



governmentattic.org

"Rummaging in the government's attic"

Description of documents: 19 Defense Contract Audit Agency (DCAA) Publications, 1996-2013

Requested date: 11-April-2013

Released date: 03-May-2013

Posted date: 26-August-2013

Source of document: FOIA Request
Defense Contract Audit Agency
ATTN: FOIA Service Center
8725 John J. Kingman Road, Suite 2135
Fort Belvoir, VA 22060-6219
Email: DCAA-FOIA@dcaa.mil

Note: See following page for list of included publications

The governmentattic.org web site ("the site") 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.

Defense Contract Audit Agency (DCAA) Publications Included

DCAA Publication 1403.2	Reduction-In-Force Competitive Areas	July 25, 2000
DCAA Publication 1460.1	Headquarters Telework Policy	December 27, 2002
DCAA Publication 4515.2	Management and Use Of DCAA Staff Cars	April 4, 2006
DCAA Publication 5015.4	Mail Program	May 15, 2000
DCAA Publication 5015.6	DCAA Forms Index	April 6, 2005
DCAA Publication 5030.16	Supporting Congressional Requests for Information	Updated Aug 2001
DCAA Publication 5210.1	Personnel Security Program Manual	March 1, 1996
DCAA Publication 5340.1	Video Information (VI)	July 8, 2002
DCAA Publication 5410.8	DCAA Freedom of Information Act Program	March 13, 2013
DCAA Publication 5410.11	Release of Official Information in Litigation and Testimony by DCAA Personnel as Witnesses	October 5, 2006
(DCAAP 5410.14) DCAA FOIA Processing Guide	DCAA Freedom of Information Act Processing Guide	August 13, 2012
DCAA Publication 5500.4	Coordination of Significant Litigation and Other Matters Involving the Department of Justice	July 20, 2006
DCAA Publication 5500.8	Allegations Against Senior Officials of DoD	February 13, 2008
DCAA Publication 7050.1	Access to DCAA Records and Information by the Inspector General, DoD	June 17, 2010
DCAA Publication 7050.2	Responding to Oversight Reviews	August 28, 2003
DCAA Publication 7640.12	Follow-Up on Oversight Reports and Memoranda Concerning DCAA Operations	June 16, 2011
DCAA Publication 7640.15	Management and Monitoring of Suspected Contractor Fraud and Other Contractor Irregularities Program	June 30, 2006
DCAA Publication 7640.16	Reporting Suspected Contractor Fraud and other Contractor Irregularities	December 23, 2010
DCAA Publication 7640.17	Formal Reporting Procedures for Denial of Access to Contractor's Records	December 19, 2008



IN REPLY REFER TO

**DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE**

8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

CM 502.4
I-13-042-H

May 3, 2013

This letter is a final response to your Freedom of Information Act (FOIA) request dated April 11, 2013 (DCAA FOIA Case Number I-13-042-H). You are requesting a copy of the following records:

DCAA Publication 1403.2
DCAA Publication 1460.1
DCAA Publication 3020.2
DCAA Publication 4515.2
DCAA Publication 5015.4
DCAA Publication 5015.6
DCAA Publication 5030.16
DCAA Publication 5210.1
DCAA Publication 5340.1
DCAA Publication 5410.8
DCAA Publication 5410.11
DCAA Publication 5410.14
DCAA Publication 5500.4
DCAA Publication 5500.8
DCAA Publication 7050.1
DCAA Publication 7050.2
DCAA Publication 7640.12
DCAA Publication 7640.15
DCAA Publication 7640.16
DCAA Publication 7640.17

PDF copies of the records requested are included on the enclosed compact disc and are released to you without redactions. For your information, the DCAA FOIA Processing Guide has replaced DCAAP 5410.14. The DCAA FOIA Processing Guide is enclosed.

For your information, DCAA Manual No. 3020.2 is being withheld in full in its entirety under exemption (b)(2) as it applies to operating rules and guidelines that must remain privileged in order for this Agency to adequately fulfill its mission. The information withheld is related solely to the internal personnel rules of the agency.

Should you disagree with the finding cited above, you may appeal in writing within 60 calendar days from the date of this letter to Mr. J. Philip Anderson, Assistant Director, Resources, at the above address. If you have further questions, please contact the DCAA Information and Privacy Adviser at 703-767-1022.

Sincerely,

A handwritten signature in black ink, appearing to read 'Duane R. Adens', with a horizontal line extending to the right.

Duane R. Adens

Chief

Information and Records Management Branch

Enclosure:

1. I-13-042-H Release Compact Disc

DCAA HI 1403.2

Reduction-In-Force Competitive Areas

JUL 25, 2000

CPO

Reference:

DCAAM 1400.1 Chapter 52, *Reduction in Force*

1. **Purpose.** To establish competitive areas throughout the Headquarters, DCAA for reduction-in-force purposes.
2. **Cancellation.** DCAA HQ Instruction 1403.2, *Reduction in Force*, dated 3 September 1993, is cancelled.
3. **Responsibilities.** The Director, DCAA, has responsibility for establishing competitive areas for the Headquarters, DCAA.
3. **Policy.** DCAAM 1400.1, Chapter 52, provides competitive areas to be established to outline the specific geographical or organizational boundaries within which employees compete in Reduction-In-Force (RIF) actions. Competitive areas are to be large enough to permit adequate competition among employees and limited enough to be administratively manageable. They will be structured to cause a minimum amount of disruption in the work force, minimize the costs of any reduction-in-force, and must be published at least 90 days before the effective date of a reduction-in-force. In accordance with 5CFR, PART 351, (Subpart D) competitive areas require a single administrative authority. In DCAA each region, the Field Detachment and the Headquarters are determined to be separate administrative authorities and their employees are in separate competitive areas.
4. **Procedures.** The enclosure establishes the competitive areas and will include all non-SES employees in the established areas. The enclosure will be updated annually to reflect competitive area changes during the year previous to the date of this instruction.

/Signed/
William H. Reed
Director

Enclosure

Headquarters Competitive Areas

The following competitive areas are applicable to Headquarters employees for both first and second round competition in RIF actions.

