b) (7)(E), the contact is made by (b) (7)(E). In the case of referrals signed by (b) (7)(E), the contact is made by the (b) (7)(E). In the event of continued non-responsiveness by the management official, the matter is referred for follow-up by (b) (7)(E).

Upon receipt of the completed Disposition Report form, the SAC (whose office generated the referral) evaluates whether the reported administrative action is commensurate with: (1) the factual investigative findings; and (2) the appropriate Agency regulations concerning administrative actions. If the action does not appear commensurate with these findings and regulations, the SAC should contact the management official, discuss the matter, and document the investigative file.

#### 919.03 Referrals to Other Agencies

##### 919.03A Referrals to the FBI

Standards and procedures for referrals to the FBI are presented in Section 908.01C.

##### 919.03B Referrals to Other Law Enforcement Agencies

Standards and procedures for referrals to law enforcement agencies other than the FBI are presented in Section 908.01D.

##### 919.03C Referrals to Other Executive Branch Agencies

OIG investigative results involving the programs or employees of other agencies are referred either by letter that transmits the Report of Investigation or by Letterhead Report.

Normally, these referrals are addressed to the local head of the other agency's OIG or the local head of the other agency; and they are signed by (b) (7)(E). However, when the referral is to an AIGI in another agency, it is signed by (b) (7)(E); and when the referral is to the head of another agency, or the IG of another agency, it is signed by (b) (7)(E).

In instances where administrative action by the other agency is warranted, the transmittal letter used for this purpose contains the following:

- a paragraph that concisely sets forth the significant wrongdoings or irregularities;
- if applicable, a statement that the case was referred to DOJ/a U.S. Attorney's Office for prosecution, and a report on the status of that referral;
- statements that identify the system of records and the routine use under the Privacy Act of 1974;
- a statement that the information is furnished for whatever action is deemed necessary; and
- if applicable, a request that the signatory of the referral be advised of actions taken on it.

#### 919.03D Referrals to the Office of Government Ethics

All investigative cases in which a referral from the OIG has been made to the Department of Justice (DOJ) of allegations involving federal conflict of interest violations, namely 18 USC 203 (compensated representational activities before the government), 205 (acting as an agent or attorney before the government), 207 (post- employment eliminations), 208 (acts affecting a personal financial interest), and 209 (supplementary salary) require notification to the Office of Government Ethics (OGE). Any office making a referral to the DOJ for conflict of interest cases will be responsible for making the referral to OGE. Special Agents will complete OGE form 202, Notification of Conflict of Interest Referral (<http://www.usoge.gov/>), and submit the form to his/her supervisor for approval. (b) (7)(E) will review the form and forward it to the OGE at the address listed on the form in a timely manner. A copy of the form should also be sent to the Deputy Assistant Inspector General for Investigations (DAIGI).

Each office must promptly notify OGE of the disposition of such referrals, i.e., indictment and prosecution, declination, and any disciplinary or corrective action taken when one of these referred cases has been declined. Information relating to the disposition of a referral must be communicated to the OGE in writing and a copy should be sent to the DAIGI. Completed copies of OGE Form 202 and subsequent disposition notifications will be incorporated into the official case file. Each office will also initiate and maintain an administrative file containing completed copies of all notifications made to OGE. On an (b) (7)(E) basis the Office of Investigations will report the number of OGE referrals to the GSA Office of General Counsel.

Effective Date 2/12/2014

## 920.00 PROGRAM FRAUD CIVIL REMEDIES ACT INVESTIGATIONS AND REFERRALS

### 920.01 Investigations and Referrals Under the Program Fraud Civil Remedies Act (PFCRA)

#### 920.01A Definition and Regulatory Basis for Administrative Action Under the PFCRA

The PFCRA (31 U.S.C. §§3801-3812) creates an administrative procedure whereby authorized federal agencies may litigate false claims and false statements administratively. If found liable, a person may be penalized up to \$5,500 per claim or statement and may also be assessed damages.

The PFCRA necessitates that (1) the false claims or false statements involve a value of less than \$150,000 and (2) the Department of Justice (DOJ) approve initiation of this procedure.

The regulatory basis for General Services Administration (GSA) actions in this regard is 41 Code of Federal Regulations 105-70.

#### 920.01B Causes for Litigating Under the PFCRA

The Agency initiates this administrative remedy when there is adequate evidence to believe that a person (meaning any individual, partnership, corporation, association or private organization) has made, submitted, presented, or caused to be made, submitted, or presented, false fictitious, or fraudulent claims or written statements to GSA authorities or to their agents.

A claim is defined as any request, demand, or submission made to:

- GSA for property, services, or money; or
- recipients of property, services, or money when GSA paid for any portion of the underlying contract.

A statement is defined as any representation, certification, affirmation, document, record, or accounting/bookkeeping entry made with respect to:

- claims or approval or payment of a claim; or
- bids, proposals, or contracts.

The PFCRA only applies to false claims or false statements made on or after October 21, 1986.

#### 920.01C OIG Policy on Investigations and Referrals Involving the PFCRA

The Office of Investigations (OI) opens and conducts investigations of alleged false claims and false statements to develop evidence for referral to prosecutive authorities for criminal action and/or civil suit under the False Claims Act.

When the value of the false claims/false statements is under \$150,000 and, pursuant to 41 CFR Part 105-70.004(b), JI concludes that an action under PFCRA may be warranted, JI refers the matter to the Office of the Counsel to the Inspector General (JC) for review and referral to GSA's General Counsel for administrative litigation.

(b) (7)(E)

Subpoena requests pursuant to the authority conferred by 31 U.S.C. §3804(a) are made in accordance with OIG policy set forth at Section 707.02 of the OIG Policy and Procedures Manual.

1. Referrals to General Counsel. All PFCRA referrals include: (1) a referral memorandum; (2) the Report of Investigation as an attachment to the memorandum; and (3) (b) (7)(E) as attachments to the referral memorandum. The referral memorandum is addressed to the General Counsel and prepared for the signature of (b) (7)(E). A concurrence line for (b) (7)(E) is placed on the official file copy of the referral memorandum. The content of (b) (7)(E) memoranda is as follows:

- Subject: presents the wording "Recommendation for Administrative Litigation under the Program Fraud Civil Remedies Act" followed by the title of the case, and the name(s) of the individual, corporation, association, or organization believed to be liable, and the investigations file number.
- Opening Paragraph: presents the recommendation, the names of all involved individuals and concerns, and the evidence supporting the allegations of liability. This paragraph should also indicate that the investigation is substantially complete and reference the declination/confirmation letters. The opening paragraph usually starts: "This memorandum contains a recommendation that you consider issuing a complaint against .... pursuant to subparagraph 105.70.007 of the Code of Federal Regulations . . ."
- Subsequent Paragraphs: present the following information:
  - a description of the claims or statements upon which the allegations of liability are based;
  - an estimate of the amount of money or the value of property, services, or other benefits falsely requested or demanded;
  - a statement of any exculpatory or mitigating circumstances that may relate to the claims or statements; and
  - a statement that there is a reasonable prospect of collecting an appropriate amount of penalties and assessments.
- Current Addresses: presents the current addresses of the concerns and individuals.
- Disposition Report: references the Disposition Report that is attached with each PFCRA referral memorandum and provides for the General Counsel to reply to (b) (7)(E) on whether action was taken. The Disposition Report Form is presented at Figure 919-02.

- Privacy Act Statement: presents the following statement: “You are advised that this information is from a system of records known as “GSA/ADM 24, Investigation Case Files,” which is subject to the provisions of the Privacy Act of 1974. Consequently, this information may be disclosed to appropriate GSA officials who have a need for it in the performance of their official duties.”

- Statement of Limitations: presents the following statement: “Release or disclosure of information in this memorandum or any attached documentation or report to the subject(s) of the investigation or to other parties outside the General Counsel’s Office must have the prior written approval of (b) (7)(E). The General Counsel is to notify my office if any portion is duplicated.”

- Point of Contact Within the OIG: presents the name and telephone number of (b) (7)(E) and states that he/she is to be contacted if General Counsel needs additional information.

- Attachments: references all items that are attached to the referral memorandum.

If names of individuals or business concerns are used in the referral memorandum, Report of Investigation, and/or declination/confirmation letters, and they were not involved in the alleged fraud, a statement to that effect should be included in the referral memorandum.

2. Subsequent Investigative Activity. In subsequent referrals of an action to the General Counsel, JI, along with JC, serves as the point of contact for any questions raised by the Office of General Counsel.

If, in the course of further investigation, evidence is disclosed indicating criminality or civil liability, the Special Agent notes that nothing in the PFCRA limits the OIG’s discretion to refer allegations directly to the DOJ.

Upon conclusion of investigative activity, the Special Agent prepares the Report of Investigation in accordance with standard procedures. The Report is formally transmitted to General Counsel.

Effective Date 3/14/2018

## 921.00 POLICY FOR COMPUTER FORENSICS

### 921.01A Purpose

This section contains policies and procedures applicable to the seizure and forensic analysis of digital media/devices conducted by the GSA OIG. The Digital Crimes and Forensics Unit (DCFU) will be the primary unit charged with seizing and analyzing computers and related digital media consistent with the guidance prescribed in this section. Due to the evolving state of computer technology, this policy and all DCFU operating procedures will be reviewed (b) (7)(E) to ensure accountability for the latest developments in technology.

### 921.01B Reference

1. This chapter is issued under the Inspector General Act of 1978 (5 U.S.C Appendix) as amended.
2. Quality Standards for Digital Forensics (QSDF), Council of the Inspectors General on Integrity and Efficiency (CIGIE) Publication, November 2012.
3. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Department of Justice (DOJ) Bulletin, July 2002.
4. Legal Ramifications of Digital Imaging in Law Enforcement, Federal Bureau of Investigation (FBI) Publication, October 2000.
5. 18 U.S.C. § 1030 (fraud and related activity in connection with computers); and 18 U.S.C. § 1029 (fraud and related activity in connection with access devices).

### 921.01C Definitions

Acquisition: The collection, seizure, or voluntary deposit of digital evidence.

Approved Forensic Software: (b) (7)(E)

Archive: (b) (7)(E)

Binary: A two-digit (Base-2) numerical system, that computers use to store data and compute functions. Computers use the binary system because digital switches inside the computer can only be set to either on or off, which are represented by a 1 or 0. Although the binary system consists of only ones and zeros, aggregation of the two digits can be used to represent any number.

Case Agent: The SA who is responsible for conducting the investigation.

Copy: An accurate reproduction of information contained on an original digital storage platform, independent of the original digital storage platform (e.g., a printout of an email). A copy in this sense is not necessarily an identical duplicate of a file, but a representation of the file's contents.

Data Objects: Objects or information of potential probative value associated with digital storage platforms (e.g., a file or database record). Data objects may occur in different formats without altering the original information.

Digital Crimes and Forensics Unit (DCFU): The GSA OIG's forensic program for organizing and executing forensic analyses of digital evidence.

Digital Evidence (DE): Information of probative value in binary or digital form.

Digital Evidence Acquisition: (b) (7)(E)

Digital Media: Any device which can store information in electronic form. This includes, but is not limited to, all of the following: cellular device, flash drive, floppy disk, hard drive, thumb/USB drive, and global positioning systems.

Digital Media Forensic Analysis: The systematic process of examining digital evidence to extract and/or recover data objects.

Digital Storage Platforms: Items on which data objects or information may be stored and/or through which data objects are transferred. These platforms include physical items such as hard drives, memory cards, and logical storage locations, including network shares.

(b) (7)(E) The (b) (7)(E) oversees the DCFU unit and, tangentially, Special Agents assigned to Regional GSA/OIG offices with collateral DCFU duties, specifically the (b) (7)(E) has responsibility of those SA's DCFU activities.

Forensic Image: Exact, sector-by-sector or bit-by-bit copy of the subject evidence media.

Hardware/Software Write-Protection: Write-protection is the ability of a hardware device or software program to prevent new information from being written or old information being changed. Typically, this protection means you can read the data, but not edit or add data. (b) (7)(E)

Hard Drive Imaging (b) (7)(E)

Hash Value: A string of characters and numbers derived from a file, group of files, or portion of a file, based on a standard mathematical algorithm applied to the data. A hash value can be used to confirm that two digital files or objects are the same by comparing their separate hash values. (b) (7)(E)

The Federal court ruled that one method of authenticating electronic evidence under the Federal Rules of Evidence 901 (b)(4) is the use of hash values.

Official Case File: All documents and other items of probative value relating to a specific investigation generally maintained in (b) (7)(E)

Original and forensic copies of original: The original digital storage platform is the source drive or storage location at the time that the examiner makes the first acquisition. The concept of "original

digital evidence" is used to establish chain of custody and ownership when data is acquired or a storage platform is seized. Subsequent image files with the same content in the data area will also be considered identical even if they are packaged differently or generated at a different time (e.g., a compressed versus an uncompressed forensic image of a hard drive).

Removable Media: Items that store digital information and can be easily removed. This media includes, but is not limited to, all of the following: Blu-Ray disks, CDs, cartridges, DVDs, diskettes, floppy disks, tape, flash drives and USB drives.

Requestor: The SA or organization requesting the computer forensic analysis.

Reporting Organization: The organization in charge of the investigation, i.e., GSA OIG.

Seized Computer Evidence Recovery Specialist (SCERS): Employees who have successfully completed FLETC computer forensic training. There are different tiers of expertise within the DCFU program: (b) (7)(E)

Scientific Working Group for Digital Evidence (SWGDE): Organization comprised of members from U.S. Government and law enforcement organizations actively engaged in the field of digital and multimedia evidence. The organization's purpose is to foster communication and cooperation as well as to ensure quality and consistency within the forensic community.

#### 921.01D Authority

GSA OIG must lawfully search and seize digital media when aiding an investigation. The Fourth Amendment limits the ability of government agents to search for and seize evidence without a warrant. Prior to forensic examination, DCFU personnel must ensure they have legal authority (i.e., search warrant, consent, etc.) to search digital data. Due to data storage methods on computers and other digital devices, the large volume of data usually present, and the complexities involved with searching the data, an organization is frequently authorized to seize all the digital data and subsequently search this data at a later time in a controlled environment. The subsequent search must be within the bounds of the consent or comply with the search warrant or other authority. (b) (7)(E)

#### 921.01E Responsibilities

It is (b) (7)(E) responsibility to ensure that the DCFU complies with CIGIE standards for legal authority, integrity of evidence, qualified personnel, forensic documentation, and forensic analysis reports.

1. Legal Authority: (b) (7)(E)

Refer to Section 921.01D.

2. Integrity of Evidence: Digital data can easily be altered, and environmental conditions (such as strong magnetic fields) can affect the integrity of data on certain storage mediums. (b) (7)(E)

Refer to Section 921.01K.

3. Qualified Personnel: All personnel performing a forensic review must be fully trained to prevent any evidence reviewed from being invalidated. DCFU personnel assigned to perform digital forensic activities must possess technical competency for the tasks they are assigned. All DCFU personnel who are actively engaging in forensic cases must be current on all training and certification requirements to qualify as compliant with updated CIGIE requirements. Refer to Sections 921.01F, 921.01G and 921.01H. All DCFU personnel are required to immediately report any arrest, conviction, or other potential misconduct issue that may impeach or otherwise jeopardize the performance of your duties.

4. Forensic Documentation: Evidentiary standards require that each forensic digital evidence review is documented. The documentation must detail forensic activities and results to meet the requestor's needs and allow for the evaluation of forensic activities with these standards. Refer to Section 921.01L.

5. Forensic Analysis Reports: Reports and related documentation should include case identifiers, submission numbers, identify the dates of the forensic work as well as results, conclusions and derived items. Refer to Section 921.01M.

The (b) (7)(E) and has overall responsibility of the DCFU unit. The (b) (7)(E) or designee, provides oversight of all OIG digital evidence operations. The (b) (7)(E) shall have the following duties:

1. Guide DCFU personnel in acquiring, seizing, handling, and storing of all DE.
2. Create DCFU policy and procedures as needed.
3. Be responsible for the operation and administration of the DCFU. Responsibilities include, but are not limited to the following:
  - a. Coordinates requests for forensic examinations.
  - b. Ensure DCFU personnel properly document supporting documentation.
  - c. Conducts quality management reviews of all DCFU work products.
  - d. Prepare reports as required.
  - e. Requisition and maintenance of equipment and supplies.
  - f. Coordinate quality control efforts and liaison with other digital crimes programs.
  - g. Ensure DCFU personnel receive training to conduct forensic examinations as described in Section 921.01H and that professional and technical standards are maintained.
  - h. Support DCFU requests from outside agencies when appropriate.