<u>Organization</u>	<u>Grade Level</u>	<u>Competitive Area</u>
Headquarters	GS-15 and below	Headquarters-wide (Fort Belvoir Headquarters Complex, VA)
DCAI, OIT & OTS (Field)	GS-15 and below	Commuting area (Memphis, TN)
OAL PLAs & FASC (Field)	GS-14 and below	Washington Metropolitan Commuting areas (Alexandria Arlington, Fort Belvoir, VA Nearby Maryland locations Pentagon, and Washington, D.C.) Aberdeen Proving Ground, MD Albuquerque, NM Aurora, CO Columbus, OH Eglin AFB, FL El Segundo, CA Ft. Drum, NY Ft. Hood, TX Ft. Irwin, CA Ft. Monmouth, NJ

Hanscom AFB, MA

Hill AFB, UT

Houston, TX

Lester, PA

Norfolk, VA

North Charleston, SC

Patuxent, MD

Redstone Arsenal, AL

Richmond, VA

Robins AFB, GA

Rock Island, IL

San Antonio, TX

San Diego, CA

Scott AFB, IL

St. Louis, MO

Tinker AFB, OK

Warren, MI

Wright Patterson AFB, OH



DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

CP
DCAA HQ INSTRUCTION
NO. 1460.1

December 27, 2002

HEADQUARTERS TELEWORK POLICY

References: (a) Department of Defense Telework Policy
(b) Department of Defense Telework Guide
(c) DCAAR 4140.2, Use of Government Office Equipment
(d) DCAA MRD 01-CPP-075(R)

1. **PURPOSE.** This instruction supplements the DoD Telework Policy, the DoD Telework Guide, and the DCAA MRD on Telework Policy, references a., b., and c. The instruction establishes procedures governing the Telework Program at Headquarters.

2. **CANCELLATION.** This instruction cancels MRD 94-D-09(R), dated February 15, 1994, on Flexiplace.

3. **APPLICABILITY AND SCOPE.** This instruction applies to all organizational elements within Headquarters and the Field Detachment.

4. **DEFINITIONS.**

4.1. Telework is any arrangement in which an employee performs officially assigned duties at an alternative work site on either a regular and recurring or on an ad hoc basis.

4.2. Alternative work site is a workplace away from the traditional work site that has been approved for the performance of officially assigned duties. It may be an employee's home, a telecenter, or other approved work site.

4.3. Regular and recurring telework is an approved work schedule where eligible employees regularly work at least one day per biweekly pay period at an alternative work site.

4.4. Ad hoc telework is approved telework at intervals that are less frequent than one day per biweekly pay period. This may include occasional, one-time, or irregular telework by an employee at an alternative work site, typically for a day, or block of days, to work on projects or assignments that can be effectively performed away from the office.

5. POLICY. All Headquarters positions will be considered eligible for ad hoc teleworking with the following exceptions: customer service representatives (CPO); the DCAA security officer, security specialists, and security assistants, (CPS); the mail clerk and driver, (CMO); and, secretaries with floating organizational assignments. All positions in the Field Detachment are ineligible for telework participation due to the classified nature of their work.

The following requirements apply to participation in the Telework Program at Headquarters.

5.1. Employees who participate in the Telework Program will complete the enclosed Telework Self-Certification Safety Checklist and provide it to their supervisor before they begin work at the alternate work site.

5.2. The existing rules on hours of duty apply to employees who participate in the Telework Program. The assigned telework hours can parallel those in the conventional work site or be specific to the alternate work site with the supervisor's approval.

5.3. While working at the alternate work site, employees must be reachable by telephone during their regularly scheduled hours of duty. Employees must provide the telephone number at the alternate work site as a condition of participation in the program. The employee will use the "extended absence greeting" feature on their voice mail indicating the phone number at which they can be reached or the name of another staff member who can be contacted during their absence from the conventional work site.

5.4. If requested by the supervisor, the employee in telework status must be available to report to the conventional work site as the need arises.

5.5. While in telework status, employees will be listed as such, to include listing the phone number where they can be reached, on the daily Personnel Attendance Locator (PAL).

5.6. Situations that lend themselves to participation in the Telework Program on an ad hoc basis may include but are not limited to:

5.6.1. During convalescence from a short-term injury or illness.

5.6.2. When the conventional work site is not usable, e.g., during renovation.

5.6.3. When travel conditions are treacherous and the employee requests to work at home rather than at the conventional work site during those hours when the office is open.

5.6.4. When there is a short-term work assignment that can be performed at an alternate work site free from interruptions.

6. RESPONSIBILITIES.

6.1. The Assistant Director, Resources is responsible for the overall Telework Program.

6.2. The DCAA Telework Coordinator (CPP), under the guidance and supervision of the Chief, Human Resources Management Division (CP), is responsible for:

6.2.1. Providing direction, guidance, training information, and assistance on all telework matters to Agency human resources offices.

6.2.2. Maintaining liaison with the DoD Telework Program Manager and other Federal agencies.

6.2.3. Meeting all external reporting requirements.

6.3. The Headquarters Human Resources Office (CPO), under the guidance and supervision of the Chief, Human Resources Management Division, is responsible for providing guidance to all Headquarters elements on the DCAA Telework Program.

6.4. Heads of Principal Staff Elements (HPSEs) are the approval authority for all requests for participation in the Telework Program originating from the employees in their organizations. Each HPSE must maintain records within their element for periodic and annual reporting requirements to include requests that have been disapproved. During the implementation stages of this program, these records will include: a copy of employee requests with the documented outcome, copies of the signed Self-Certification Safety Checklists submitted by participants, the current number of eligible employees, the number of instances of telework participation within each fiscal year, and the number of disapprovals during the same period.

6.5. Supervisors review telework requests from their employees and make initial determinations of the suitability of the telework proposals and the eligibility of the employees for participation in the program. Suitability determinations are made consistent with the DoD eligibility requirements. Supervisors make recommendations on each case to the HPSE through the usual supervisory chain.

7. PROCEDURES.

7.1. Employees request participation in the Telework Program by submitting a written request to their immediate supervisor. The request will include the dates that the employee proposes to work at the alternate work site, comments, where applicable, on any special circumstances necessitating the request, a description of the specific work to be performed, the location of the alternate work site, e.g., work at home, telecenter, etc., and a completed Self-Certification Safety Checklist.

7.2. Supervisors make the preliminary determination of the employee's suitability for participation in the program based on the employee's work proposal and demonstrated performance. Once the supervisor has made the determination that the work proposal and employee's demonstrated performance are appropriate for telework, the supervisor passes this recommendation through the supervisory chain to the HPSE for approval. Telework requests must be approved by at least a day before the employee intends to telework. Exceptions to prior day approval can be made on a case by case basis.