DCFU personnel will perform forensic examinations and reviews. Their roles and responsibilities are detailed in Table E-1: Personnel Roles & Responsibilities Chart.

Table E-1: Personnel Roles & Responsibilities

(b) (7)(E)

#### HANDLE, IMAGE & SEIZE DIGITAL MEDIA

- DCFU personnel with minimal training.
- Personnel are considered first responders authorized to handle, image, and seize.

(b) (7)(E)

#### TECHNICAL ANALYSIS

- Additional training and a minimum of (b) (7)(E) experience.
- DCFU personnel who have been trained to the technician level can image, search, find and extract digital evidence.

(b) (7)(E)

#### ADVANCED TECHNICAL ANALYSIS & TROUBLESHOOTING

- These personnel have received extensive training and possess the experience necessary to complete the most technically complex digital evidence examinations and analysis.

Tier 4: (b) (7)(E)

#### DCFU Administrator

- The (b) (7)(E) has expert knowledge, training and experience to perform all three previous roles and duties.
- The (b) (7)(E) will have oversight of Administrative Reviews, Technical Reviews, Validation Testing, and Review of Quality System (see Section 921.01N) per CIGIE guidelines.

#### 921.01F Selection for DCFU Personnel

A Special Agent may apply to the DCFU program by contacting their respective Special Agents in Charge (SACs) who have the discretion to forward the candidate's name to the (b) (7)(E) for consideration. Final approval to the program requires (b) (7)(E) concurrence and approval; as well as budgetary and resource concerns. Once accepted into the program, they must complete specialized training. Both are discussed in Section 921.01H, Table H-1, under (b) (7)(E)

Digital forensics support to investigations can involve a wide range of activities. During an examination,

(b) (7)(E)

Therefore, the selection process takes the following into consideration: education, experience, character, ability to understand technical concepts and the ability

to solve problems. Preferably, all DCFU candidates will have a 4-year college degree, but hands-on experience handling complex problems encountered during forensic reviews is a valid substitute for a college education. Each candidate must possess and maintain the highest standards of conduct and ethics, including unimpeachable honesty and integrity. With regards to technical skills, candidates must be able to comprehend and communicate complex forensic concepts. They must also be able to analyze a forensic problem and determine the best course of action to resolve it. This skill set is vital when troubleshooting various types of computer equipment and when determining the proper course of action to resolve forensic challenges.

#### 921.01G Competency

Personnel performing digital forensics must demonstrate they are competent to perform digital forensics before performing independent work. Most formal digital forensic training programs include both a written and practical exam at the end of the course, and this examination is sufficient to demonstrate competency. Likewise, an agency may choose to accept a formal certification in digital or computer forensics achieved through testing as a demonstration of competency.

#### 921.01H Training and Professional Development for DCFU Personnel

After the DCFU candidates have completed the introductory training, they will be considered (b) (7)(E) DCFU personnel and will assist the regional DCFU personnel. In accordance with new CIGIE guidelines, additional training will be required for the DCFU personnel to attain (b) (7)(E) status; otherwise they will be deemed noncompliant with CIGIE requirements. The DCFU personnel must use the forensic software approved by the (b) (7)(E) DCFU personnel should remain proficient in their area of computer forensic expertise. Supplemental training will be approved for continuing education by the (b) (7)(E) DCFU personnel must demonstrate that they are competent to perform digital forensics before performing independent work.

These new DCFU personnel must receive training to build up competency; this training includes the following concepts:

1. Digital evidence theory
2. Pre-examination procedures
3. Digital evidence integrity
4. Digital device acquisition
5. Media assessment and analysis
6. Data recovery
7. Analysis of recovered data
8. Documentation and reporting

9. Legal considerations and ethics

10. GSA OIG forensic analysis SOPs

11. GSA OIG quality management processes

DCFU personnel must receive continuing education and training to maintain the necessary skills to perform digital forensic tasks despite ever changing technologies. The (b) (7)(E) will perform (b) (7)(E) review of the DCFU team's proficiency and schedule training to ensure that CIGIE guidelines for training are being met, refer to Table H-1: Training Guidelines. This continuing education and training is crucial in maintaining the integrity of the forensic program since training and education records may be introduced as part of legal proceedings involving the individual's qualifications.

Table H-1: Training Guidelines

(b) (7)(E)

During a 3 year period, DCFU personnel must receive a minimum of (b) (7)(E) of training.

- DCFU Training Program

- (b) (7)(E) DEASTP and SCERS (or their equivalents as determined by the (b) (7)(E)

- Cellebrite Mobile Forensics Course

(b) (7)(E)

During a 3 year period, DCFU personnel must receive a minimum of (b) (7)(E) of training.

- The (b) (7)(E) will review and approve other training venues with due consideration for both technical and budgetary requirements.

(b) (7)(E)

During a 3 year period, DCFU personnel must receive a minimum of (b) (7)(E) of training.

- The (b) (7)(E) will review and approve other training venues with due consideration for both technical and budgetary requirements.

Tier 4: (b) (7)(E) (Forensics Examiner)

During a 3 year period, the (b) (7)(E) must receive a minimum of (b) (7)(E) of training.

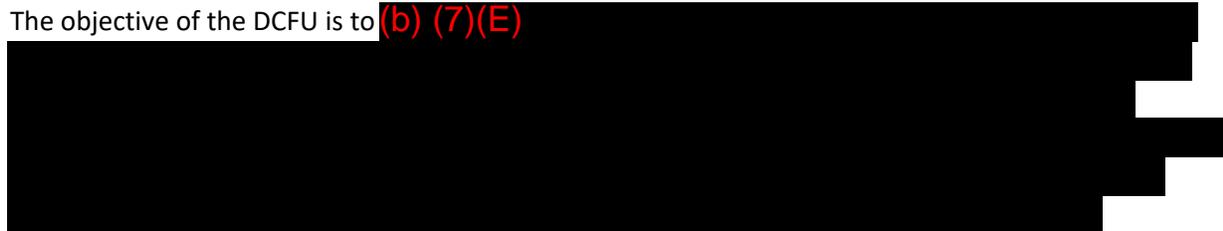
- The (b) (7)(E) will review and approve other training venues with due consideration for both technical and budgetary requirements.

All personnel performing digital forensics must receive continuing education in digital forensics, information technology, or related topics. This training can be accomplished through a variety of methods, including but not limited to: formal training classes, conferences, online training, and in-house training or practice as approved by the (b) (7)(E)

Personnel performing digital forensics must continue to maintain their proficiency to perform digital forensics. DCFU personnel must pass a practical proficiency test once every three years. An agency may choose to have forensic personnel complete this requirement through a test developed in-house. DCFU will retain records of the successful completion of the proficiency tests.

#### 921.01I Resources

The objective of the DCFU is to (b) (7)(E)

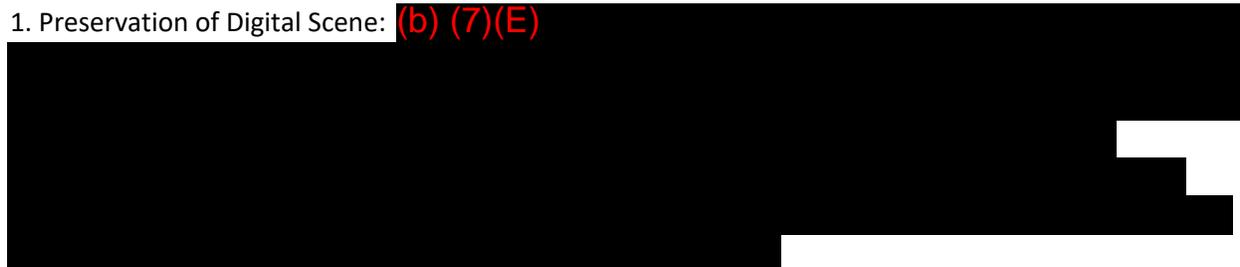


#### 921.01J Requesting Digital Forensic Assistance

If an agent assigned to a case requires forensic analysis, they should complete a Digital Forensics Request form (see Figure 921-01). If an agent requires search warrant support, they should complete a Search Warrant Support Report form (see Figure 921-01A). Both forms, as needed, shall be approved by (b) (7)(E), and sent to the (b) (7)(E). The (b) (7)(E) will assess which resources are needed to fulfill the expectations of the case agent regarding forensic analysis. Since DCFU personnel are located in various regional offices and have different workloads and priorities, the (b) (7)(E) will then contact the appropriate SAC to determine DCFU's availability. Depending upon time availability and experience tier level (refer to Section 921.01H), the (b) (7)(E) will assign DCFU personnel to the requesting case agent per (b) (7)(E) approval.

#### 921.01K Forensic Examination Standard Operating Procedures

1. Preservation of Digital Scene: (b) (7)(E)



2. Documentation of Scene and Digital Media: (b) (7)(E)



3. Transportation of Digital Media: (b) (7)(E)



(b) (7)(E) [Redacted]

4. Documentation of Storage: (b) (7)(E) [Redacted]

5. Forensic Examination: (b) (7)(E) [Redacted]

6. Forensic Examination Report. (b) (7)(E) [Redacted]

7. Forensic Media Archiving: (b) (7)(E) [Redacted]

8. Quality Assurance Review: (b) (7)(E) [Redacted]

#### 921.01L Forensic Documentation Requirements

As part of the DCFU's reporting duties, he/she will create a work file for each assigned task. The file should contain the following at a minimum:

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

### 921.01M Forensic Reporting Requirements

In accordance with CIGIE guidelines, the forensic report will, at a minimum, contain the following elements:

1. Identity of reporting organization
2. Case number
3. Identity of submitter
4. Relevant dates of forensics work to include the date of report.
5. Descriptive list of the evidence examined
6. Examination requested
7. Description of examination
8. Name and signature of examiner
9. Results, conclusions and derived items

(b) (7)(E)

### 921.01N Quality Management

Digital forensic analyses may require DCFU personnel to apply a wide range of techniques to retrieve data, and frequently examiners must interpret data to offer an expert opinion on what that data means. This standard places on the organization the responsibility for ensuring OIG has the quality standards and procedures in place sufficient to provide confidence that the results of forensic examinations are of high quality. These opinions can affect the outcomes of investigations, prosecutions, or other remedies. It is therefore essential that quality reviews are performed regularly to ensure confidence in the integrity of the forensic work performed by DCFU personnel. The four reviews for quality assurance are: administrative review, technical review, validation testing, and review of quality system.

1. Administrative Review: All digital forensic analysis reports must be reviewed and approved by the (b) (7)(E) for consistency with agency policy and for editorial correctness.
2. Technical Review: At least 10 percent of final digital forensic examination reports must be technically reviewed by either the (b) (7)(E), or both. This peer review must be performed before the reports are published. The reviewer must ensure the following:
  - a. The report is clear and understandable.
  - b. The procedures performed were adequately documented and forensically sound.
  - c. The exam documentation was sufficiently detailed to enable reproduction of the results.

d. The interpretations and conclusions of the examiner were reasonable, supported by the examination documentation, and scientifically valid.

3. Validation Testing: Forensic tools used to acquire digital evidence should be validated to operate as intended and accurately acquire the data. The validation testing may be performed by the organization or other reputable entity (for example, another digital forensic laboratory). According to the SWGDE, tools, techniques and procedures that are in widespread use and accepted by the larger IT community are generally acknowledged as reliable and trustworthy. Consideration may be given to a generally accepted forensic tool, technique or procedure when determining its validity.

(b) (7)(E)

Validation Process: When conducting internal testing and validation of computer forensic hardware and/or software, the following process should be followed.

a (b) (7)(E)

d. Validation Reporting: In accordance with CIGIE standards, the validation testing report must be available if requested. Whoever performs the validation testing must document the test. The report should contain the following, at a minimum:

i. The requirements that were tested.

ii. The expected results.

iii. The actual results of the testing.

4. Review of Quality System: An in-house review of the quality management system should be performed once every three years to ensure the system is (1) functioning according to the DCFU program's needs, (2) meeting current industry quality standards established in the latest training classes (3) and meeting the quality needs of the OIG.

Effective Date 4/2/2018

## 922.00 SPECIALIZED INVESTIGATIVE TECHNIQUES

### 922.01 Purpose

This chapter provides the policy and procedures which govern the use of specialized investigative techniques used to gather evidence in OIG investigative cases.

### 922.02 (b) (7)(E) Information

#### 922.02A (b) (7)(E) Requests for (b) (7)(E) Information Other Than (b) (7)(E) Information

1. (b) (7)(E) Requests. (b) (7)(E) for use in investigations of federal criminal statutes (b) (7)(E). The (b) (7)(E) refers to such requests as (b) (7)(E) requests.

Pursuant to an (b) (7)(E) request, the (b) (7)(E) will provide only limited (b) (7)(E) information, i.e., information it has obtained other than that provided by the (b) (7)(E) or the (b) (7)(E) representative. (b) (7)(E)

Agents may refer to the (b) (7)(E) Manual, Part (b) (7)(E) (b) (7)(E) (b) (7)(E) for more information.

2. Coordination with JC. (b) (7)(E) must be submitted through JC for review and concurrence. Once JC determines that a request meets the legal sufficiency standards set forth in (b) (7)(E) JC will prepare, for the (b) (7)(E) signature, a letter to the (b) (7)(E). In addition to including the information required by (b) (7)(E) the letter shall specify that the (b) (7)(E) provide the information directly to the agent who generated the initiating request.

The (b) (7)(E) requires that agencies in receipt of (b) (7)(E) information track (b) (7)(E). For this purpose, the OIG SAs must report in writing to JC all disclosures made to DOJ trial attorneys or Assistant United States Attorneys in the course of prosecution discussions (b) (7)(E). Due to strict (b) (7)(E), SAs should not provide copies of the (b) (7)(E) information itself to JC.

Agents may refer to the OIG Manual Section (b) (7)(E) Information for more information regarding coordination with JC.

3. Return of (b) (7)(E) Information. When the (b) (7)(E) information is no longer needed for the criminal investigation, it must be (b) (7)(E) with a cover letter. A copy of the cover letter must be forwarded to JC.

#### 922.02B Ex Parte Requests for (b) (7)(E) Information

Agents seeking (b) (7)(E) information should coordinate with the U.S. Attorney's Office and the (b) (7)(E)

#### 922.02C Requests for (b) (7)(E) Information

If an OIG investigation involves a (b) (7)(E), then the SA can request the entity's (b) (7)(E) information using (b) (7)(E)

#### 922.03 Obtaining (b) (7)(E) Information

##### 922.03A Obtaining (b) (7)(E)

(b) (7)(E) (b) (7)(E) to recognized law enforcement agencies. Requests for this data must: (1) be in writing; (2) be signed by (b) (7)(E) directed to the (b) (7)(E) of the particular area; and (3) state that the information is necessary for law enforcement purposes.

(b) (7)(E)

##### 922.03B Obtaining (b) (7)(E)

(b) (7)(E)

Such disclosure can be made verbally, by letter, or by providing copies of (b) (7)(E)

(b) (7)(E)

Requests for (b) (7)(E) information are made in accordance with the following procedures:

1. Where possible, the request is made in person by the SA. When submitted in writing, (b) (7)(E)

2. The request is directed to the (b) (7)(E) of the particular area.

3. The request includes a statement either that: (b) (7)(E)

4. If the request involves (b) (7)(E)

922.03C Obtaining (b) (7)(E)

1. Definition, Purpose, and Legal Basis for (b) (7)(E). (b) (7)(E)

(b) (7)(E), to obtain information in order to:

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E) Regulations, which constitute (b) (7)(E) (b) (7)(E) are set forth in: Title (b) (7)(E) Code of Federal Regulations, Part (b) (7)(E) Section (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

2. OIG Policy on (b) (7)(E). OIG policy on (b) (7)(E) is as follows:

(b) (7)(E)

(b) (7)(E)

3. Obtaining (b) (7)(E) Information. Requests for (b) (7)(E) are (1) made in writing by completing the (b) (7)(E) Template (Figure 922-01) accompanied by a cover letter (b) (7)(E); (2) usually targeted to a stated individual or concern at a given address; and (3) limited to not more than a (b) (7)(E) period.

SAs should contact the (b) (7)(E) at (b) (7)(E) for additional information regarding (b) (7)(E) requests, to obtain (b) (7)(E) Procedures for (b) (7)(E) Requests, or to obtain an electronic version of the (b) (7)(E) template.

4. Canceling and Renewing Requests for (b) (7)(E). Requests for (b) (7)(E) are cancelled if the information sought (b) (7)(E). Cancellation notices are sent by the (b) (7)(E) to the (b) (7)(E).

Requests for (b) (7)(E) may be renewed by using the same procedures as for an original request.