8. EFFECTIVE DATE. This instruction is effective immediately.

“signed”

Jody A. Trenary
Assistant Director, Resources

Enclosure:
Checklist

Attachment 1

Safety Checklist

SAFETY CHECKLIST	
DoD TELEWORK PROGRAM	
The following checklist is designed to assess the overall safety of the home worksite. The participating employee should complete the checklist, sign and date it, and return it to his or her supervisor (and retain a copy for his or her own records).	
1. Are temperature, noise, ventilation, and lighting levels adequate for maintaining your normal level of job performance?	Yes [] No []
2. Is all electrical equipment free of recognized hazards that would cause physical harm (frayed wires, bare conductors, loose wires or fixtures, exposed wiring on the ceiling or walls)?	Yes [] No []
3. Will the building's electrical system permit the grounding of electrical equipment (a three-prong receptacle)?	Yes [] No []
4. Are aisles, doorways, and corners free of obstructions to permit visibility and movement?	Yes [] No []
5. Are file cabinets and storage closets arranged so drawers and doors do not enter into walkways?	Yes [] No []
6. Are phone lines, electrical cords, and surge protectors secured under a desk or alongside a baseboard?	Yes [] No []

EMPLOYEE'S SIGNATURE _____ DATE _____

NAME: _____ COMPONENT: _____

POSITION: _____

ADDRESS: _____

LOCATION OF DESIGNATED HOME OFFICE OR WORK AREA: _____

HOME TELEPHONE: _____

SUPERVISOR'S NAME: _____

DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

CMA

April 4, 2006

DCAA HQ INSTRUCTION
NO. 4515.2

MANAGEMENT AND USE OF DCAA STAFF CARS

References:

- (a) DoD 4500.36-R, Management, Acquisition, and Use of Motor Vehicles, March 1994
- (b) DoD Instruction 4515.7, Use of Motor Transportation and Scheduled DoD Bus Service in the National Capital Region, July 31, 1985
- (c) FPM Bulletin 930-33, Final Regulations Revising the Identification Requirements for the Federal Motor Vehicle Operator Program

1. REISSUANCE AND PURPOSE. To establish policy, procedures and responsibilities for management, and use of DCAA's official staff cars.

2. CANCELLATION. DCAA HQ Instruction 4515.2, Use of Staff Cars, dated 19 May 1992, is cancelled.

3. APPLICABILITY AND SCOPE. This instruction applies to all Headquarters, DCAA organizational elements located at Fort Belvoir.

4. POLICY:

4.1. It is DoD and DCAA policy that Government-owned or leased motor vehicles shall be FOR OFFICIAL USE ONLY. Official use does not include transportation between residence and place of employment, or to, from, or between locations for the purpose of conducting personal business. It also does not include transportation to or from airport or railroad terminals for temporary duty travel. In addition, it does not include going out and picking up lunch for either themselves or others in the office.

4.2. The Director (D), Deputy Director (DD), and Heads of Principal Staff Elements (HPSEs) are authorized the use of the staff car(s) and driver(s). All other employees may use the staff car(s) on an as-available basis, utilize public transportation, or privately owned vehicles (POV) to conduct official Government business.

4.3. Vehicles, if available, may be used by employees at DCAA Headquarters who possess a valid state driver's license.

4.4. Parking and traffic tickets received while conducting official government business are the personal responsibility of the driver.

4.5. Mail service will be provided on a daily basis between Fort Belvoir, the post office, Pentagon, and IG. Special pick ups or deliveries to or from other metropolitan area locations will be subject to conditions outlined in paragraph below.

5. RESPONSIBILITIES

5.1. The Assistant Director, Resources is responsible for the overall management and administrative control over the use of staff cars.

5.2. The Chief, Acquisition & Administrative Management Branch, under the guidance and supervision of the Chief, Administrative Management Division is responsible for:

5.2.1. Coordinating and providing local transportation requirements for authorized personnel.

5.2.2. Providing guidelines and ensuring the accomplishment of maintenance management, safety, accident prevention and reporting, registration, inspection, and licensing of the staff cars.

5.2.3. Providing mail pickup/delivery services.

5.3. The Heads of Principal Staff Elements are responsible for approving all requests for hand delivery and pick up requests to locations not provided for in this instruction. Hand delivery and pick up requests to locations not provided for in this instruction are subject to driver availability. If a driver is not available, each office will make its own arrangements to meet these needs.

6. PROCEDURES

6.1. Request for Driver Service. When driver service is required, an e-mail should be provided to the Chief, Acquisition & Administrative Management Branch (DCAA-CMA) with a copy to Cheryl Larkin and both the drivers. The e-mail shall contain the names of individuals being driven, the time of departure, the location of meeting, time of pick up, and the name and phone number of a point of contact. The above information will enable CMA to schedule requests.

6.2. Transportation of Personnel. When staff car(s) are not available for transportation of Headquarters personnel, the following modes of transportation may be authorized for travel to perform Agency business:

6.2.1. Metro. A SmartCard will be provided to anyone who needs to travel to a meeting or training.

6.2.2. POV. The use of a POV, with reimbursement for mileage, may be authorized if determined to be advantageous to the Government.

6.2.3. Public Transportation. Use of public transportation, to include taxi cabs (when not on TDY), with reimbursement, may be authorized if determined to be advantageous to the Government.

6.3. Mail Pick up/Delivery

6.3.1. Mail will be picked up/delivered to the Fort Belvoir Post Office and the Pentagon once a day. Fort Belvoir Post Office mail will be picked up in the morning and the Pentagon mail will be picked up in the afternoon.

6.3.2. Hand deliveries shall show office symbol of originating office, complete address and phone number of intended recipient and a phone number for a backup in case they are unavailable.

6.3.3. DCAA employees should notify their counterparts in the Pentagon that DCAA mail should be sent via the U.S. Postal Service or placed in the DCAA mail box in Room 3A948 (OSD Mail Room).

6.4. Automobile Usage Guidelines for Employees.

6.4.1. Each operator shall have a valid Agency identification card as well as state driver's license in his or her possession at all times while driving a government-owned or leased vehicle.

6.4.2. Each vehicle will carry a log book containing a supply of DD Form 1970, Motor Vehicle Utilization Record (enclosure 1). A separate form is completed for each usage day. Each operator will complete the form showing details of usage by that operator.

6.4.3. Drivers are required to adhere to traffic laws and should never double-park, park in fire lanes, handicapped spaces, bus zones, cross-walks, etc. If necessary, park in a commercial garage and submit a claim for reimbursement.

6.4.4. No **eating, drinking, or smoking** is permitted in DCAA vehicles.

6.4.5. Seatbelts will be worn by both driver and passengers at all times.

6.5. Maintenance Management

6.5.1. The DCAA driver(s) will inspect both staff cars located at Fort Belvoir daily to ensure the cars are in safe operating condition and will complete the Vehicle Inspection and Maintenance Schedule Form (enclosure 2) prior to utilization of either vehicle.

6.5.2. The DCAA driver(s) will perform minor service such as replacement of wiper blades, fuses, light bulbs, etc. as well as servicing the water, fuel, oil, and tires for all vehicles.

6.5.3. The DCAA driver(s), or any operator of the vehicles will report any noted deficiencies to CMA. The DCAA driver will schedule appropriate repair/maintenance as soon as authorization is granted by CM/CMA.

6.5.4. When servicing is to be performed by other designated personnel, they are responsible for ensuring services are performed, and that the vehicles are in safe and serviceable operating condition before, during, and after operation.

6.5.5. The DCAA driver(s) will arrange for a wash and vacuum of all the DCAA vehicles on an as requested or as needed basis.

6.5.6. The DCAA driver shall ensure a supply of accident reporting forms is in each vehicle at all times.

6.5.7. A spare set of keys for each staff vehicle will be held by the DLA Security Office.

6.6. Scheduled Inspection and Service

6.6.1. The DCAA driver will arrange for and accomplish, at an appropriate maintenance facility, the inspection of each staff car for safety at intervals not to exceed 12 months. Safety inspections shall comply with state and local safety inspection intervals.

6.6.2. A tune-up must be performed at least once every 12,000 miles or 12 months, whichever occurs first, or in accordance with manufacturer's recommendation.

6.6.3. An oil change must be performed at least every 3,000 miles or 6 months, whichever occurs first, or in accordance with manufacturer's recommendation.

6.6.4. Maintenance procedures for vehicles leased from GSA's Fleet Management System shall be in accordance with GSA instructions.

6.7. Registration and Licensing of Staff Cars

6.7.1. Each staff car will be registered and licensed with Government tags.

6.7.2. Vehicles leased under a purchase order shall be registered and tagged by the vendor. CMA will purchase Government tags from UNICOR.

6.7.3. CMA will maintain a current record of all official Government tags in use. Such records shall specify, by type and registration number, the motor vehicle to which the tags are assigned, and shall include information regarding all subsequent reassignment of tags and void tag numbers.

6.8. Safety and Emergency. Each staff car will have a First Aid Kit and an Emergency Road Kit.

6.9. In Case of an Accident. Drivers involved in an accident shall:

6.9.1. Stop immediately.

6.9.2. Call police.

6.9.3. Render assistance to any injured person(s). Injured persons shall not be moved unless absolutely essential for their protection.

6.9.4. Warn other motorists of any existing highway hazard. During hours of darkness or poor visibility, flares or reflectors shall be used.

6.9.5. Not express opinions (orally or in writing) to claimants or their agents concerning liability, investigation findings, or the possibility of a claim approval.

6.9.6. Not leave the accident scene except as authorized by state/local law officials or other proper authorities.

6.9.7. Complete SF 91, Operator's Report of Motor Vehicle Accident (enclosure 3), Optional Form 26, Data Bearing Upon Scope of Employment of Motor Vehicle Operator (enclosure 4), and SF Form 94, Statement of Witness (enclosure 5), if appropriate. If these forms cannot be completed by the driver because of injury or death, the report shall be completed by the next senior person directly responsible for motor vehicle operation.

6.9.8. Comply with state and local laws governing the reporting of vehicle accidents. Forms SF 91 and Optional Form 26 shall be submitted to CMA which will process the accident report to include coordination through DCAA DL for review to ensure that the rights of the U.S. Government are not prejudiced by an admission of liability which may obligate the Government.

6.9.9. Obtain clearance from DL prior to releasing any accident reports to a third party including state and local governments. Drivers shall not make official accident investigation reports available to a claimant or to any individual or representative of any non-DoD organization.

6.9.10. Deliver the completed SF 91 and Optional Form 26 to his/her supervisor to be forwarded to CMA as soon as possible thereafter.

7. EFFECTIVE DATE: This instruction is effective immediately.

FOR THE DIRECTOR:

/s/

J. Philip Anderson
Assistant Director, Resources

Enclosures (4)

1. DD Form 1970, Motor Equipment Utilization Record
2. Daily Vehicle Inspection and Defect Report
3. SF Form 91, Motor Vehicle Accident
4. SF Form 94, Statement of Witness

DCAAR 5015.4

Mail Program

MAY 15, 2000

CM

- 1. Purpose.** Establish the policies governing the Mail Program.
- 2. Cancellation.** The 23 January 1995 edition of this regulation is cancelled.
- 3. Applicability and scope.** Applies to all organizational elements in DCAA.
- 4. Policy.** Agency policy prescribes compliance with those cited in DoD 4525.8-M. All transactions with USPS must be by cash, check, or Advance Deposit Trust Account (ADTA) using prepaid "commercial" postage. Appropriated fund postage may be used to pay postage on bill payments resulting from official travel charges on credit cards issued under the Travel and Transportation Expense Program established by the General Services Administration (GSA).
- 5. Responsibilities.**
 - 5.1.** The Assistant Director, Resources, has overall responsibility for the mail program.
 - 5.2.** The Chief, Administrative Management Division serves as the Agency Official Mail Manager (OMM), and is responsible for the accomplishment of the responsibilities identified in paragraph C of DoD 4525.8-M.
 - 5.3.** The Chief, Operating Administrative Office (CMO), serves as the Official Mail Manager for the Headquarters and performing the duties outlined in DoD 4525.8-M. The Mail Manager will prepare and submit the Semi-annual Report of Prepaid Postage to Headquarters, CM, and be responsible for authorizing overnight mail services using DCAA Form 5015-4.
 - 5.4.** Heads of Principal Staff Elements are responsible for preparing Agency mail in accordance with the policies and procedures outlined in DoD 4525.8-M, and appointing individual(s) to be responsible for authorizing overnight mail services using DCAA Form 5015-4.
 - 5.5.** The Regions and Field Detachment will designate a Mail Manager to manage their mail program in accordance with DoD 4525.8-M, and appoint individual(s) to be responsible for authorizing overnight mail services using DCAA Form 5015-4. The Mail Manager will prepare and submit the Semi-annual Report of Prepaid Postage to Headquarters, CM.
 - 5.6.** Field Audit Offices will manage their mail program in accordance with DoD 4525.8-M.