5. Reproducing and Returning (b) (7)(E) Information. (b) (7)(E) documents are the property of the (b) (7)(E) and are loaned with the understanding they will be treated confidentially. (b) (7)(E).

All (b) (7)(E) Forms (b) (7)(E) (b) (7)(E), must be returned within (b) (7)(E) to the (b) (7)(E) official from whom they were received.

922.04 (b) (7)(E)

(b) (7)(E)

Procedures for arranging (b) (7)(E) are as follows:

1. (b) (7)(E) submits a request for use of the (b) (7)(E) to (b) (7)(E). The request includes the case number, case title, and a brief explanation of the purpose of the (b) (7)(E), including the name of the person to be (b) (7)(E) and whether the person requested the (b) (7)(E).
2. If (b) (7)(E) concurs with the request, (b) (7)(E) arranges for a (b) (7)(E).

922.05 Questioned Documents

922.05A Definition of Questioned Documents

A questioned document is a document whose authenticity, identity, or origin has been questioned in whole or in part. Verification of the document's authenticity, identity, or origin may involve a comparison of handwriting, printing, or typewriting samples, a determination of the age of the document or the ink, or an examination of erasures, obliterations, or overwriting.

922.05B Standards for Comparison with Questioned Documents

In order that a determination can be made on a questioned document's authenticity, identity, origin, or relationship to some matter, the SA submits (b) (7)(E)

(b) (7)(E) Each such sample is called an exemplar and collectively the exemplars constitute standards for comparison.

These standards for comparison are admissible in court, based on 28 U.S.C. 1731, which provides that:

"The admitted or proved handwriting of any person shall be admissible, for purposes of comparison, to determine genuineness of other handwriting attributed to such person."

Although this statute specifically addresses only standards of comparison for handwriting, it is understood to apply equally to standards of comparison for typewriting.

(b) (7)(E)

#### 922.05C Obtaining Handwriting Exemplars

1. Types of Handwriting Exemplars. When a SA becomes aware that the authenticity or origin of a document may be questioned, he/she attempts to obtain handwriting exemplars of the parties whose handwriting appears on the document. Handwriting exemplars may consist of:

a. Previous writing that the subject has either admitted to creating or that the government can prove was created by the subject; and/or

b. (b) (7)(E) The taking of handwriting exemplars does not violate a person's constitutional rights. The Fifth Amendment privilege against self-incrimination applies to compulsory communications, while a handwriting exemplar (in contrast with the content of what is written) is an identifying physical characteristic that falls outside the protection of the Fifth Amendment. See *Gilbert v. California*, 388 U.S. 263 (1967). A person can be cited for contempt if he/she refuses to provide an exemplar to a grand jury.

2. Standards and Techniques Relating to Handwriting Exemplars. Standards and techniques relating to obtaining handwriting exemplars will be determined through discussions with the SA, prosecutor, and the lab/expert witness.

The SA (b) (7)(E)

#### 922.05D Using Questioned Document Examiners and Examination Facilities

1. Functions and Use of Questioned Document Examiners. (b) (7)(E)

A questioned document examiner makes examinations and analyses of documents to:

a. (b) (7)(E)

(b) (7)(E)

Questioned document examiners prepare reports on their observations and conclusions, and also testify in court as expert witnesses.

2. Arranging for Questioned Document Examiner Services. The following standards and procedures apply when making arrangements for questioned document examiner services:

a. (b) (7)(E)

b. If the questioned document examiner (b) (7)(E)

c. The questioned documents and the related exemplars are transmitted to the questioned document examiner facility in accordance with procedures stipulated by that facility. When the facility does not stipulate transmittal procedures, the following transmittal guidelines apply:

(b) (7)(E)

#### 922.06 Title III or Electronic Surveillance Requiring a Warrant or Court Order

Court-authorized interceptions of wire, oral, or electronic communications are among the most intrusive investigative techniques currently available to law enforcement. The rigors of the approval process, expenditures of financial and human capital resources, and the probability of challenges by the defense make this technique subject to intense scrutiny. Surreptitious electronic surveillance using closed-circuit television presents similar considerations. Accordingly, any investigation involving the interception of communications pursuant to 18 U.S.C. § 2510, et seq., electronic surveillance using closed-circuit television in situations where a warrant is required, or any other court ordered electronic surveillance, shall be conducted (b) (7)(E)

. Subsequent to such notification, (b) (7)(E) may choose to join the investigation, but is not required to do so. However, in all instances in which the OIG intends to engage in court authorized electronic surveillance without the participation of (b) (7)(E), one of the following federal investigative agencies must participate in the investigation and supervise the application for and use of the surreptitious electronic surveillance. (b) (7)(E)

(b) (7)(E)

#### 922.06A Title III Interception of Communications

Title III is a reference to 18 U. S. C. § 2510, et seq, and prohibits the warrantless non-consensual interception of wire or electronic communications and the warrantless non-consensual use of devices to intercept oral communications in which one or more participants has a reasonable expectation of privacy. A Title III Court Order must be obtained to lawfully intercept one of these communications.

To intercept wire or oral communications, the SA must have probable cause that one of the predicate offenses listed in 18 U.S.C. § 2516 (1) is being committed. The application for the Title III court order must be reviewed and approved by the United States Attorney for the district where the intercept will occur. Final approval for the application must come from the appropriate Department of Justice official designated by the United States Attorney General. These approvals are required before the application is presented to a Judge.

To intercept electronic communications, the SA must have probable cause that any federal felony is being committed. The application must be approved by the AUSA for the Criminal Division before it is presented to a Judge where the intercept or electronic communications is over other devices, such as computers or facsimile machines.

#### Contents of the Application

Each application for a Title III court order must contain specific information before a court may authorize interception. The application must contain the following information:

1. Identity of the law enforcement officer making the application and DOJ official who authorized it.
2. Statement of facts and circumstances relied on to justify the applicants belief that a Title III court order should be issued.
3. Necessity statement as to whether other investigative procedures have been tried and failed or why they would reasonably appear to be unlikely to succeed if tried or would be too dangerous.
4. Time period for which the interception will be maintained.
5. Statement regarding any previous applications for a Title III court order.
6. The application must have a statement that the surveillance will be "conducted in a way as to minimize the interception of communications not otherwise subject to interception."

#### 922.06B Electronic Tracking Devices

Electronic tracking devices serve an important function for law enforcement by allowing agents to track the movement of a person or an object. (b) (7)(E)

, the installation and monitoring of a tracking device is regulated

by the Fourth Amendment. In most cases, when the OIG does not have the consent of the person or owner of the object to be tracked, a search warrant authorizing installation and use of a tracking device is required. Agents must consult with the AUSA in determining if a search warrant is required before installing or using an electronic tracking device.

1. Search Warrant Required. A Fourth Amendment Search is triggered when there is a government intrusion of a constitutionally protected area—an area where an individual has a reasonable expectation of privacy. In the context of electronic tracking devices, the government's installation and use of an electronic tracking device can constitute a Fourth Amendment search. For example, the Supreme Court has held that installing a GPS tracker to an individual's vehicle and then using the GPS to monitor the vehicle's movements was a Fourth Amendment search. See *United States v. Jones*, 565 U.S. 400 (2012). If an individual has a reasonable expectation of privacy in the area in which a tracking device is installed and/or used, a search warrant is required. Thus, it is essential that the SA consult with the AUSA for approval to use any tracking device and to determine any changes or new requirements before using a tracking device.

The warrant to install and monitor tracking devices (Rule 41 of the Federal Rules of Criminal Procedure) must contain the following:

- a. Identity of person or property to be tracked.
- b. Identity of the magistrate judge to whom the return will be made.
- c. A reasonable period of time that the device will be used.
- d. A command that the device will be installed within 10 days from the time the warrant is issued and during the daytime, unless good cause can be shown for another time.
- e. A command that there shall be a return on the warrant.

2. Consensual Use of Electronic Tracking Devices. When the owner of the object has given permission for the installation of an electronic tracking device, a warrant might not be required. Nevertheless, the SA must still consult with the AUSA for approval before using a tracking device.

(b) (7)(E)

3. No Search Warrant Required. In rare circumstances there may be situations where a reasonable expectation of privacy does not exist. For instance, there may be a situation where a subject does not have a reasonable expectation of privacy in a motor pool GOV (note, however, that every situation will depend on the facts). If the AUSA determines that a search warrant is not required, then the agent will get approval to use a tracker from the agent's (b) (7)(E) or (b) (7)(E). Absent a search warrant, the SA will prepare a memorandum to the (b) (7)(E) outlining the proposed use of an electronic tracking device. This memorandum must include the following information:

(b) (7)(E)

(b) (7)(E)

#### 922.06C Pen Registers and Trap and Trace Devices

SAs should be aware that pen registers and trap and trace devices are not regulated by Title III. The use of such devices is subject to the provisions of Title 18 USC §§ 3121 -3127. The general rule provides that no person may install or use a pen register or trap and trace device without first obtaining a warrant under section 3123. The application must be made by an "attorney for the government"; therefore, agents should coordinate with the assigned AUSA in order to use a pen register or a trap and trace device.

#### 922.06D Cell Phone Tracking

When a SA considers cell phone tracking, the SA should consult with the AUSA on the investigation. The SA should consider that the courts are generally divided into two views about what authority is required in order for the government to obtain real and prospective cell site information. The majority view is that probable cause and a Rule 41 warrant are required in order to compel the cell phone service provider to disclose real time and prospective data. A minority of courts have allowed the government to use its pen register/trap and trace authority to obtain single cell site information in real time. The courts have consistently required the government to have a search warrant in order to obtain multiple cell site triangulation information from cell phone service providers. SAs should consult with the AUSA regarding obtaining cell phone tracking data.

#### 922.06E Video-Only Surveillance

When a SA considers using video-only surveillance, the SA should be aware that the use of video-only surveillance to record an area where a reasonable expectation of privacy exists is governed by the Fourth Amendment, not Title III. The controlling factor regarding the use of video-only surveillance is whether or not those present in an area, where the activity will be recorded, have a reasonable expectation of privacy. A search warrant will be required when video-only surveillance will be used to record an activity in an area where a reasonable expectation of privacy exists. DOJ requires an investigative agency to receive approval from the DOJ prior to seeking to use court-ordered video surveillance.

922.07 Surveillances

922.07A Definition of and Reasons for Surveillances

Surveillance is the physical observation of an individual or group of individuals. Generally, surveillances are used to:

- (b) (7)(E)
- 
- 
- 
- 
- 
- 
- 
- 
- 

922.07B OIG Policy on Surveillances

The conduct and supervision of surveillance activity is a field office responsibility. All surveillance must be authorized by (b) (7)(E) and documented. All surveillance decisions, including assignment of SAs, methods, and documentation, are made by (b) (7)(E) in accordance with applicable laws.

Effective Date 2/24/2017

## 924.00 GOVERNMENT OWNED VEHICLES

### 924.01 Purpose

This directive establishes the U.S. General Services Administration, Office of Inspector General (GSA-OIG), policy and procedures concerning Government Owned Vehicles (GOVs), which are those vehicles acquired by GSA-OIG through lease, purchase, or transfer from another agency.

### 924.02 Policy

GOVs will be assigned to investigative offices at the discretion of (b) (7)(E) based on the needs of each office. The (b) (7)(E) will assign office personnel the responsibility for maintaining specific vehicles and preparing required vehicle reports.

### 924.03 Administrative Requirements

#### 924.03A Registration

GOVs used for investigative fieldwork will be properly registered with a state Department of Motor Vehicles and will obtain a license plate from the state of registration. At the discretion of the SA, a Government license plate may be displayed (e.g., on the dashboard) to facilitate parking. (b) (7)(E)

The investigative office will maintain a copy of all registration documents. Each vehicle will be properly registered (b) (7)(E)

All required inspection requirements for the state of registration shall be in compliance. GSA leased vehicles will be registered and inspected in accordance with instructions from GSA Fleet Management Centers.

#### 924.03B Tolls

If tolls are frequently used, SAC's should obtain revenue toll passes (e.g., EZPass) for each GOV from the state (b) (7)(E). If revenue passes are not available, all tolls incurred during official use shall be reimbursed by GSA OIG.

#### 924.03C Assignments

(b) (7)(E) are responsible for vehicle assignments. Continuing assignment of GOVs during normal duty hours is essential based on the responsibility inherent in criminal investigator positions and the fact that immediate use of transportation is absolutely essential to the accomplishment of the GSA OIG mission.

(b) (7)(E) will ensure that the authorized size of their assigned vehicle fleet is appropriate for the number of employees. (b) (7)(E) will report any necessary fleet reductions or increases to headquarters. If the number of employees is more than the number of vehicles available, (b) (7)(E) will ensure that all employees have access to a vehicle to conduct their duties.

#### 924.03D Motor Vehicle Control Officers

(b) (7)(E) shall appoint, in writing, the Motor Vehicle Control Officer for each location under their purview. The control officer will coordinate the necessary reports, repairs, and vehicle maintenance as necessary.

#### 924.03E Authorized Drivers and Reporting Requirements

1. Supervisors will ensure that only drivers with valid licenses will operate GOVs. Employees are responsible for reporting to their supervisor if their driver's license status has changed for any reason.
2. If at any time a supervisor becomes aware of any physical, medical, legal, or other condition that might adversely affect an employee's ability to operate a motor vehicle, the supervisor will suspend the employee's privilege to operate a GOV and will notify (b) (7)(E) of the reasons for taking such action. (b) (7)(E) will make all final determinations for termination of an employee's privilege to operate a GOV.
3. Any employee who receives a citation for a traffic violation while operating any GOV, or receives a parking violation, must report the citation to their immediate supervisor and the Motor Vehicle Control Officer.
4. Any employee who is cited, arrested, or otherwise charged with driving under the influence of drugs or alcohol, or driving while intoxicated while operating a GOV, must immediately report such action in writing to their (b) (7)(E). (b) (7)(E) will provide written notification to (b) (7)(E) as soon as possible.

#### 924.04 Use of GOVs

##### 924.04A Authority

Federal statute (31 U.S.C. § 1344), Federal regulations (41 C.F.R. Parts 102-5 and 102-34), and GSA directive (ADM P 5620.1, dated September 12, 2005) require that the use of all government owned or leased motor vehicles be restricted to "official purposes" (as defined in section 924.04C of this subchapter) only. Use of government owned, leased, or rented vehicles in a matter for a purpose other than specified in law, regulation, or this directive is prohibited.

##### 924.04B Adverse Personnel Action

Pursuant to 31 U.S.C. § 1349(b), an officer or employee of the US government who willfully uses or authorizes the use of a GOV (except for an official purpose authorized by 31 U.S.C. § 1344) or otherwise

violates 31 U.S.C. § 1344 shall be suspended without pay for (b) (7)(E). If the circumstances warrant, the employee may be suspended for a longer period of time or summarily dismissed from federal service.

#### 924.04C Official Purposes

1. Official Use. GSA OIG personnel shall use GOVs for official purposes only. An official purpose is considered to be a use directly related to the fulfillment of the mission of GSA OIG. This use includes, but is not necessarily limited to, all investigative related matters, as well as official conferences and meetings, training, business, to and from physical fitness training, or approved home-to-work (HTW) (discussed and defined below) transportation.

2. Limitations on Use. Except for minor personal use, GOVs shall not be used for personal matters, recreation, or personal transportation. Minor personal use such as a brief stop while in route between duty assignments or during HTW travel (as provided below) is authorized. Use of a GOV is also authorized for meal breaks from the office or site of official business. Agents are expected to use good judgement, and GOV use is at the discretion of (b) (7)(E).

3. Official Temporary Duty (TDY). GOVs may be used during TDY assignments, and may be used to obtain goods or services necessary to the health and well-being of the employee. This includes, but is not limited to, travel in a GOV to obtain medical services, attend religious services, and to obtain goods and services at restaurants, barbershops, beauty shops, drugstores, laundries, and dry-cleaning establishments.

#### 924.04D Parking

Vehicles normally will be parked in a secure area (b) (7)(E). Personnel incur the responsibility for ensuring that the vehicle is locked and parked in a secure area. Parking vehicles on (b) (7)(E) is generally considered secure. If available, (b) (7)(E) shall obtain local police parking permits ("placards") for every GOV, and such permits shall only be used as directed by the issuing agency.

When SAs park government vehicles overnight or for extended periods of time, accountable and/or law enforcement sensitive government property of value shall be removed from the vehicle. SAs can be held liable for the cost of any items not properly secured. (b) (7)(E)

#### 924.04E Consumption of Alcoholic Beverages and Use of Narcotics and Medications

OIG personnel are prohibited from consuming alcohol and shall not be under the influence of alcoholic beverages while operating a GOV. (b) (7)(E)

Except in cases where a drug has been prescribed by a physician, and would not cause impairment, OIG personnel are prohibited from

operating a GOV while under the influence of any narcotic, including marijuana and other drugs. Furthermore, OIG personnel should refrain from using any medication that could cause drowsiness or dizziness when operating a GOV.