6. Address Format and Style. In addition to the requirements outlined in DoD 4525.8-M, mail addresses (both delivery and return) should be typed and will be limited to five lines. Each line will be limited to a maximum of 47 characters (including spaces). However, addresses for the DCAA Directory of Offices or for labels printed from AMIS will be limited to a maximum of 35 characters (including spaces). This format, as shown below, does not authorize the printing of envelopes for each staff office.

X X X X X X X X X X	-- Office name line
X X X X X X X X X X	-- Optional line
X X X X X X X X X X	-- Name of DoD Activity
Street address, Suite Number or PO Box Number	-- Delivery address line
City State ZIP + 4 Code	-- Last line

7. Use of USPS Express Mail and Private "Overnight" Couriers. DCAA Form 5015-4, **DCAA Overnight Mail Service Request Form for Mission Critical Items**, should be used for requesting and justifying overnight services.

8. Use of Facsimile (FAX) Machines or Electronic Mail. If correspondence needs to move quickly, is not voluminous, and is not classified, it should be faxed or sent electronic mail. If an item has been sent by fax or electronic mail, it should not be otherwise sent by the mail service.

9. Handling Instructions for Sensitive Mail. Sensitive Mail should be opened **Only** by the addressee.

10. Express Mail Limitations. DCAA personnel are not permitted to use USPS Express Mail for transmission of any classified information.

11. Effective Date. This regulation is effective immediately.

/Signed/

William H. Reed

Director

Enclosure

DoD 4525.8-M (<http://web7.whs.osd.mil>)

DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

CM

April 6, 2005

DCAA PAMPHLET
NO. 5015.6

DCAA FORMS INDEX

This pamphlet is designed to identify DCAA forms, available only in hard copy format, that have been prescribed or approved for use by all or certain DCAA activities. None of the forms listed in this publication have been automated. DCAA forms that have been converted to an electronic format are available on the LAN as part of our inventory of electronic forms. Users should refer to the electronic forms menu for a complete listing of DCAA forms. The electronic forms inventory is updated quarterly as part of the regularly scheduled DIIS updates.

FORM NO.	TITLE	EDITION DATE	OPR	PRESCRIBING DIRECTIVE
1000-2	Signature - Coordination Tabs	09/91	CM	M 5020.1
1441-6	Performance Award Certificate (Overprinted)	11/91	CPP	M 1400.1
1441-7	Performance Award Certificate	11/91	CPP	M 1400.1
1441-8	Superior Accomplishment Award	11/91	CPP	M 1400.1
1441-9	Suggestion Award Certificate	11/91	CPP	M 1400.1
1441-10	Certificate of Appreciation	11/91	CPP	M 1400.1
1441-11	Certificate of Service	11/91	CPP	M 1400.1
1441-12	Distinguished Civilian Service Award	11/91	CPP	M 1400.1
1441-13	Meritorious Civilian Service Award	11/91	CPP	M 1400.1
5210-8	Auditor Credentials	08/86	CPS	R 5000.3
5210-8-1	Special Credentials	12/72	CPS	R 5000.5

This issuance replaces DCAA Pamphlet 5015.6, dated June 2004, published in electronic format only, which is obsolete.

/s/

Jody A. Trenary
Assistant Director, Resources

DCAAR 5030.16

Supporting Congressional Requests for Information

**(Updated Aug 2001)
JUL 25, 2000**

**DEFENSE CONTRACT AUDIT AGENCY
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219**

PAS

References:

(a) DoD Directive 5400.4, *Provision of Information to Congress*, 30 January 1978
<http://web7.whs.osd.mil>

(b) DoD Instruction 5500.16, *Relationship with the Surveys and Investigations Staff, House Appropriations Committee*, 21 October 1996 <http://web7.whs.osd.mil>

1. Purpose: This regulation implements references (a) and (b) (enclosures), and provides guidance for (1) processing congressional inquiries, including requests for submission of audit reports, (2) handling visits by congressional committees or their staffs, and (3) preparing material for use before congressional committees.

2. Cancellation. DCAA Regulation 5030.16, dated 23 July 1996, is superseded and canceled.

3. Applicability and Scope.

3.1. This regulation applies to all organizational components of DCAA.

3.2. Excluded from the scope of this regulation are:

3.2.1. Preparation and Processing of Legislation, Executive Orders, and Proclamations. (See DCAAR 5020.3, same subject.)

3.2.2. Matters relating to appropriations which fall under the cognizance of the Under Secretary of Defense (USD)(Comptroller).

4. Policy.

4.1. It is the policy of the Department of Defense and the DCAA to make information concerning DCAA operations and activities available to members of Congress, congressional committees, and their staffs. All material prepared for or presented to congressional committees or their staffs will be factual, completely responsive, and submitted in a timely manner through Headquarters. Congressional committees and their staffs visiting DCAA offices will be accorded the proper courtesy and respect, and provided working space and facilities for their activities. This policy is subject to the limitations described in DoD Directive 5400.4, and other limitations, summarized in section 4.2.

4.2. Limitations Indicated by DoD Directive 5400.4.

4.2.1. Information with a security classification in the interest of national defense must be properly safeguarded and will be furnished to members of Congress, committees, and their staffs in accordance with established security procedures only by or with permission of the Director or Deputy Director, DCAA, when the information is needed to enable Congress to perform its Constitutional function.

4.2.2. Information designated "For Official Use Only" (FOUO) must be protected from disclosure to the general public. Access is provided to Congress in confidence, since use by Congress is needed to enable it to perform its constitutional function.

4.2.3. In some cases, questions may arise as to whether security classified, FOUO, or other material, may be made available to Congress, even in confidence. Such cases may involve the following situations:

4.2.3.1. Information which would unduly interfere with the performance of functions of the DCAA or some other department or agency of the Government, including but not limited to such functions as pending litigation, maintenance of discipline, conduct of investigations, and conduct or relations with foreign governments.