#### 924.04F Storage

Employees will ensure that unattended vehicles are properly secured and locked. Portable radios, technical equipment, cameras, and similar sensitive or costly equipment, will not routinely be stored in GOVs. (b) (7)(E). Firearms, long guns, evidence, or official funds should not be placed in any unattended vehicle, except under exigent circumstances and approved by (b) (7)(E). In such situations, these items should be placed in (b) (7)(E)

#### 924.04G Home-to-Work (HTW) Transportation

1. Authority. 31 U.S.C. § 1344, as implemented in 41 C.F.R. Part 102-5 and GSA Order ADM P 5620.1, authorizes the use of HTW transportation by employees serving in positions essential to the safe and efficient performance of intelligence, counterintelligence, protective services, or criminal law enforcement duties. A one-time-only written request is required for the approval of the Administrator. GSA OIG received such approval (Authorization Memorandum (Nov. 30, 1988) Figure 924-01).
2. Applicability. The nature of the work of a SA, including SAC and ASAC, requires the ability to respond in a safe and timely manner 24 hours a day to conduct law enforcement activities. Accordingly, the use of GOVs is considered to be for official government business when driving from home to work and shall be deemed within the scope of official government duty. However, time during which the employee-operator uses HTW transportation shall not be considered when calculating core-duty hours nor LEAP hours for that individual.
3. Policy. When called upon to conduct a law enforcement activity, each SA should have access to an assigned GOV. SAs are expected to respond to calls (b) (7)(E). Use of GOV for transportation of SAs between their residence and place of employment is essential for the safe and efficient performance of criminal law enforcement duties by investigative personnel.
4. Definitions. The following definitions apply:  
"Home" means the primary place where an employee resides and from which the employee commutes to their place of work. "Work" means any place within the accepted commuting area, as determined by GSA OIG for the locality involved, where an employee performs his or her official duties, including official work requiring the employee's presence at various locations, other than their regular place of work, such as official conferences and meetings, training, liaison, business, to and from physical fitness training during duty hours, etc... "Home-to-work" means home-to-work and work-to-home transportation.

5. HTW Transportation Procedure. All GSA OIG GOV operators must remain aware of the policies governing HTW transportation authority and acknowledge such through certification.

(Figure 924-02).

#### 924.04H Firearms

In addition to the policies and procedures relating to firearms provided by Section 902 of this manual, all SAs shall (b) (7)(E), and any other necessary law enforcement equipment when operating a GOV and traveling HTW, unless the agent is engaged in an approved operation where (b) (7)(E) or a waiver has been issued by (b) (7)(E).

#### 924.04I Transporting Others

1. Non-GSA OIG Personnel. SAs may transport persons who are not employed by GSA OIG only under the following conditions:

- To transport employees of other federal agencies and non-federal employees conducting official business when it benefits the government;
- To transport persons in emergency or disaster situations while assisting persons with injuries or in pain, and preventing death or serious damage to persons or property;
- GOVs may be operated by a non-GSA OIG employee only as part of a specific law enforcement-related event. Any use of a GOV by a non-GSA OIG employee requires the approval of the (b) (7)(E) or, when anticipated in advance by (b) (7)(E);
- The use of GSA OIG controlled vehicles by informants is generally prohibited unless (b) (7)(E) first approves the use or in a bona fide emergency;
- Other non-federal law enforcement officers may operate GSA OIG controlled vehicles when such use is in direct support of the GSA OIG mission and is approved by the GSA OIG (b) (7)(E) or used in bona-fide emergency situations without prior approvals. All instances of emergency use without prior approval will be reported after the fact to the (b) (7)(E) or
- Student interns may be transported in GOVs, but may not operate them.

2. Family Members. No GSA OIG employee shall transport family members, friends, or other persons, who are not conducting official business in a GOV (except as provided above) unless approval is obtained from their (b) (7)(E)

#### 924.04J Use of Other Federal Agency's GOVs

GSA OIG SAs can operate another federal agency's GOVs within the guidelines of that particular agency. Agents should familiarize themselves with the rules and regulations of that agency before driving the vehicle.

#### 924.04K Vehicle Stops

(b) (7)(E) it may be necessary to stop a vehicle in connection with exigent investigative circumstances (e.g., the arrest of a fugitive felon). Generally, in cases prior to executing a vehicle stop, SAs should attempt to obtain assistance from (b) (7)(E). GSA OIG directives detailing arrest procedures should be followed when planning an arrest and executing an arrest warrant. (b) (7)(E)

#### 924.04L Pursuits

(b) (7)(E)

(b) (7)(E)

Upon termination of such situation, the agent shall immediately notify their (b) (7)(E) of the situation.

#### 924.04M Use of Emergency Response Equipment

Emergency response equipment may be used only during emergencies when quick response is essential, and it may not be used for non-emergencies such as to avoid traffic congestion.

Emergency lights may be used at the discretion of the agent operating the vehicle when it is deemed necessary to identify the vehicle as a law enforcement vehicle or to ensure the safety of agents or the public.

#### 924.04N Operating Safety

1. Traffic Laws. All GOV operators are expected to operate motor vehicles in a defensive manner and obey all traffic laws and regulations. The safety of the public and the employee has higher priority than

any "official purposes" or enforcement activity. Traffic and parking laws will not be violated, except in extraordinary circumstances

2. Seatbelts. For personal safety, all occupants of GOVs (b) (7)(E) have their seatbelts fastened whenever the vehicle is in motion. It is the responsibility of every GOV operator to ensure that all occupants fasten their seatbelts.

3. Vehicle Equipment. Each GOV will be equipped with at least the following items:

- Spare tire (if applicable);
- Jack and lug wrench;
- Dry-type fire extinguisher;
- Flares or equivalent safety equipment;
- First Aid kit;
- Flashlight;
- Emergency equipment or materials necessary for the climate in which the vehicle is operated, such as, snow shovels and tire chains in frigid climates, and emergency water in desert areas;
- Battery jumper cables; and
- Accident forms (e.g., SF-91 & SF-94)

4. Cellular Phone Use. GOV operators should become aware of state/local requirements concerning the use of cellular phones while driving. In many areas, it is illegal to talk on a cellular phone while driving without a hands free device. Unless it is an emergency, talking on the cellular phone while driving is discouraged. The use of hands free cellular phone equipment in GOVs is encouraged.

Pursuant to Executive Order 13513, "FEDERAL LEADERSHIP ON REDUCING TEXT MESSAGING WHILE DRIVING", GOV operators shall "not engage in text messaging (a) when driving GOV, or when driving POV while on official Government business, or (b) when using electronic equipment supplied by the Government while driving."

#### 924.05 Maintenance, Repairs, and Services

Supervisors will ensure that all GSA OIG vehicles are maintained and used uniformly. Vehicles must be washed when necessary. Additionally, car windows should be cleaned and window-washing fluids replenished when necessary to ensure visibility. The GSA vehicle credit card can be used for payment of these services.

Maintenance of GOVs shall be performed in accordance with GSA instructions. All charges for routine maintenance (e.g., oil changes, tire repairs, etc.) shall be paid using the vehicle credit card (b) (7)(E) [REDACTED]. Emergency services or repairs should only be made after consulting with GSA fleet management services.

#### 924.06 Administrative Control of Credit Cards/ Government License Plates

Accountability of GSA vehicle credit cards/plates will be strictly maintained by each GOV operator to avoid loss and preclude the occurrence of unauthorized charges. (b) (7)(E) and GSA Fleet will promptly be notified of all lost or stolen GSA credit cards/plates.

#### 924.07 Cash Purchases in Lieu of Credit Cards

Cash purchases of gasoline and emergency repairs in lieu of GSA credit card purchases will only be made in emergency situations, for example, a location where a vendor refuses to honor a government credit card or in instances where the use of a government credit card may compromise an investigation.

#### 924.08 Accidents and Damage to Vehicles

##### 924.08A Theft and Vandalism

Vandalism to, theft of, or damage of GOVs will be reported immediately to (b) (7)(E) and documented in a detailed memorandum. (b) (7)(E) will notify (b) (7)(E) (and GSA for leased GOVs), as well as (b) (7)(E) [REDACTED]. A written report is required within (b) (7)(E) of the incident. A copy of this report will be provided to (b) (7)(E). At the discretion of (b) (7)(E), or (b) (7)(E), an investigation may be initiated to determine the circumstances surrounding the incident. A finding of negligence on the part of the employee may result in disciplinary action.

##### 924.08B Accidents

1. Procedures. The operator of the vehicle owned, leased, rented, or borrowed for official use by GSA OIG, that is damaged or involved in an accident, will follow the procedures listed below. If the operator, due to injury, cannot perform these listed tasks, the senior agent at the scene will perform them.

- Ensure that injured persons are attended.

(b) (7)(E) [REDACTED].

- If possible, try to ensure that the vehicle(s) does not create a hazard.
- Notify a supervisor.
- Notify GSA Accident Management Center (b) (7)(E) [REDACTED]
- Avoid discussions with or making statements to any witnesses or other parties to the accident regarding the cause or fault.
- The vehicle operator shall obtain and record information pertaining to the accident on Standard Form (SF) 91, Operator's Report of Motor Vehicle Accident Report. The SF 91 should be furnished to the vehicle operator's (b) (7)(E) [REDACTED] within (b) (7)(E) of the accident. The vehicle operator shall also obtain the names, addresses, and telephone numbers of any witnesses and whenever possible, have witnesses complete

Standard Form 94, Statement of Witness, and submit the completed SF 94 and other related information to (b) (7)(E).

2. Reporting Requirement. All accidents or damage involving GOVs will be reported promptly to the operator's (b) (7)(E). (b) (7)(E) will promptly notify (b) (7)(E). Copies of all accident reports will be provided to (b) (7)(E), who will forward them to (b) (7)(E).

Notification will be immediate if any of the following conditions exist:

- Serious personal injury or death;
- An arrest, traffic citation, or detention of GSA OIG operator;
- Any indication or allegation that GSA OIG operator was operating the vehicle under the influence of alcohol or drugs, left the scene of the accident, or was operating the vehicle outside the scope of employment; and/or
- Where there is a recognized potential for adverse publicity.

#### 924.08C Injury to a Third Party or Damage to a Third Party's Property

With respect to damages caused to a third party as a result of the operation of a vehicle by an OIG employee, who was determined not to be acting within the scope of their employment at the time of the accident or incident, the employee could be personally liable to the third party for any resulting damage or personal injury.

Effective Date 2/13/2014

## 925.00 EVIDENCE

### 925.01 Law of Evidence

In order to develop cases that will withstand legal scrutiny, Special Agents (SAs) need to be thoroughly familiar with the Federal guidelines concerning evidence. Because these Rules are subject to continuing change:(1) they are not summarized in this Manual; and (2) SAs must be careful and refer only to the most current version.

#### REFERENCES:

The following Federal guidelines govern the admissibility of evidence in Court:

Title 28, U.S.C., Federal Rules of Evidence (FRE)

Title 18, U.S.C., Federal Rules of Criminal Procedure

Title 28, U.S.C., Federal Rules of Civil Procedure

### 925.02 Evidence Determination

Evidence is the material from which inferences may be drawn as the basis for proof of the truth or falsity of a fact in issue. It is all the means by which any alleged matter of fact, the truth of which is submitted to investigation, is established or disproved. Evidence is testimony, writings, material objects, or other things presented to the senses that are offered to prove the existence or nonexistence of a fact.

Evidence is any item that is seized, collected or surrendered to OIG Special Agents and that is deemed to be of evidentiary value in a potential prosecution in establishing the elements of an offense, or the truth of the matter being investigated. To be admissible evidence must be relevant and legally obtained.

Standards for identification of evidence are as follows:

- The unique nature of OIG investigations requires a practical policy and feasible procedures for identifying, securing and handling evidence. (b) (7)(E)

The SA must provide reasonable security for the property while an evidentiary determination is being made to avoid any challenge to the authenticity of the property.

- As soon as an item is determined to be evidence it must be documented on the Evidence Custody Form (Figure 925-01). Appropriate protections must be provided to ensure the physical security of and to establish controlled access to the item(s). The SA assigned to an investigation must ensure that the

receipt of any item into evidence is promptly and accurately documented and entered into the OIG Evidence room as soon as possible, in accordance with the procedures set forth in this chapter.

### 925.03 Receiving, Identifying, and Preserving Evidence

#### 925.03A Chain of Custody

Chain of custody means the preservation, in original condition, of the instrument of a crime or any relevant writing or other evidence, by the successive custodians of the evidence. Maintaining chain of custody is extremely important to show the evidence is in the same condition as when it was obtained.

The following paragraphs present OIG procedures designed to ensure that the chain of custody is fully maintained in receiving, identifying, and preserving evidence.

#### 925.03B Receiving, Identifying, and Tagging Records and Documents

A Receipt for Property (Figure 925-02 or equivalent) is issued in every instance when a SA removes records or documents, either by agreement or legal process other than grand jury subpoena, from the premises of a principal or witness. (b) (7)(E)

When such records or documents constitute evidence, the special agent: (b) (7)(E)

(Figure 925-01); (b) (7)(E)

(b) (7)(E)

It should be noted that, unless required by specific instructions and/or special circumstances, receipts are not issued for records and documents obtained through the mail. In such cases, the correspondence requesting and providing the records and documents is normally sufficient documentation. However, if documents and records obtained through the mail (b) (7)(E)

#### 925.03C Identifying and Tagging Seized Documentary Evidence

In order that a seized document may be admissible as evidence, the SA must prove that: (1) it is the same document that was seized; and (2) the document is in the same condition as when it was seized. Therefore, the SA identifies such documents as soon as they are seized.

Normally, the SA identifies the documents by (b) (7)(E)

the special agent: (b) (7)(E)

(b) (7)(E)

In order to maintain the chain of custody for such documents, (b) (7)(E)

#### 925.03D Identifying and Tagging Physical Evidence

Every piece of physical evidence must be (b) (7)(E) as soon as practicable. (b) (7)(E)

The SA then completes the (b) (7)(E)

#### 925.03E Preserving Documentary and Physical Evidence

The OIG preserves and controls documentary and physical evidence through a system involving (b) (7)(E)

1. (b) (7)(E). Each SA is responsible for ensuring the chain of custody and integrity of evidence collected during his/her assigned investigations. (b) (7)(E)

2. (b) (7)(E)

(b) (7)(E)

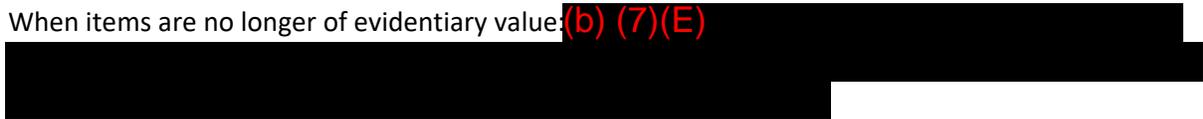
3. (b) (7)(E) As indicated above, the case agents (b) (7)(E)

(b) (7)(E)



#### 925.04F Disposition of Evidence

When items are no longer of evidentiary value: (b) (7)(E)



When the evidentiary items are dangerous drugs, the SA consults the Drug Enforcement Administration about the disposition of the drugs. (b) (7)(E)



Under no circumstances are JI employees permitted to take possession of or use evidentiary items for personal purposes.

#### 925.04 Grand Jury Evidence

Rule 6(e) of the Federal Rules of Criminal Procedure imposes strict obligations on SAs who are duly appointed agents of the grand jury to protect the secrecy of matters occurring before the grand jury. SAs who are working with grand jury materials are responsible for ensuring their confidentiality. SAs handling grand jury materials shall not disclose their content to any third party unless the SA is certain that the disclosure meets applicable legal standards. Whenever disclosure issues arise, the SA must seek clearance from the appropriate prosecuting attorney. SAs must seek the advice from the appropriate prosecuting attorney before disclosing grand jury material to anyone, including a civil government attorney. Refer to Section 910 for further information on handling and storing grand jury material.

Effective Date 2/13/2014

926.00 (b) (7)(E)

#### 926.01 Purpose

This chapter will provide the policy and procedures which govern the use of information and data obtained through the (b) (7)(E).

926.02 (b) (7)(E)

(b) (7)(E) compiles and maintains documented police information for use only by duly authorized law enforcement agencies. Office of Inspector General (OIG) Special Agents (SAs) are authorized access to (b) (7)(E) data only in connection with official OIG investigations.

Procedures relating to use of (b) (7)(E) data are as follows:

- (b) (7)(E): Access to (b) (7)(E) data is controlled by an (b) (7)(E). The (b) (7)(E) assigned to Office of Investigations (JI) is (b) (7)(E).
- Data Entries and Queries: Entries to and queries of the (b) (7)(E) are normally made through the (b) (7)(E). When appropriate, entries and queries may also be made through (b) (7)(E).

926.03 Use of (b) (7)(E) Information

(b) (7)(E)

Any employee who purposely requests or uses such (b) (7)(E) information for improper purposes, including the unauthorized dissemination of such information, may be subject to disciplinary action up to and including termination (see section on discipline below).

#### 926.03A Responsibility

The OIG (b) (7)(E)

(b) (7)(E) is responsible for ensuring that: (1) the policies for the use of (b) (7)(E) information are in place and all employees are aware of the responsibilities; (2) the system is operating according to applicable procedures; and (3) adequate records are maintained to document requests for information.

Employees who request (b) (7)(E) information must be authorized to do so and must ensure their requests are for authorized purposes. As part of this responsibility, the (b) (7)(E) will ensure that all employees who come into contact with (b) (7)(E) information are appropriately screened, trained, and supervised to ensure compliance with this policy and the applicable requirements.

#### 926.03B Controls

The OIG (b) (7)(E) will ensure the OIG complies with security controls in the (b) (7)(E) Security Policy. Controls to be followed within the OIG include the following:

- 1) The individuals who install and maintain the equipment and programs needed to access (b) (7)(E) data must be (b) (7)(E) of employment.
- 2) All personnel in contact with (b) (7)(E) information will have appropriate background investigations, including an FBI review (b) (7)(E). Anyone with a felony conviction will not be granted access to (b) (7)(E) information.
- 3) All telecommunications equipment, computers, and programs used to access (b) (7)(E) information will be safeguarded and (b) (7)(E). The (b) (7)(E) is responsible for ensuring that physical, administrative, and technical security complies with the (b) (7)(E) Security Policy.
- 4) All OIG employees authorized access to (b) (7)(E) information will be responsible for safeguarding it and ensuring its proper disposition as defined in the (b) (7)(E) Security Policy.

#### 926.03C Requests for Information

All requests for computerized (b) (7)(E) information, including (b) (7)(E) inquiries, must be accompanied by a file number or other tracking number (b) (7)(E).

#### 926.03D Guidelines on the Dissemination of (b) (7)(E) Information Obtained From Computerized System

Dissemination of information obtained through these computerized systems is strictly controlled. Information about a particular individual may be subject to Privacy Act restrictions and Department of Justice (DOJ) regulations. OIG agents should be sensitive to the privacy interests that may be adversely affected if (b) (7)(E) information that is not generally available to the public is improperly disclosed. OIG employees are responsible for notifying the OIG (b) (7)(E) whenever they release outside the OIG any computer-derived (b) (7)(E) information.

- Before (b) (7)(E) information is disseminated (b) (7)(E), the agent disseminating the information must ensure: (b) (7)(E)

(b) (7)(E) except to the extent necessary during an OIG criminal investigation or with the approval of the (b) (7)(E).

(b) (7)(E) information shall not be disseminated (b) (7)(E) in connection with employment-related inquiries.

(b) (7)(E) information shall not be disseminated (b) (7)(E) unless they are expressly authorized to receive such information (e.g., in connection with background investigations for criminal justice positions or criminal investigations conducted by the agency receiving the information).

- Information from (b) (7)(E)

### 926.03E Standards of Discipline

OIG personnel are responsible for following this policy and (b) (7)(E) operators are also responsible for following the (b) (7)(E) policies which are set forth in the (b) (7)(E) operating manual, including any updates issued by the (b) (7)(E). Any questions should be raised to the (b) (7)(E) before making an entry or inquiry.

1. System misuse. Misuse of this system will include, but not be limited to the following:

- (b) (7)(E)

2. Disciplinary actions. Misuse will result in disciplinary action; the nature of the action will depend on the circumstances, and may include termination. Additionally, misuse of the system may result in criminal charges.

### 926.03F Dissemination of (b) (7)(E) Information Obtained From Other Sources

(b) (7)(E) information obtained from other sources is not subject to the above rules. For example, the following types of information generally may be disclosed outside the OIG as long as Privacy Act requirements are met.

- Information obtained from court records or which is otherwise a matter of public record, including conviction and conviction-related data from court records of public judicial proceedings or published in court or administrative proceedings.
- Records maintained by state departments of transportation or motor vehicles for the purpose of regulating drivers, pilots, or other operators license.

Effective Date 2/13/2014

## 927.00 PREAPPOINTMENT INVESTIGATIONS OF OFFICE OF INSPECTOR GENERAL APPLICANTS AND EMPLOYEES

### 927.01 General

This manual subchapter contains policies and procedures relating to preappointment investigations of OIG applicants and employees in the General Services Administration - Office of Inspector General (GSA-OIG).

(b) (7)(E) is responsible for the conduct of preappointment investigations. The GSA (b) (7)(E) is responsible for adjudicating completed preappointment investigations. The OIG (b) (7)(E) is responsible for initiating requests for preappointment investigations, for requesting Office of Personnel Management (OPM) Background Investigations, and for providing OPM with a copy of the OIG's preappointment investigation through the GSA Security Office.

#### 927.01A OIG Applicants for Noncritical-Sensitive Positions

The preappointment investigation for OIG applicants for Noncritical-Sensitive positions will cover the following information:

- (b) (7)(E) and local police checks;
- telephonic check with FBI (birth date prior to 1956);
- credit record checks;
- verification of applicant's most recent two years of employment;
- the last significant education and all claimed degrees; and
- any additional coverage, which may be requested by the OIG Security Manager, depending upon the position the applicant is to fill.

#### 927.01B OIG Applicants for Critical-Sensitive Positions

Investigations for applicants for critical-sensitive positions also will include the following:

- conduct interviews with applicant's supervisor and coworkers;
- neighborhood interviews; and
- reference interviews.

927.02 Procedures for Conducting Preappointment Investigations

927.02A Responsibilities

(b) (7)(E) is responsible for obtaining the applicant's resume and the signed Authorization for Release of Information form (Figure 927-01). (b) (7)(E) are responsible for conducting the preappointment investigation. The procedures to be followed depend upon the sensitivity of the position the applicant is being hired for and whether the applicant is a JI applicant, a Non-JI applicant, a GS-14 or above, or a Summer or Temporary Hire.

The (b) (7)(E) staff is responsible for:

(b) (7)(E)

(b) (7)(E)

For OIG Applicants. Upon receipt of the (b) (7)(E) from a Central Office OIG official, the (b) (7)(E) staff:

(b) (7)(E)

The (b) (7)(E) is responsible for:

- conducting pre-appointment investigations for all OIG applicants, excluding (b) (7)(E), which are completed by the (b) (7)(E) staff; and

- (b) (7)(E)

(b) (7)(E)

- (b) (7)(E)

(b) (7)(E)

### 927.02B General Guidelines for Investigative Coverage

The following sections provide guidelines concerning investigative coverage in conducting preappointment investigations.

1. Objective. The overall objective of the preappointment investigation is to obtain information which will enable the hiring official to determine if the applicant is suitable for Federal employment. Due to the sensitive nature of duties performed in the OIG, certain basic information on which to base sound decisions on suitability is required.
2. Privacy Act Notification. Each person interviewed and each record custodian, with the exception of custodians of public records and frequently contacted (b) (7)(E) should be informed that all information they provide, including a (b) (7)(E) identity, may be disclosed to the subject of the investigation upon his or her request. If the interviewee specifically requests that his identity be kept confidential, the interviewee may be treated confidentially in accordance with established procedures.

Additionally, each such person should be notified of the statutory authority for collecting the information, the principal purpose for which it will be used, and any "routine uses" of the information. See 5 U.S.C. § 552a(e).

(b) (7)(E)

3. Safeguards Against Invasion of Privacy. Inquiries concerning an applicant shall be limited to matters relevant to a determination of suitability for a position in OIG. Federal regulations prohibit unwarranted invasion of privacy of applicants. The prohibitions of this regulation are applicable for all preappointment inquiries, with the following specific restriction warranting emphasis: Office of Investigation employees are not authorized to inquire about race, religion, national origin, sexual behavior, union membership, fraternal, or political affiliations, or the constitutionality or wisdom of legislative policies and procedures.
4. Information to be Developed. The following sections describe the areas of investigative coverage and information to be developed in conducting preappointment investigations for OIG applicants.

- Date and Place of Birth. Verification of the applicant's date and place of birth by official records is not necessary if this information can be corroborated by school, employment, or other records. Should a discrepancy be disclosed, the investigator should ask the applicant to exhibit his/her birth certificate or direct a letter of inquiry to the appropriate State Bureau of Vital Statistics for verification of the date and place of birth.

- Citizenship. Normally, citizenship will be verified through date and place of birth. If the applicant is foreign-born, or a naturalized U.S. citizen, citizenship will be verified through review of appropriate court records or Immigration and Naturalization Service district office records, or acceptable documentation. (Examples include United States Passport; Certified Birth Certificate; Consular Report of Birth; Naturalization Certificate; Certificate of Citizenship; U.S. Citizenship Identification Card; INS Form 1-197; and Military Discharge Form DD-214.)

- Physical and Mental Limitations. Review information which indicates a current or past physical or mental disability and report such information.

- Employment. For all Critical Sensitive positions and all JI applicants, verify the last two years of employment, including interviews with supervisors and work associates. For all other applicants in Non Critical positions, verify the last two years of employment; the hiring component staff will be responsible for conducting interview with supervisors. The following guidelines apply:

- If this coverage is inadequate or if an applicant has had frequent changes of employment, verify/interview additional employers for at least a 3-year period.

- If for any reason the applicant requests that his/her last employer not be interviewed, the official requesting the suitability inquiry will so state in the referral memorandum. However, the applicant will be advised that, after all other checks have been made, his/her last employer must be interviewed prior to completion of the inquiry.

- If an applicant is a present or past Federal employee, review the applicant's Official Personnel Folder and Department/Agency Security file and report derogatory information, employment, and other background data.

- As applicable, review administrative files, OIG records, employment dates, and reasons for leaving.

- Education. Review academic and disciplinary records; verify all claimed degrees; check other school records, including the campus security office, for the last significant period of education. In the case of a recent graduate with little or no work history, interviews of teachers, counselors, and security officers are appropriate. Note: Prior to initiation of the inquiry, it should be determined that the applicant has signed a release(s) in order that all appropriate records may be expeditiously reviewed or obtained.

- Police and Criminal Records. Check (b) (7)(E) and local police departments at places of residence, education and employment for the past two years. If results reveal arrest information without disposition(s) check appropriate court records.

- Credit Records. Report information on the applicant's credit standing and financial responsibility as reflected from records of such sources as credit bureaus, merchants or other credit establishments. Questions of poor credit or financial irresponsibility must be resolved. Clear records should be reported as "Record Favorable."

- References (b) (7)(E) When appropriate, during interviews of references, attempt to corroborate periods of unemployment, self-employment and foreign travel not verified by records, in addition to the basic suitability coverage.

- Neighborhood (b) (7)(E) Neighbors may know an applicant from a different perspective than an employer, coworkers or references. When appropriate, interviews with neighbors should also attempt to corroborate periods of unemployment, self-employment and foreign travel not verified by records, in addition to the basic suitability coverage.

5. Adverse Information. Adverse or potentially disqualifying information developed during the inquiry shall be brought immediately to the attention of the appropriate OIG hiring official and the OIG (b) (7)(E) (b) (7)(E). If the OIG hiring official considers the adverse information disqualifying, terminate the pre-employment inquiry. The hiring official who makes the preliminary determination not to hire an applicant for cause must ensure that all applicable procedures are followed and that the applicant is notified. Additional inquiry may be necessary to resolve conflicting information. After all material matters have been fully resolved, a second contact with the applicant may be necessary. After these due process steps have been completed, the determination on whether to select the applicant should be made, and the applicant notified accordingly. This process must be documented by a memorandum to the file, with a copy to the (b) (7)(E). These procedures should be followed in each case of this type. The information acquired up to the point of termination should be incorporated in a report together with the reasons for discontinuing the investigation.

Generally, circumstances described in any of the following three categories may result in the discontinuance of the investigation. Any such discontinuance will always be at the direction or with the approval of the (b) (7)(E). The (b) (7)(E) notifies the OIG (b) (7)(E) prior to the discontinuance.

- If, at any stage of an investigation, official notification is received to the effect that the applicant is no longer being considered, or that the applicant's services have been terminated by a resignation or otherwise, the investigator should stop the inquiry and submit a report setting forth the results of such inquiries as have been completed. The report should also reflect the reason and authority for discontinuing the inquiry.

- If the investigator develops credible derogatory information that raises any question of loyalty to the Government of the United States, indicates subversive activity, indicates that the individual may have been or may be subject to coercion, influence, or pressure to act contrary to the interests of the national security, or is or has been involved in any criminal conduct, the investigation must be discontinued. A report containing all pertinent information is immediately forwarded to the (b) (7)(E).

#### 927.02C Format and Distribution of Letter Reports

The SAC reports investigative results in the format shown in Figure 927-02, and forwards the letter report to JIB for processing at Central Office.

Effective Date 6/26/2013

928.00 LAW ENFORCEMENT AVAILABILITY PAY (Formerly Section 403.00, which was updated July 12, 2006, and November 12, 2009)

The Law Enforcement Availability Pay Act of 1994 provides that covered criminal investigators (“special agents”) will receive availability pay to ensure their availability, based on the OIG’s needs, for unscheduled duty in excess of a 40-hour workweek.

Authority governing Law Enforcement Availability Pay (LEAP) is found in the Inspector General Act as amended, 5 U.S.C. App.3, and the Law Enforcement Availability Pay Act of 1994, § 633 of the Treasury, Postal Service, and General Government Appropriations Act, FY 95, Pub.L.No. 103-329 (5 U.S.C.

§ 5545a, 5542(d)). This policy follows and is subject to regulations issued by the Office of Personnel Management at 5 CFR § 550.181 et seq.

#### 928.01 Definitions

1. Availability pay is generally 25 percent of the rate of basic pay for a special agent position on an annual basis and is a form of premium pay granted in the Law Enforcement Availability Pay Act of 1994. A special agent may be paid availability pay only to the extent that the payment does not cause the employee’s aggregate rate of pay for any pay period to exceed the lesser of 150 percent of the gross pay for GS-15, Step 1, or the rate payable for Level V of the Executive Schedule. Availability pay will be considered as part of basic pay for the purposes listed in 5 CFR § 550.186, e.g., for computing advances in pay under 5 USC § 5524a, severance pay, workers’ compensation, Thrift Savings Plan, retirement benefits, lump sum annual leave, and life insurance.
2. Available for work means that a special agent is generally and reasonably accessible to perform official duties outside of the agent’s basic workweek based on the needs of GSA OIG. A special agent cannot be credited as being “available for work” on non-regular workdays.
3. Unscheduled duty hours are those hours a special agent performs work or is available for work per this policy, which are not part of the 40 hours in the basic workweek or not regularly scheduled overtime hours. Specifically, for regular workdays, unscheduled duty hours may only consist of hours a special agent performs work or is available for work. For non-regular workdays, such as weekends, unscheduled duty hours may only consist of hours actually worked by a special agent
4. Administrative work week means a period of 7 consecutive calendar days designated in advance by the head of an agency under 5 U.S.C. § 6101
5. Basic work week for full-time employees means the 40-hour workweek.
6. Regular workday for the purpose of determining whether a special agent shall be paid availability pay means each day in the basic workweek during which the special agent works at least 4 hours. The following does not count towards the 4 hour work requirement: regularly scheduled overtime hours, unscheduled duty hours, hours attending officially approved training, official travel hours, approved

leave with pay (e.g., annual, sick or administrative leave), or excused absences (e.g. court leave, holidays and inclement weather closures). (Excluding from regular workdays those days when a special agent does not work at least 4 hours ensures that a special agent is not penalized for spending duty time in management directed activities.) Official travel hours for this purpose is limited to those hours during which a special agent is engaged in officially ordered non-local travel away from the special agent's official duty station. Any local travel, including while in travel status, is considered a part of a special agent's regular workday

## 928.02 General Rules

1. A special agent shall be eligible for availability pay if the annual average of unscheduled duty hours per regular workday is, or in the case of a newly hired special agent, is expected to be, equal to or greater than 2 hours. Unscheduled duty hours are defined in paragraph 3 of the definitions sections of these guidelines. Special agents must certify that they meet and/or expect to meet, as the case may be, this annual average requirement. (See paragraphs 2 and 3 below.) The annual average is computed as follows:

Average annual hours = total unscheduled duty hours/total regular workdays

2. A newly hired special agent must certify that they expect to meet the annual unscheduled duty requirements of these guidelines. A sample certification memorandum is shown as Attachment A. [REDACTED], must also certify that a newly hired special agent is expected to meet the annual unscheduled duty requirements of these guidelines. A sample [REDACTED] certification memorandum is shown as Attachment D. The [REDACTED] memorandum will authorize the payment of availability pay to the special agent.