4.2.3.2. Information recognized as privileged under the Privacy Act, Freedom of Information Act, or other statutory or legal authority. For example, certain non-factual information, such as the recommendations and conclusions in Inspector General reports and special investigations reports, is generally considered privileged information. (DCAAR 5410.8 and DCAAR 5410.10)

4.2.3.3. Information which might result in injury to an innocent person, such as unsubstantiated allegations derogatory to the character or conduct of the individual.

4.2.3.4. Information whose release is restricted under DoD Instruction 5500.16, 5.10. (See Enclosure 2.)

4.2.3.5. Information documenting interim DCAA positions on issues, including interim or preliminary audit findings and recommendations, which have not progressed through DCAA's management review and approval process.

4.2.3.6. Information that was not originated by DCAA, unless approval to release the information to Congress is received from the originator.

4.2.3.7. Information relating to or derived from the DoD Program Objective Memorandum (POM). This information is considered to be interim guidance and not releasable outside DoD.

5. Responsibilities.

5.1. Headquarters.

5.1.1. The Auditing Standards Division is responsible for Agency compliance with the provisions of DoD Directive 5400.4 and DoD Instruction 5500.16. The Auditing Standards Division will:

5.1.1.1. Process all congressional inquiries and requests for audit reports and other information, other than those pertaining to legislation, executive orders, and proclamations. (Such inquiries will be processed by the General Counsel, DCAA, in accordance with the provisions of DCAAR 5020.3.)

5.1.1.2. As necessary, notify the Assistant Secretary of Defense (Legislative Affairs) (ASD(LA)) and the USD (Comptroller) of all congressional requests for information or briefings, requests to visit DCAA facilities, and requests to testify before congressional committees when the congressional request was received directly by DCAA. ASD(LA) has overall responsibility for such congressional activity and shall be furnished copies of all direct written communications to and from Congress regarding such requests.

5.1.1.3. Coordinate the preparation of material and/or testimony to be presented to congressional committees and monitor the status of transcripts.

5.1.1.4. Coordinate the material with the appropriate elements of the Office of the Secretary of Defense (OSD), the services, and non-DoD departments or agencies.

5.1.1.5. Ensure DCAA compliance with the requirements of congressional committees relating to the presentation of material or testimony.

5.1.1.6. Provide the proposed testimony and required transmittal forms for appropriate departmental coordination as soon as possible before the scheduled hearing.

5.1.1.7 For testimony requested by Congress or the ASD(LA), ensure that all written testimony prepared for submission to the Congress by the Director, DCAA, together with a one-page analysis, is provided to the ASD(LA) no later than 72 hours prior to the hearing. Written testimony to be presented by subordinate witnesses may also be provided to the ASD(LA) at DCAA's discretion. The analysis should include:

- stated purpose of the hearing;

- items of interest for the Committee/Subcommittee or individual members of Congress; and
- contentious issues or those that may generate broad public interest.

5.1.2. The Heads of the Principal Staff Elements will, within their respective areas, prepare or review requested information or testimony for presentation to congressional committees and will submit it to the Auditing Standards Division.

5.1.3. The Director or Deputy Director will provide final approval of all requested information or testimony prepared for presentation to congressional committees.

5.2. Regions.

5.2.1. Regional Directors will notify Headquarters of all congressional requests for information (requests made directly to DCAA or known requests for DCAA-generated materials made to a DCAA customer) or pending visits by congressional members or their staffs.

5.2.2. When requested by Headquarters, Regional Directors and staff elements will prepare and/or review requested information or testimony for presentation to congressional committees.

5.3. Field Audit Offices.

FAO managers will inform Regional Directors of all congressional requests for information (requests made directly to DCAA or known requests for DCAA-generated materials made to a DCAA customer) or of pending visits by congressional members or their staffs.

6. Procedures.

6.1. Congressional Requests for Written Information.

6.1.1. Headquarters.

6.1.1.1. Congressional inquiries received in Headquarters, including requests for audit reports, will be forwarded immediately to the Auditing Standards Division.

6.1.1.2. The Auditing Standards Division (PAS) will:

6.1.1.2.1. Discuss the need for a written request for any data requested orally with the Assistant Director, Policy and Plans (P). If appropriate, PAS will request that the inquiry be furnished in writing.

6.1.1.2.2. For requests for information and/or material not originated by DCAA, suggest that the requestor obtain the information directly from the originating organization. If this fails, PAS will seek permission from the originator to release the material to Congress.

6.1.1.2.3. Review the inquiry and recommend to P which major staff element should be responsible for preparing a reply. Designate the appropriate Headquarters signing official, and establish a due date by which the responsible staff element is to prepare the reply. Although a matter of judgment in each case, correspondence related to legislative/legal, resources, audit operations, or audit policy matters may be prepared for the signature of General Counsel (DL) or the Assistant Directors for Resources (C), Operations (O), or Policy and Plans (P), respectively, when signing by the Director is not required. The Director (or in his absence the Deputy Director) normally will sign the response when major policy or operational matters are involved; when the subject is of direct interest to the SecDef, DepSecDef, or Comptroller; and when the matter is highly sensitive to DoD, DCAA, or client agencies.

6.1.1.2.4. Hand carry inquiries pertaining to existing or proposed legislation, executive orders, or proclamations to Defense Legal Services for process in accordance with DCAAR 5020.3.

6.1.1.2.5. When Congressional correspondence is received directly by DCAA, acknowledge the request and indicate when the information will be provided. When congressional correspondence is referred to DCAA for staff action by the Secretary of Defense or the Deputy Secretary of Defense, PAS will initiate whatever action is required. When the action to be taken is the preparation of a direct reply, PAS will complete a **Secretary of Defense Correspondence Action Report** (SD Form 391, furnished with the request) and forward it together with a copy of DCAA's response to the Correspondence Control Division (CCD), Washington Headquarters Services. If a reply cannot be provided within a reasonable length of time (no more than thirty days), when received direct, or by the OSD established due date when referred by OSD, an immediate interim reply will be prepared advising the requestor of a date by which the information will be supplied. A copy of the interim reply, together with a copy of SD Form 391, or other correspondence control form furnished with the referral, setting forth the justification for the delay shall be sent to the Correspondence Control Division (CCD) for OSD referrals.

6.1.1.2.6. Ensure that replies to congressional inquiries, including requests for audit reports, are timely and completely responsive.