3. Each special agent who is receiving availability pay must annually certify that he or she currently meets, and is expected to continue to meet during the upcoming year, the annual unscheduled duty requirements of these guidelines. A sample certification memorandum is shown as Attachment B.

In addition, each [REDACTED] shall conduct an annual review and certification of qualification for availability pay, and report such to the [REDACTED] by memo. The purpose of the memo is to certify the special agents who have met and are expected to continue to meet the requirements of these guidelines. The certification will be done on a [REDACTED] basis and will be due to [REDACTED] [REDACTED]. A sample [REDACTED] certification memorandum is shown as Attachment E.

4. For various reasons, including personal situations, family hardships, or physical limitations, some special agents may not be able to perform official duties during unscheduled duty hours or generally be available for work to the extent required by these guidelines. A special agent, with [REDACTED] approval, may opt out of the availability pay requirements at any time by signing a memorandum documenting this request and his/her understanding that availability pay will not be paid during this period. This opt-out period is generally expected to be 3 months or more in duration.

The opt-out request memorandum will be directed to [REDACTED], who will forward the request to the [REDACTED] for final approval. The [REDACTED] is the supervisor for any [REDACTED] who wishes to use this opt-out provision. A sample opt-out request memorandum is shown as Attachment C. The special agent

will be placed back on availability pay only after he or she recertifies that he or she will be available. A new certification (Attachment A) is required.

The (b) (7)(E) may, however, recall a special agent to full availability pay duty status at any time if the workload demands of the GSA OIG require that additional special agents be called on to perform unscheduled duty time.

5. Management may deny or cancel a special agent's LEAP certification at any time if due to changed circumstances (e.g., the avoidance of work or non-availability by the special agent) the special agent no longer is expected to meet the average 2 hours per day requirement. Any revocation of an originally valid certification will be made on a prospective basis and will result in the agent's removal from availability pay. A denial or cancellation by management of a certification constitutes an involuntary reduction in pay for the purpose of applying the adverse action procedures under 5 U.S.C. § 7512 and 5 C.F.R. Pt. 752. All such actions must be coordinated through the (b) (7)(E)

6. Compensation, either by pay or compensatory time off, for unscheduled duty hours worked over the annual daily average requirement is not authorized.

7. All GSA OIG special agents (GS-5 through GS-15) who are receiving availability pay are exempt from the Fair Labor Standards Act.

8. To ensure that unscheduled duty hours are applied to the maximum practical extent for the work needs of the Office of Investigations and to facilitate required supervisory certification, unscheduled duty hours are generally hereby authorized without prior supervisory coordination. Special agents are responsible for recognizing, without supervision, circumstances that require them to be on duty or to be available for work outside of their basic workweek.

9. Special agents will continue to receive availability pay while on agency approved training, travel, and annual or sick leave so long as they meet the annual requirements for receiving availability pay set forth in 928.02, paragraph 1. Agents will also receive availability pay while on certain categories of excused absence, such as for relocation or while on military leave.

10. As noted previously, hours spent in training and on travel may not be counted against the special agent as a regular workday for the purpose of calculating a special agent's total regular workdays under this policy. However, hours spent in training and on travel may count to the benefit of the special agent as unscheduled duty hours for the purpose of calculating an agent's average annual hours under this policy in the following scenarios:

- Time spent in training beyond an agent's scheduled tour of duty, whether on a regular workday or non-regular workday; or
- Pursuant to the "hours of employment" test in 5 U.S.C. 5542(b)(2), time spent in official travel status (i.e., approved, non-local travel) beyond an agent's scheduled tour of duty, whether on a regular workday or non-regular workday, only when the travel:
  - Involves the performance of work while traveling;
  - Is incident to travel that involves the performance of work while traveling;

◦Is carried out under arduous conditions; or

◦Results from an event which could not be scheduled or controlled administratively, including travel by an employee to such an event and the return of such employee from such event to his or her official-duty station (e.g. non-agency initiated or scheduled events).

11. GSA OIG special agents normally will not be assigned regularly scheduled overtime; however, they will be assigned tasks which will likely require unscheduled duty. They will, because of their assignments, experience erratic and irregular periods of work, the nature and required duration of which cannot be ascertained in advance.

12. Since availability pay generally requires a special agent to be available at irregular hours to perform unscheduled work, this factor will be considered for all requests for approval of outside employment or other activities, and generally such requests will not be approved absent a showing by the special agent that such employment or activity will not interfere with his/her ability to be available. In addition, the GSA OIG may revoke the approval of an outside employment request if the workload demands of the office require such action.

13. Unscheduled duty hours will normally be self-initiated for direct labor activities, as defined in the (b) (7)(E) User Guide, Time Reporting Information. It is expected that non-direct activities will occur during normal office business hours. Exceptions will be granted, however, with prior justification and supervisory coordination.

### 928.03 Reporting Requirements

1. Biweekly Reporting. The recording of unscheduled duty hours for annual availability pay purposes will be accomplished by entering the appropriate hours in the specified fields in the (b) (7)(E) module. The (b) (7)(E) module will automatically calculate a special agent's LEAP hours every two weeks. Each special agent must maintain his/her time in (b) (7)(E) and submit his/her electronic timesheet for approval. Since Saturdays and Sundays are not normal workdays, any availability pay hours generated on Saturdays and Sundays will be entered under the column for that particular day. The (b) (7)(E), is responsible for ensuring that special agents' reports of hours of unscheduled duty hours worked or available are accurate. (b) (7)(E) should carefully review (b) (7)(E) to ensure that time charged corresponds with the work during the period. Special agents will always report the actual number of unscheduled duty hours worked or available. (b) (7)(E) hours will be reviewed by the (b) (7)(E) or the (b) (7)(E)

2. Approval of Availability Hours. (b) (7)(E) will review and approve special agent availability hours in (b) (7)(E) and verify that special agents are meeting the 2 hour average minimum of unscheduled duty hours per week. If for some reason a special agent's annual cumulative daily average of unscheduled duty time falls below the minimum, the (b) (7)(E) should advise the special agent that he/she is in danger of not meeting the annual qualification for availability pay. The (b) (7)(E) and special agent must develop a plan to ensure that the special agent will meet the qualification for availability pay. Based on individual schedules, special agents may schedule their workday according to the needs of their respective schedules, so long as their unscheduled hours annually average two or more per day. (The (b) (7)(E) supervisor for purposes of this section.)

Effective Date 3/14/2018

## 930 INVENTORY AND PROPERTY MANAGEMENT POLICY

### 930.01 Purpose and Scope

This policy sets forth the standards and procedures governing the Office of Investigations (JI) requirements for the Property Management and Inventory Programs. It also establishes the duties and responsibilities of Property Management Officers (PMO), Inventory Administrators (IA), Custodial Officers, and JI employees responsible for inventorying and managing JI issued property.

The OIG follows GSA Order ADM 7800.12, "Management of the U.S. General Services Administration's (GSA) Internal Personal Property," except where the provisions in that Order conflict with OIG policy.

This policy does not cover property issued to JI personnel by JP. Policies and procedures governing requirements for JP issued property are set forth in OIG Policy, Subchapter 441.00 Property Management Program.

### 930.02 Definitions

The following definitions are pertinent to JI operations:

1. **Accountable Property:** Government owned property, regardless of cost, that requires control because of its sensitivity to loss or theft.
2. **(b) (7)(E):** The electronic database used by JI staff to log, track and monitor equipment and resources purchased by JI. Users assigned to the Admin group are able to create Technical, Accountable and Expendable Property inventory items in (b) (7)(E).
3. **Technical Equipment:** Represents equipment such as cameras, recorders, monitors, radios, etc. Users are able to search and view the entire Technical inventory.
4. **Expendable Property:** Represents items that may be worn during field activities such as clothing and holsters.
5. **Custodial Area:** The physical location of an office or division that is assigned to a Custodial Officer.
6. **Custodial Assigned:** Any property not currently assigned to personnel, it can be assigned to a particular field office and may be shared (i.e., copier, shredder, color printer, etc.).
7. **Physical Inventory:** A physical identification and count of technical and accountable property that has been logged into (b) (7)(E).

### 930.03 Responsibilities

#### 1. Property Management Officer (PMO)

The (b) (7)(E) shall serve as the PMO for all technical and accountable assets purchased by and assigned to JI components. PMO responsibilities shall include:

- a. Providing leadership and guidance to OIG staff on the proper use, care, and disposal of property.
- b. Ensuring that inventory records are maintained for each assigned custodial area.
- c. Approving and archiving items from the system (i.e., excess, recycle, donation or destruction). Ensuring that custodial officers are aware that all technical and accountable property is recorded in JI's property management and tracking system, (b) (7)(E).
- d. Ensuring that (b) (7)(E) physical inventory of all JI issued technical and accountable property is conducted.

#### 2. Inventory Administrators (IA)

The PMO will designate an Inventory Administrator (IA) who shall act as the primary staff responsible for overseeing JI issued technical and accountable property. IA responsibilities include:

- a. Adding, updating, and maintaining technical and, accountable property in (b) (7)(E). All common, shared, or temporarily unassigned IT property at a physical location should be assigned in (b) (7)(E) to the office's Custodial Officer.
- b. Ensuring all assignments, reassignments and disposals of accountable property is recorded in (b) (7)(E) (b) (7)(E).
- c. Log shipments of new accountable or technical property into HQ's inventory in (b) (7)(E) (b) (7)(E).
- d. Ship property to the appropriate field office and transfer the property in (b) (7)(E) to the assigned field office or physical location. The Custodial Officer will accept the property into their offices inventory and assign it to the designated employee within that field office.
- e. Work closely with the Custodial Officer who will authorize/approve updates as required.
- f. Assist Custodial Officer's as necessary to properly excess, dispose or recycle property.
- g. Inform custodial officers of any inventory requirements that arise throughout the year.
- h. Assist the Custodial Officers as needed with processing electronic recycling equipment with UNICOR or USPS.

#### 3. Custodial Officers

The (b) (7)(E) or (b) (7)(E) if designated by the (b) (7)(E) of each field office will serve as the inventory Custodial Officer. The (b) (7)(E) may also appoint a technical custodial officer to oversee the technical property assigned to each field office. The Custodial Officer responsibilities include:

- a. Accounting for all property (assets) assigned to a designated physical location. A list of property that will be accounted for can be found in Figure 930-01.
- b. Identifying and properly disposing of items that are no longer necessary within the custodial area.
- c. Properly documenting in (b) (7)(E) disposal, transfer or excess of property assigned to their custodial area.
- d. Designating secure storage areas for accountable property not issued to prevent theft of OIG property.
- e. Notifying the PMO and IA of loss of assigned custodial property.
- f. Custodial Officer's will conduct an (b) (7)(E) physical inventory of all technical and accountable property assigned to their field office.
- g. The Custodial Officer will identify property that can be disposed of or recycled and coordinate the disposal or recycling of the property utilizing the GSAXcess system.
- h. Custodial Officers may also assign ammunition updates to (b) (7)(E) inventory within (b) (7)(E).
- i. Accepting accountable and technical property assigned to your field office's region and marking it as inventoried in (b) (7)(E) at that time.
- j. Assigning accountable property to designated employees as needed
- k. Ensuring acceptance of assigned property by employees in (b) (7)(E)
- l. Returning property to HQ when no longer needed by the field office; marking it as transferred in (b) (7)(E)
- m. Ensuring that assigned (b) (7)(E) maintain a current inventory of ammunition and magazines locally. These inventories are required to be uploaded to (b) (7)(E) (b) (7)(E) (can be conducted during (b) (7)(E) ) or when requested to do so by HQ or the (b) (7)(E).

#### 4. Employees

Upon receipt of accountable or technical property, employees shall assume the responsibility for its protection and safekeeping. JI employees will have read-only access to their own inventory record in (b) (7)(E). Specific employee responsibilities include:

- a. Confirming/rejecting changes to their inventory within (b) (7)(E) of the change.
- b. Exercising reasonable and responsible care of all accountable and technical property.
- c. Reviewing and electronically confirming their personal inventory record during the (b) (7)(E) inventory and after receiving or returning any personal property.
- d. Reporting lost, stolen, or damaged property to the Custodial Officer as soon as possible.

e. Returning all issued property to the Custodial Officer prior to transferring to another field office or prior to their last day of employment with GSA OIG.

#### 930.04 Inventory Management

Control of all accountable property issued by JI shall be appropriately documented and maintained in a traceable and orderly manner. All technical and accountable property must be recorded in (b) (7)(E) Designated IAs and Custodial Officers are responsible for ensuring the integrity of the information entered into (b) (7)(E) by ensuring that all property received is assigned, reassigned, or disposed of and recorded in (b) (7)(E) of the transaction.

(b) (7)(E) inventory will be conducted each calendar year (b) (7)(E). Both technical and accountable inventory (to include GOV's and ammunition) will be checked at this time. Upon completion of conducting a 100% inventory for all property assigned to the Custodial Officer's custodial area, the Custodial Officer will update (b) (7)(E) that the inventory was completed by marking it as inventoried. Discrepancy reports (i.e. list of missing property) will be sent to the PMO who will notify the (b) (7)(E) and (b) (7)(E).

a. During (b) (7)(E) inventory all technical property will be marked as inspected. In order to inspect property the technical item must be turned on and operated in the manner to which it is to be used. This will ensure JI only maintains fully operational equipment. Once its usability has been tested the item will be marked as "inspected" in (b) (7)(E).

i. Any property that is no longer functional or has been deemed as not needed will be processed according to GSA property disposal guidelines (see section 930.06).

ii. Offices will coordinate with the IA to process the disposal of this type of property.

#### 930.05 Lost or Stolen Property

Employees are charged with safeguarding all property and must immediately report any lost or stolen technical or accountable property to his or her Custodial Officer and the police if applicable. Employees may be held liable for JI issued property that is lost, stolen, or damaged if there is evidence of negligence or misconduct by the employee. However, when loss, theft, or damage occurs there are reporting requirements that must be strictly followed. JI personnel may be found to be financially liable for the property per GSA OIG Subchapter 508.00 Financial Liability for Stolen, Damaged, Lost or Destroyed Government Property.

#### 930.06 Disposal of Property

Federal Management Regulation §102-36.30 deems property to be excess when it is no longer needed to carry out the functions of official programs within an agency. The Custodial Officer must request approval for the disposal of all property through the PMO. The process for disposing of property differs depending on the location and the sensitivity of the property and should be coordinated with the IA.

## CHAPTER 1000 - INSPECTIONS AND FORENSIC AUDITING POLICIES AND PROCEDURES

### 1001.00 OFFICE OF INSPECTIONS AND FORENSIC AUDITING (JE)

1001.01 Responsibilities

### 1002.00 ORGANIZATION

1002.01 Inspections

1002.02 Forensic Auditing

1002.03 Quality Assurance

### 1003.00 ROLES

1003.01 Director

1003.02 Deputy Director

1003.03 Teams

1003.04 Evaluation Attorney

### 1004.00 INSPECTION STANDARDS

1004.01 Competency

1004.02 Independence

1004.03 Professional Judgment

1004.04 Quality Control

1004.05 Planning

1004.06 Data Collection and Analysis

1004.07 Evidence

1004.08 Records Maintenance

1004.09 Timelines

1004.10 Fraud, Other Illegal Acts, and Abuse

1004.11 Reporting

1004.12 Follow-up

1004.13 Performance Measurement

1004.14 Working Relationships and Communication

### 1005.00 OIG QUALITY ASSURANCE

1005.01 Federal Manager's Financial Integrity Act

1005.02 Annual Assurance Statement

1005.03 Assurance Statement Responsibilities

1005.04 Assurance Statement Process

1005.05 Internal Control Review

1005.06 Internal Control Review Responsibilities

1005.07 Seven Steps of an Internal Control Review

1005.08 FMFIA Record Management

1005.09 Operational Assessments

1005.10 Operational Assessment Procedures

1005.10A Operational Assessment Scheduling

1005.11 Operational Assessment - Component Assistance

1005.12 Questionable Charges and Delinquent Accounts

1005.13 Questionable Charges and Delinquent Accounts - Initial Inquiry

1005.14 Questionable Charges and Delinquent Accounts - Component Responsibility  
1005.15 Questionable Charges and Delinquent Accounts - Reporting

1006.00 RECORDS OFFICER  
1006.01 Records Officer

1007.00 PROJECT INITIATION  
1007.01 Project Initiation

1008.00 REFERRALS TO THE OFFICE OF INVESTIGATIONS  
1008.01 Referrals to the Office of Investigations

1009.00 INTERAGENCY COMMITTEES AND WORKING GROUPS  
1009.01 Interagency Committees and Working Groups

#### APPENDICES

Appendix A - Report of Continuing Professional Education

Appendix B - Independence

Appendix C - Management Decision Record for Inspections

Footnotes

Effective Date 12/15/2014

## 1001.00 OFFICE OF INSPECTIONS AND FORENSIC AUDITING (JE)

### 1001.01 Responsibilities

JE independently and objectively: (1) analyzes and evaluates GSA's programs and operations through management and programmatic inspections and evaluations (hereinafter inspections) that are intended to provide insight into issues of concern to GSA, Congress, and the American public; (2) reviews and evaluates potentially fraudulent or otherwise criminal activities through the use of forensic auditing skills, tools, techniques, and methodologies, and; (3) formulates, directs, and coordinates quality assurance for the OIG.

The Inspector General Act of 1978 as amended, 5 U.S.C. App. 3 (IG Act), authorizes the OIG to inspect GSA programs and operations. Inspections are neither audits nor investigations; rather, they are systematic and independent assessments of the design, implementation, and/or results of an Agency's operations, programs, or policies. They provide information that is timely, credible, and useful for agency managers, policymakers, and others. Inspections can be used to determine efficiency, effectiveness, impact, and/or sustainability of agency operations, programs, or policies. They often recommend improvements and identify where administrative action is necessary.

Effective Date 12/15/2014

## 1002.00 ORGANIZATION

JE generally conducts the following types of activities.

### 1002.01 Inspections

An inspection examines the efficiency, effectiveness, and impact of a policy, program, function, operation, activity, or practice in order to add value. An inspection may also review a program, function, operation, activity, or practice perceived to be at risk in order to determine the extent to which it adheres to standards, good practices, or criteria, and to identify corrective action as needed. An inspection may also be issued as a "survey report." This is generally the same as an inspection, but is typically narrower in scope.

### 1002.02 Forensic Auditing

Forensic auditing is the use of data analysis and other new technologies to identify irregularities that may indicate fraud, waste, or abuse in GSA operations. At the direction of the Inspector General, Deputy Inspector General, or the Associate Inspector General, JE:

- Conducts reviews of potentially fraudulent, improper, wasteful, and/or abusive activities;
- Conducts anti-fraud efforts through proactive prevention, early detection, and timely inquiries regarding potential fraud related to GSA operations, and works with other OIG components, as appropriate, in the subsequent pursuit of criminal, civil, and administrative remedies; and
- Engages in computer analysis and other technological strategies intended to bolster traditional audit and investigative practices and procedures.

### 1002.03 Quality Assurance

The internal evaluation and analysis program was established to provide quality assurance for the OIG organization. The quality assurance program does not replace, but rather supplements, line managers' responsibilities. The quality assurance program is conducted through operational assessments of OIG audit and investigative field offices, as well as Central Office support staffs. The quality assurance function includes responsibility for planning, directing, and coordinating the OIG's reporting requirements under the Federal Managers Financial Integrity Act of 1982 (FMFIA), to include both the Annual Assurance Statement and Internal Control Reviews. The quality assurance function also handles the first line of inquiry regarding OCFO questionable transactions involving OIG purchase cards and travel cards, as well as delinquent balances on travel cards.

Effective Date 12/15/2014

## 1003.00 ROLES

### 1003.01 Director

The Director, Office of Inspections and Forensic Auditing (Director), provides supervisory oversight of all JE matters, including personnel; office administration; strategic planning; compliance with OIG policies and procedures; and the planning, production, and maintenance of the JE Plan. The Director reports to the Associate IG.

### 1003.02 Deputy Director

The Deputy Director serves as second in charge of JE when needed. The Deputy supervises Senior Management Analysts and Senior Auditors, and team leads in the initiation, planning, development, and completion of work assignments to ensure the projects meet the highest quality and professional standards of the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation (January 2012) (CIGIE I&E Blue Book). The Deputy Director also ensures resources are focused on high impact/high risk areas.

### 1003.03 Teams

Senior Management Analysts and Senior Auditors report to the Deputy Director, and provide direction for multiple projects, as assigned, across all JE responsibilities. Team Leads are designated for specific projects, and they are responsible for directing the work of others assigned to the project and for the successful completion of the project.

### 1003.04 Evaluation Attorney

The JE Evaluation Attorney provides quality assurance for JE's products through legal research and analysis to identify the legal framework for JE's forensic audit and inspection products, and ensures any legal issues reflect the views of the OIG's Office of Counsel. The Evaluation Attorney is also the OIG records management liaison, providing policy, and guidance on records management issues OIG-wide. The Evaluation Attorney reports to the Director.

Effective Date 12/15/2014

## 1004.00 INSPECTION STANDARDS

The IG Act, § 11(c)(2), provides that Offices of Inspector General "shall adhere to professional standards developed by the Council" of the Inspectors General on Integrity and Efficiency (CIGIE). In June 2010, CIGIE officially adopted quality standards for inspections, revised in 2012, which form the "Quality Standards for Inspection and Evaluation" (CIGIE I&E Blue Book), available at <http://www.ignet.gov/pande/standards/oeistds11.pdf>. The CIGIE I&E Blue Book is incorporated in this Manual by reference. All JE staff must be aware of and comply with its standards. (The term "evaluation," used in the CIGIE I&E Blue Book, includes "inspection" and "review.")

The 14 CIGIE I&E Blue Book standards that govern the performance of JE inspections are:

- Competency
- Professional Judgment
- Planning
- Evidence
- Timeliness
- Reporting
- Performance Management
- Independence
- Quality Control
- Data Collection and Analysis
- Records Maintenance
- Fraud, Other Illegal Acts, and Abuse
- Follow-up
- Working Relationships and Communication

In addition to complying with the CIGIE I&E Bluebook requirements, OIG policy for JE is as follows.

### 1004.01 Competency

JE staff members will strive to complete biennially 80 hours of CPE that directly enhances their professional proficiency, and they must biennially complete 40 hours. At least 20 CPE hours per year should be in subjects directly related to the work of JE, and 20 CPE hours should be completed every year. This requirement is independent of, but may overlap with, professional license requirements.

JE supervisors will use the core competencies and general skill levels outlined in Appendices A and B of the CIGIE I&E Blue Book as a guide. In general, skills will be achieved via formal classroom training, online training, on-the-job training (OJT), briefings, training conferences, and seminars.

Each staff member's professional development is the joint responsibility of JE management and the staff member. Skills training for grades GS-05 through GS-12 will be directed by JE management. The Deputy Director functions as the JE Training Officer. Staff members at grades GS-13 and above are responsible for identifying appropriate educational opportunities. The Director is responsible for administering the JE training budget, and approving the Training Officer's plan for education as appropriate.

Each staff member is responsible for the submission of a completed Report of Continuing Professional Education (Appendix A) and supporting documentation, where appropriate. The Training Officer is responsible for ensuring appropriate records of training are kept.

### 1004.02 Independence

Each JE employee, or subject matter expert who participates in an inspection, including the Director and Deputy Director, must complete the Statement of Independence (Appendix B) on an annual basis.

As part of the planning process for every assignment, the responsible Senior Management Analyst/Senior Auditor will hold discussions with the entire inspection team to address the issue of impairments. The results will be documented in a statement of Independence (Appendix B). The same process is repeated when an employee joins a project already in progress.

JE staff are responsible for notifying their Team Lead if participation in a particular matter could cause a reasonable person with knowledge of the relevant facts to question the employee's impartiality. The Team Lead will notify the Director or Deputy Director, as well as the responsible Senior Management Analyst/Senior Auditor, of any potential impairment issues. The Director or Deputy Director, in consultation with the responsible Senior Management Analyst/Senior Auditor and Team Lead, will make an "determination" on a case-by-case basis, based on the independence standards set forth in the Quality Standards for Federal Offices of Inspector General, Part II, "Ethics, Independence, and Confidentiality (page 10).

#### 1004.03 Professional Judgment

All staff are expected to exercise professional judgment, thereby ensuring that each inspection or project is performed efficiently, effectively, and in accordance with professional standards. Professional judgment includes an element of respectful skepticism. Inspectors must:

- Document significant decisions affecting the objectives, scope, methodology, observations, conclusions, and recommendations that result from the application of professional judgment.
- Diligently gather evidence and objectively evaluate its sufficiency, competency, and relevance to the matter under consideration.
- Become reasonably assured of his/her evidence, analytical methods, and conclusions throughout the evaluative process.
- Maintain the highest degree of integrity, objectivity, and independence in the application of professional judgment.

#### 1004.04 Quality Control

Team Leads, or designated senior JE professionals, monitor work efforts and review documentation prepared by team members throughout the fieldwork process. This includes working with inspection team members to ensure that instructions are fully understood and followed. Team Leads should record decisions made and instructions given regarding the review process.

Team Lead reviews of completed analyses, tests, and determinations should ensure that appropriate evidence or information exists to support findings, conclusions, observations, and recommendations. Team Leads and senior JE professionals should record supervisory reviews. The document should include responses by the team members and final determinations by the reviewer. Team Lead review must be completed for all documented evidence that supports the report's findings and conclusions and all documented evidence must be reviewed (as appropriate including report referencing) prior to report issuance.

## 1004.05 Planning

There are two types of planning – workload planning and planning of individual projects. The CIGIE I&E Bluebook standard deals with the latter. With regard to workload planning, JE annually plans reviews in order to identify and establish the workload for the fiscal year. The plan has three components: (1) inspections intended to provide insight into issues of concern to GSA, Congress, and the American public; (2) reviews and inspections of potentially fraudulent or otherwise criminal activities through the use of forensic auditing skills, tools, techniques, and methodologies; and (3) OIG quality assurance reviews. Workload planning is a shared responsibility with input provided by all JE staff. Changes to plans and objectives are often necessary due to the ever changing operating environment of the OIG, and are directed by the Associate IG, Deputy IG, and/or IG.

With regard to planning assigned projects, the responsible Senior Management Analyst/Senior Auditor, along with the Team Lead, are responsible for producing an Inspection Work Plan that the team is to follow and adapt as appropriate throughout the review. Planning is a collaborative effort, but the Team Lead is responsible for managing the work of other team members. The Team Lead is responsible for ensuring that team members follow and understand the work plan objective(s), scope, and methodology. The responsible Senior Management Analyst/Senior Auditor is responsible for arranging an appropriate work site and for contacting appropriate officials to obtain their cooperation and assistance throughout the review. The Team Lead is expected to work through issues and challenges encountered during each assignment and consult with the responsible Senior Management Analyst/Senior Auditor and Deputy Director to keep them informed of the status of the assignment and seek advice and guidance as needed.

## 1004.06 Data Collection and Analysis

The responsible Senior Management Analyst/Senior Auditor and Team Lead are responsible for directing the inspection team's resources toward achieving the review objectives. The responsible Senior Management Analyst/Senior Auditor and Team Lead should develop a work plan that identifies the source, location, and type of data to be collected, and how the data will be used in the review. Data collection may include accessing GSA systems, conducting interviews of Agency personnel and/or third-party stakeholders, researching, and other means.

Inspectors must take reasonable steps to assess the reliability of computerized data used as evidence. Examples of how this may be accomplished include:

1. Identifying prior reviews by GSA OIG, GAO, or system managers attesting to the computer system and data reliability,
2. Discussing data extraction criteria with an information technology (IT) expert to ensure the methodology used for data extraction will produce the data needed, or
3. Conducting data accuracy tests to ensure required data elements have been provided and are in the expected format.

#### 1004.07 Evidence

Requests for evidence should be in writing (email, memorandum, letter, etc.) and should specify the date by which the evidence should be received. The Team Lead is responsible for determining a reasonable date and has the discretion to work with the recipient of the request to ensure that the time frame is reasonable and practicable. The Team Lead will maintain records of the status of all outstanding requests and promptly inform the responsible Senior Management Analyst/Senior Auditor and Deputy Director of any undue delays.

#### 1004.08 Records Maintenance

JE uses CCH® TeamMate (TeamMate) as the method for documenting inspection evidence in electronic format. TeamMate should be used for all Agency reviews. Exceptions to this policy must be approved by the Director or Deputy Director. The maintenance and disposition of documentation must be in accordance with OIG records disposition schedules. The Team Lead should consult with the OIG Records Officer regarding any records management questions.

OIG policy 421.00 discourages use of Instant Messaging to conduct official business. Should Instant Messaging be used in an inspection, then the electronic record, including meta data, must be preserved in accordance with the OIG's file plan.

Documentation created in conjunction with an inspection is considered an official government record and team members must safeguard it in accordance with existing legal and administrative requirements. They must ensure that documentation is not lost, stolen, altered, destroyed, or accessed by unauthorized persons. Material obtained during the review may contain proprietary information or sensitive unclassified information. A separate TeamMate subfolder entitled "Sensitive" should be established in the project file to protect any such documents. Access to workpapers will be limited to the responsible Senior Management Analyst/Senior Auditor, Team Lead, team members, independent reviewers, Director, Deputy Director, and Associate IG. Team members should not leave documentation unattended or unsecured. In addition, team members should not make the documentation available outside of JE without the knowledge of JE management. Additional guidance is provided in the OIG Policy and Procedures Manual, Subchapter 505, Managing Privileged and Sensitive Information.

#### 1004.09 Timelines

Time frames should be flexible in response to changing priorities and unforeseen circumstances such as the need to expand the scope of a review or to add objectives.

The responsible Senior Management Analyst/Senior Auditor monitors the team's progress and provides guidance as necessary to ensure that assigned review steps are completed in a timely manner. The Team Lead should continue discussions with each team member throughout the review to ensure there are no misunderstandings regarding tasks assigned and expected outputs to be produced.

#### 1004.10 Fraud, Other Illegal Acts, and Abuse

Team members should be alert to circumstances that indicate potentially fraudulent practices or other illegal acts. If a team member detects possible fraud or other illegal activities, then the team member should promptly notify the Team Lead and provide supporting documentation if available.

The Team Lead, after discussing the possible fraudulent activity with the team member, should then notify the responsible Senior Management Analyst/Senior Auditor, and either the Director or Deputy Director. Any evidence of potentially fraudulent practices or other illegal acts also should be discussed with JI at an appropriate point during the inspection.

The Director will submit a written referral to JI when appropriate.

#### 1004.11 Reporting

Draft and final reports generally are prepared for inspections, although there may be instances when a final report is issued without a draft, such as for an limited review.

The draft report phase includes the Director or Deputy Director's review and the quality control review of the Team Lead's work papers by responsible Senior Management Analyst/Senior Auditor; independent report review (referencing); and review for legal sufficiency by the OIG Office of Counsel (JC). The final draft report is forwarded to the Deputy IG and the Associate IG for further review prior to transmittal to the Agency. Since final inspection results are to be made publicly available (unless restricted by law or regulation), the Director, Deputy Director, and responsible Senior Management Analyst/Senior Auditor are responsible for ensuring that the official draft report does not contain privileged or confidential information. After approval by the Associate IG, the draft report is transmitted by the Director to Agency officials. When an inspection report is restricted, the Team Lead should include that determination as part of the review documentation.

Preparation of the final report includes summarizing management comments and, if necessary, revising the report based on those comments. In addition, JE responses to management comments are provided, subject to review by the Director, the Deputy IG, and the Associate IG prior to transmittal to the Agency.

In most cases, final reports are signed by the Director and distributed by transmittal letter. The Deputy IG and Associate IG are included on the distribution of final reports. When the Administrator or an official outside of GSA is the report addressee, the final report is signed in accordance with section 102 of the OIG Policy and Procedures Manual. Final reports are distributed based on the nature of the review, type of report, and report recipient. The distribution of restricted reports depends upon the nature of the restriction.

Final reports are to be posted to the OIG public and/or intranet sites within three business days of making the content public, and must comply with Section 508 of the Rehabilitation Act of 1973, as amended.

The Team Lead prepares a Management Decision Record (MDR) for inspection reports (Appendix C). The MDR is transmitted along with the final report and sent to HSSOs, RAs, or other officials and serves as the instrument for documenting the Agency's inspection resolution process. JE completes section A before the MDR is transmitted with the final report to the report addressee. Instructions for completing the MDR are contained in GSA's Internal Audit Followup Handbook (ADM P 2030.2D).