6.1.1.2.7. If classified materials are being disclosed, coordinate transmittal letters with the DCAA Security Officer to ensure that appropriate statements are included regarding required security precautions governing the handling and disclosure of such materials.

6.1.1.2.8. Ensure the appropriate coordination of the proposed response. The Auditing Standards Division will coordinate the response with elements of the Office of the Secretary of Defense (OSD), the services, and non-DoD departments or agencies as necessary.

6.1.1.2.9. Inform the responsible staff element when coordination has been completed.

6.1.1.3. The head of the responsible staff element, as determined in accordance with paragraph 6.1.1.2.3, will:

6.1.1.3.1. Gather any necessary information from the appropriate sources, e.g., available files or Headquarters and regional staff elements.

6.1.1.3.2. Prepare a proposed response.

6.1.1.3.3. Coordinate the response with both the appropriate Headquarters staff elements and the affected regional office(s). When responses involve sensitive personnel matters, the information should be protected and the coordination should be limited to only those who have a need to know.

6.1.1.3.4. Furnish the proposed response to the Auditing Standards Division for coordination with the appropriate DoD elements. PAS will notify the Head of the responsible staff element when the coordination has been completed.

6.1.1.3.5. After signature, provide a copy of the response to the affected regional office(s) and to PAS for clearance of the suspense control.

6.1.2. *Regional Directors.*

6.1.2.1. Regional Directors will notify Headquarters, ATTN: PAS, of all congressional requests for information or pending visits by members of Congress or their staffs. Written requests for information received from members of Congress or their staffs should be forwarded to Headquarters for evaluation as expeditiously as possible.

6.1.2.2. When requested by Headquarters, Regional Directors will provide the following information to the responsible staff element as expeditiously as possible but no later than the date established in accordance with paragraph 6.1.1.2.3.

6.1.2.2.1. The requested material or audit report(s), along with a notification that the contracting officer has been informed that DCAA intends to release the report(s).

6.1.2.2.2. A proposed substantive reply to the inquiry or, if appropriate, comments to accompany the audit report.

6.1.2.2.3. Facts upon which the substantive reply or comments are based. This should include an assessment of compliance with Agency policy and any impact on audit operations or resources.

6.1.2.3. If release of the information is limited in accordance with section 4.2., the Regional Director will provide appropriate comments and recommendations in the communication forwarding the congressional request to Headquarters. If the requested information was not originated by DCAA, the communication should identify the originator of the material.

6.1.2.4. When a proposed substantive reply, or comments to accompany the audit report, cannot be forwarded to the responsible staff element within the date established under paragraph 6.1.1.2.3, the Regional Director will forward a brief memorandum stating the anticipated date that the information will be furnished and the steps being taken to obtain the information requested.

6.1.3. *Regions and Field Audit Offices.*

Regional and FAO personnel, upon receipt of a congressional inquiry or request for an audit report or other information, will immediately notify the Regional Director and provide the facts necessary for preparation of a completely responsive reply (including a copy of any requested audit report) or an estimate of the time necessary to gather the necessary facts. The written inquiry or request and related correspondence, including a copy of the audit report and a copy of the letter notifying the ACO of DCAA's intention to release (6.2.2.5) should be forwarded to the Regional Director and a copy provided to Headquarters, Attn: PAS.

6.2. Meetings With and Visits Made by Congressional Committees or their Staffs.

Normally, DCAA Headquarters will receive advance notification of a congressional request to provide a briefing or a pending visit by a congressional committee or its staff. In such cases the DCAA office concerned will be notified and requested to make arrangements to assist the committee.

6.2.1. Headquarters.

6.2.1.1. Heads of Principal Staff Elements receiving a written congressional request to provide a briefing or a notice of a pending visit by a congressional committee or its staff will provide the Director and the Auditing Standards Division with a copy of the written request. All verbal requests for briefings or verbal notices of a pending visit will be coordinated with the Assistant Director, Policy and Plans for determination as to whether a written request should be obtained.

6.2.1.2. PAS will immediately notify the ASD (LA) of any congressional requests for briefings or requests to visit regional or field offices. PAS will provide copies of written requests from congressional committees or their staffs to the ASD (LA).

6.2.1.3. Immediately following a congressional visit to Headquarters, the head of the principal staff element will furnish the Director a memorandum summarizing the matters discussed, opinions expressed, records furnished, and conclusions reached. A copy will be furnished to the Auditing Standards Division.

6.2.2. Regions and Field Audit Offices.

6.2.2.1. Regional Directors will immediately notify the Director if regional or field offices receive a written congressional request to visit a DCAA office. A copy of the request will also be provided to Headquarters, Attn: PAS. Oral requests to visit a DCAA office should be referred to Headquarters, Attn: PAS.

6.2.2.2. Regional and field personnel will permit committee members or their staff to examine records which concern their areas of interest or directly pertain to their investigation and are not excluded by paragraph 4.2. Requests to examine, retain, or remove records covered by paragraph 4.2. will be referred to Headquarters, Attn: PAS, for resolution. The material will be made available in the working space provided for the committee's convenience. A DCAA representative will be available at all times to render any needed assistance.

6.2.2.3. Regional Directors will refer committee requests to remove or retain records (including audit reports and working papers), or copies of them, to Headquarters, PAS, as expeditiously as possible. Advise the requestor that action to process such requests will be taken promptly and that copies of requested records will be forwarded to Headquarters for the appropriate coordination and transmission to the committee's offices in Washington, DC.

6.2.2.4. Regional Directors will forward a memorandum summarizing visits by congressional representatives to Headquarters, Attn: PAS, within five working days following the visit. The memorandum should specifically enumerate the subjects discussed during the visit, any requests for data, and questions to be answered. If the committee has made a request for audit reports or working papers, the memorandum should also include an assessment of the requested materials' compliance with Agency policy and any impact on audit operations or resources.

6.2.2.5. Regional Directors will forward to Headquarters, PAS, any information requested by committee representatives within ten working days following the visit. When audit reports are requested, a statement should be included that the contracting officer has been informed that we intend to release the report. If the information requested by the committee representatives cannot be furnished to Headquarters within ten working days, the report of the visit should briefly explain the reasons and set forth a specific date.

6.3. Testifying before Congressional Committees.

6.3.1. When a representative of DCAA expects to appear as a witness before a congressional committee he/she will obtain prior authority from the Director.