## 1004.12 Follow-up

Final reports are subject to resolution requirements set forth in GSA's Internal Audit Followup Handbook (ADM P 2030.2D) and in Public Law 104-106. These require the resolution of all report results and recommendations within six months of the report issuance date and completion of corrective actions by management within 12 months of the report issuance date. Reports not meeting the resolution and final action requirement are required to be reported to the Congress in the Inspector General's Semiannual Report to the Congress.

Upon receipt of a final report, an Agency official completes the accompanying Management Decision Record (MDR), attaches an action plan, and returns the MDR to JE so the management decision process can be completed.

If JE officials find that the proposed action plan is satisfactory, a resolution letter stating that resolution has been accomplished is forwarded to management. If the MDR is not received or the action plan is not satisfactory when received, JE officials should meet with Agency officials to discuss the issues. In instances where resolution cannot be achieved, the Director should initiate the formal resolution process. The responsible Senior Management Analyst/Senior Auditor is responsible for ensuring compliance with time frames and processing procedures contained in ADM P 2030.2D.

When reviewing proposed action plans, time frames for completing final action more than 12 months from the report issuance date should be carefully considered. If warranted, the Director should contact the action office to ascertain whether an accelerated implementation time frame can be achieved. For action packages where final action is planned for more than 12 months, the resolution letter should notify management that the OIG must report incomplete actions to the Congress in the Inspector General's Semiannual Report to the Congress.

Implementation reviews may be conducted to determine whether appropriate corrective action as stated in the proposed action plan has been taken by management on inspection reports. The scope of the review is limited to an inspection of management's actions in response to the recommendations, but should include appropriate testing to ensure that reported conditions have been corrected by the actions taken.

Implementation reviews finding that management's actions have been implemented in accordance with the action plans should be issued in letter report format. Reviews asserting that actions have not been implemented in accordance with the action plan (or actions taken have not corrected the reported condition) should be issued in either letter or standard report format, but must include management's response as an appendix to the report.

In cases where actions are not being implemented or actions taken have not corrected the reported condition, the final report transmittal letter should inform the management action official that a revised action plan should be submitted to GSA's GAO/IG Audit Response Branch (H1C) within 30 days. A copy of the transmittal letter should be sent to the GAO/IG Audit Response Branch (H1C) with the final report.

Since implementation reviews are not new inspections, the report format should be appropriately revised and no sequence number, other than the number of the original inspection, should be included in the title. Distribution of the implementation review report is the same as for the original report.

#### 1004.13 Performance Measurement

Performance measures of JE inspections include both outcomes and outputs to assess the extent to which objectives are achieved. Objectives will be adjusted to meet new demands and changing conditions, and as a result, outcomes are measured as impacts – recommendations made, implemented recommendations, and/or changes in Agency policy, and outputs are measured as quantities – reviews conducted, reports issued.

#### 1004.14 Working Relationships and Communication

In all matters, JE staff should act in good faith, respecting the mission and priorities of the Agency organization applicable to the inspection, and carry out functions with minimum disruption to the primary work of the reviewed organization.

The Team Lead is the main point of contact. Effective communication may be enhanced by, among other things:

1. Providing reasonable advance notice of inspection activities and requirements;
2. Providing timely advice on the progress of an inspection and its results;
3. Soliciting suggestions for improving the value of inspections; and
4. Providing positive feedback when warranted.

Effective Date 12/15/2014

## 1005.00 OIG QUALITY ASSURANCE

### 1005.01 Federal Manager's Financial Integrity Act

The Federal Manager's Financial Integrity Act of 1982 (FMFIA), codified at 5 U.S.C. § 3512, requires agencies and individual federal managers to take systemic and proactive measures to (i) implement cost-effective internal controls for results-oriented management; (ii) assess the adequacy of internal controls in federal programs and operations; (iii) document internal controls over financial reporting; (iv) identify needed improvements; (v) take corresponding corrective action; and (vi) report annually on internal controls through management assurance statements. To fulfill the FMFIA reporting requirements, the GSA Administrator reports annually to the President.

JE formulates, directs, and coordinates the OIG's FMFIA program, which consists of two cyclic endeavors: the Annual Assurance Statement and the periodic Internal Control Reviews. JE's responsibilities include liaison with the Agency and reporting out on behalf of the OIG for FMFIA matters, as well as overseeing the FMFIA work performed by the OIG components.

### 1005.02 Annual Assurance Statement

As required by the FMFIA, the GSA Administrator reports annually to the President describing compliance with internal control systems, material weaknesses, and action plans to correct material weaknesses for all of GSA. GSA refers to this report as the Administrator's FMFIA Assurance Statement. GSA bases the Administrator's FMFIA Assurance Statement, in part, on the data in assurance statements submitted by GSA's senior managers. As head of an independent office within GSA, the Inspector General provides a statement of assurance on whether (1) the OIG met its major program objectives, (2) the system of internal controls work properly, and (3) the OIG achieved the FMFIA objectives.

### 1005.03 Assurance Statement Responsibilities

JE has responsibility for overseeing the annual assurance statement process across the OIG. Responsibilities include interacting with the Agency as the Inspector General's representative, providing guidance to OIG component heads and their staff on preparing statements, evaluating component submissions, making recommendations to the Inspector General on the content of the annual statement of assurance, and transmitting the Inspector General's signed statement to GSA.

### 1005.04 Assurance Statement Process

To make a recommendation to the Inspector General, JE surveys the OIG's component heads annually on their assessment of the adequacy of management control techniques used in their respective components. The survey requires the component heads to determine whether their respective systems of management control, taken as a whole, achieve the objectives of the FMFIA. The response includes an attestation as to the adequacy of management controls for each component individually. In evaluating the component responses, JE follows-up with the components as necessary.

#### 1005.05 Internal Control Review

Periodically, the Inspector General is required to perform a management control evaluation on OIG program functions. The evaluation, called an internal control review ("ICR"), occurs every three years for the Office of Audits and the Office of Investigations, and every five years for the remaining OIG components. Within the OIG, JE has responsibility for planning and overseeing the OIG ICR.

#### 1005.06 Internal Control Review Responsibilities

During the ICR, each component head has responsibility to perform a detailed review of his or her component, and the results of those reviews become incorporated into the Inspector General's ICR Statement. Components required to perform an internal review will designate a liaison, or an internal control team, to interact with JE throughout the review. The component internal review will incorporate the required seven steps as noted below.

JE has responsibility for ensuring that the components complete their internal reviews, providing detailed guidance and support to the components as needed. JE evaluates the results of the component's review, including supporting materials, and follows up with the components as necessary. In addition to the component's supporting materials, JE assesses whether the component's management controls meet the objectives of the FMFIA.

JE communicates the results of the OIG ICR to the Inspector General and drafts a recommended Inspector General ICR Statement. JE transmits the signed Inspector General ICR Statement to the Agency at the conclusion of the process. JE serves as OIG liaison with the Agency for all matters pertaining to the OIG ICR, including keeping GSA ICR managers apprised of the OIG schedule.

#### 1005.07 Seven Steps of an Internal Control Review

When conducting an internal control review, each component must use the following seven steps:

Step 1 – Planning and Document Review

Step 2 – Defining the Component

Step 3 – Risk Management

Step 4 – Testing Key Controls

Step 5 – Evaluating Results

Step 6 – Recommendations

Step 7 – Reporting and Review Approval

During the course of an ICR, JE will provide detailed guidance on how to conduct each of these steps.

## 1005.08 FMFIA Record Management

The GSA File Plan (schedule 11A045) classifies the FMFIA documentation as Management Improvement Reports, and the OIG follows the Agency's File Plan for these records. Therefore, OIG must retain records it creates in accordance with the retention schedule GSA established. Schedule 11A045 requires custodians to maintain assurance statement records for five years from the end of the fiscal year in which the Agency issues the annual report to the President, and then destroy the records.

## 1005.09 Operational Assessments

The GSA OIG quality assurance function includes internal operational assessments. Operational assessments help to ensure that the OIG organization meets the quality standards applicable to federal Offices of Inspector General, including those prepared by the Council of Inspectors General on Integrity and Efficiency (CIGIE) and the Comptroller General of the United States, as well as the policy requirements of the OIG Manual.

The operational assessments, sometimes called management reviews or operational reviews, form an independent and objective assessment of the field or staff office under review and are conducted at the direction of the Inspector General. Operational assessments impartially evaluate: (1) administrative, managerial, and organizational culture in support of the OIG mission; (2) compliance with quality standards adopted by CIGIE, as well as OIG policies and procedures; and (3) efficiency and effectiveness in meeting mission responsibilities. Operational assessments supplement, but do not replace, line managers' responsibilities. JE keeps the Inspector General, Deputy Inspector General, and Associate Inspector General informed of its quality assurance operations.

## 1005.10 Operational Assessment Procedures

JE conducts operational assessments in phases, as follows:

- **Preparation Phase:** Prior to meeting with the office's management and staff, JE reviews project files (e.g., audit working papers, investigative case files), staffing and personnel actions, as appropriate, prior inspection reports, workload statistics (including performance measures), travel records, purchase card transactions, time and attendance records, financial disclosure forms, performance inspections, and any other information JE deems relevant for the review. JE may also solicit information from the office's senior management and from other OIG components.
- **Fieldwork Phase:** The field work phase may include onsite visits, surveys, data collection and analysis, or other evaluative techniques designed to focus on the office's administration and operations, as well as employee relations issues. During the onsite visit, JE reviews physical layout, equipment inventory, and security. JE also examines staffing activity (training, awards, morale, supervision, and office communications) and administrative activity (time and attendance, travel, and procurement). In addition, JE interviews stakeholders (i.e., representatives from GSA management, U.S. Attorney's Offices, and other law enforcement agencies) as appropriate. During the field work phase, JE endeavors to keep management informed of issues as they arise, to ensure that management has an opportunity to present information, when necessary, to clarify inaccuracies.
- **Reporting Phase.** At the end of the field work, JE holds an exit conference to communicate the results of the operational assessment, including both noteworthy accomplishments and material issues. The

responsible manager may invite subordinate managers to attend the exit conference. JE provides the Inspector General, Deputy Inspector General, and Associate Inspector General a briefing of the assessment results immediately after the field work phase, and provides a written report at the conclusion of the process. JE also communicates an oral summary of the assessment results to the applicable component head, but releases the written report to the respective component's senior management only if authorized by the Inspector General. Those issues needing national attention are reported to the appropriate senior level manager(s).

- Follow-up Phase. When appropriate, JE obtains a plan of corrective action covering deficiencies identified during the review. The corrective plan should include management's actions to remedy deficiencies, a timeline, and desired results. JE reviews adherence to the corrective action plan with a follow-up review, which could include an onsite visit.

#### 1005.10A Operational Assessment Scheduling

JE conducts operational assessments at the direction of the Inspector General, with JE making recommendations based on relevant risk factors. Component heads also may request quality assurance assistance from JE.

JE will notify the component head and office manager (i.e., RIGA, SAC, Director) in advance of a planned review, including proposed dates for the onsite visit. When scheduling the onsite visit, JE should make every attempt to accommodate the component's schedule and other pressing matters.

#### 1005.11 Operational Assessment – Component Assistance

The component head, office manager, and staff of the office under review will cooperate with JE during each phase of the review, including providing prompt, accurate, and complete responses, and providing prompt access to all documentation and information sought. The office manager shall make office space available for dedicated use by the review staff during the onsite visit. Such office space must provide sufficient privacy for sensitive discussions and materials. OIG personnel will meet with the review staff when requested.

JE may request additional OIG personnel to assist with a specific operational assessment, and component heads should provide appropriate staff for this purpose.

#### 1005.12 Questionable Charges and Delinquent Accounts

As part of the OIG quality assurance function, JE administers the OCFO questionable charges and delinquent account inquiries pertaining to OIG purchase cards and travel cards. JE serves as liaison with the Agency for questionable purchase card and travel card matters on the part of OIG employees. For such matters, JE initiates an inquiry within the OIG to determine whether an OIG official authorized the transaction and whether the transaction appears both necessary and for official use. If appropriate, the inquiry also seeks to determine whether corrective action occurred.

#### 1005.13 Questionable Charges and Delinquent Accounts – Initial Inquiry

On a monthly basis, the OCFO notifies the OIG, including JE, of purchase card or travel card transactions identified as questionable and accounts identified as delinquent. JE then requests a response from the

affected OIG component. Each OIG component will identify a point of contact for handling these inquiries, and JE conducts the inquiry through that contact rather than contacting the OIG employee directly.

#### 1005.14 Questionable Charges and Delinquent Accounts – Component Responsibility

Upon receipt of a questionable transaction or delinquent account inquiry, component management must review the report and respond to JE in a timely manner. For questionable transactions, the response must include supporting documentation, indicate whether the transaction was authorized, necessary, and for official business, and if appropriate, whether the component took corrective action. A format for response is provided by OCFO. For delinquent accounts, management's response must include information on whether the employee has paid the account and whether management took appropriate action, such as counseling.

#### 1005.15 Questionable Charges and Delinquent Accounts – Reporting

Once the inquiry has concluded, JE must respond to the Agency. To preserve OIG independence, JE does not provide details on OIG internal matters or the type or manner of corrective action.

Effective Date 12/15/2014

1006.00 RECORDS OFFICER

1006.01 Records Officer

The OIG Records Officer, who serves as liaison with the Agency on record management, is located within JE. The Records Officer provides guidance and assistance OIG-wide on records management issues, including conducting records inventories, adjusting the OIG File Plan, drafting internal OIG policy, arranging appraisal of permanent records, and guiding components on transmitting records to the National Records Center.

Any OIG employee may request record management guidance or assistance from the Records Officer, provided the employee's component authorizes such requests either categorically or on a case-by-case basis.

Effective Date 12/15/2014

## 1007.00 PROJECT INITIATION

### 1007.01 Project Initiation

The Inspector General, Deputy Inspector General, or Associate Inspector General assigns special projects and reviews. Such projects may derive from a Congressional inquiry, OIG Hotline complaint, or other sources. JE frequently develops proactive forensic auditing projects on its own initiative, or in concert with another OIG component or a law enforcement organization. The initiation of an inspection may result from annual planning; management requests; program/process information obtained during an ongoing inspection; or from other sources.

JE may also accept requests for assistance for forensic auditing support from the Office of Investigation, Office of Audits, or Office of Administration provided the project meets the following criteria:

- Falls within the purview of the Inspector General Act of 1978, as amended;
- Involves professional skill sets that exist within JE;
- Would not consume more staff resources than JE has available; and
- In the Director's opinion the project has a strong likelihood of producing a substantial outcome.

The Director (1) approves the initiation of a review, (2) assigns a responsible Senior Management Analyst/Senior Auditor, and (3) assigns the appropriate staff to the project. Once the staff has been assigned, project objectives will be established by the responsible Senior Management Analyst/Senior Auditor in consultation with the Director or Deputy Director. Review objectives may include the following:

- Assessing the adequacy of internal controls including the assessment of risk for fraud, waste, or abuse.
- Assessing the efficiency and effectiveness of programs and operations.
- Providing independently-gathered factual information.
- Supporting audits and/or investigations by performing specific analytical reviews.
- Assessing program results.

Preliminary steps for an inspection project initiation will include:

1. Obtaining a unique project number from the JE case database.
2. Certifying independence.
3. Setting up the project in TeamMate.
4. Determining whether notification to Agency management is necessary and issuing an engagement memorandum if required.
5. Making a determination of whether a formal entrance conference is needed. In general, a formal entrance conference should be held.
6. Determining stakeholder concerns that may need to be included in the review.
7. Gathering information to (1) determine whether the potential issues could have merit, (2) ascertain the complexity of the review and the availability of data, and (3) identify the potential inspection steps and analytical methodologies necessary to achieve the inspection objectives.
8. Engage the JE Evaluations Attorney for any necessary legal research and analysis to identify the legal framework for the inspection.

Effective Date 12/15/2014

## 1008.00 REFERRALS TO THE OFFICE OF INVESTIGATIONS

### 1008.01 Referrals to the Office of Investigations

Using various analytical tools and techniques, forensic examiners determine whether data analyses present indications of fraud, waste or abuse, and refer the suspected activities, subjects, and supporting analysis to the Office of Investigation for consideration. When called upon, the forensic examiner should assist the investigator by formulating language to be included in any subpoena.

Effective Date 12/15/2014

1009.00 INTERAGENCY COMMITTEES AND WORKING GROUPS

1009.01 Interagency Committees and Working Groups

JE fosters an environment of professional development by encouraging staff to participate actively in both intra- and inter-agency committees and working groups. Prior supervisory approval is required for participation in any outside committee or working group.