6.3.2. DCAA personnel testifying as witnesses before congressional committees will properly safeguard information which is classified in the interest of national defense, and will furnish this information to Congress only in accordance with established security procedures and with the permission of the Director, DCAA. This also applies to furnishing "*For Official Use Only*" information.

6.3.2.1. If the material is to be submitted in writing, it will contain an overall classification to designate the degree of security protection necessary.

6.3.2.2. If the Director has authorized a witness to furnish such information orally, the witness will inform the committee of the nature of the information and the need for protecting it from public dissemination, and will respectfully request that the testimony be given in closed session and that it not appear in the record of the hearings, the Congressional Record, or other documents open to public inspection.

6.3.3. In the rare case where there is a question as to whether particular information may be furnished to a committee of Congress, even in confidence, it will normally be possible to satisfy the request through some alternate means acceptable to both the requestor and DCAA. In the event that an alternate reply is not acceptable, no final refusal to furnish such information shall be made, except with the express approval of the Director, DCAA or the Secretary of Defense. The Assistant to the Secretary of Defense (Legislative Affairs) (ASD(LA)) will be informed of

such action. A final refusal to a committee of Congress may be made only with the concurrence of the ASD(LA), who shall be responsible for ensuring compliance with all procedural requirements imposed by the President or pursuant to his direction.

7. *Effective Date.* This Regulation is effective immediately. Copies of any implementing instructions shall be provided to Headquarters, Attn: PAS, upon issuance.

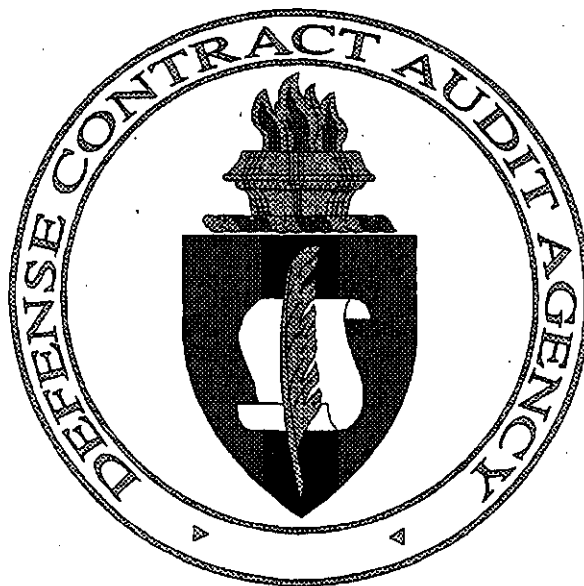
/Signed/
William H. Reed
Director

Enclosures 2

1. DoDD 5400.4 <http://web7.whs.osd.mil>
2. DoDI 5500.16 <http://web7.whs.osd.mil>

DCAAM 5210.1
March 1996

Personnel Security Program Manual



**DEPARTMENT OF DEFENSE
DEFENSE CONTRACT AUDIT AGENCY**



DEFENSE CONTRACT AUDIT AGENCY
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

CPS

March 1996

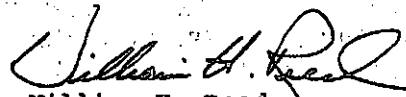
DCAA MANUAL
No. 5210.1

FOREWORD

This manual is issued pursuant to section D.3, DoD Directive 5200.2, "DoD Personnel Security Program," and section 11-101.c, DoD 5200.2-R, "DoD Personnel Security Program Regulation". Its purpose is to implement the DoD Personnel Security Program within DCAA by furnishing DoD 5200.2-R, in its entirety, supplemented only as necessary by instructions and policies to adapt it to DCAA operations and requirements. This manual also implements DoD Directive 5240.6, "Counterintelligence Awareness and Briefing Program."

This manual is mandatory for use by all DCAA organizational elements. Regional directors and the Director, Field Detachment, may issue supplementary instructions when necessary to provide for internal administration of this manual within their respective organizational elements. However, any such instructions must be approved by the Agency Headquarters prior to issuance.

Recommendations for changes to this manual should be addressed to the Agency Security Officer; Headquarters, DCAA; 8725 John J. Kingman Road, Suite 2135; Fort Belvoir, Virginia 22060-6219.


William H. Reed
Director

DISTRIBUTION:

C, G, P

OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

POLICY

DECEMBER 16, 1986

FOREWORD

THIS "PERSONNEL SECURITY PROGRAM REGULATION" IS REISSUED UNDER THE AUTHORITY OF DOD DIRECTIVE 5200.2, "DOD PERSONNEL SECURITY PROGRAM," DECEMBER 20, 1979. IT CONTAINS EXPANDED DIRECTION AND PROCEDURES FOR IMPLEMENTING THOSE REFERENCES CITED IN CHAPTER 1 AND IN APPENDIX A OF THIS REGULATION THAT PERTAIN TO ACCEPTANCE AND RETENTION OF DOD MILITARY, CIVILIAN, CONSULTANT AND CONTRACTOR PERSONNEL AND OF GRANTING SUCH PERSONS ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO A SENSITIVE POSITION. IT ALSO IMPLEMENTS SUCH RECOMMENDATIONS FROM THE DEFENSE SECURITY REVIEW COMMISSION REPORT AS PERTAINS TO PERSONNEL SECURITY AND APPROVED BY THE SECRETARY OF DEFENSE.

DOD 5200.2-R, "DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM," DECEMBER 1979, IS HEREBY CANCELED AS OF DECEMBER 31, 1986. THE EFFECTIVE DATE OF THIS REGULATION IS JANUARY 1, 1987.

THE PROVISIONS OF THIS REGULATION APPLY TO THE OFFICE OF THE SECRETARY OF DEFENSE (OSD) AND ACTIVITIES SUPPORTED ADMINISTRATIVELY BY OSD, THE MILITARY DEPARTMENTS, THE ORGANIZATION OF THE JOINT CHIEFS OF STAFF (OJCS), THE UNIFIED AND SPECIFIED COMMANDS, AND THE DEFENSE AGENCIES.

THIS REGULATION IS MANDATORY FOR USE BY ALL DOD COMPONENTS. HEADS OF DOD COMPONENTS MAY ISSUE SUPPLEMENTARY INSTRUCTIONS WHEN NECESSARY TO PROVIDE FOR INTERNAL ADMINISTRATION OF THIS REGULATION WITHIN THEIR RESPECTIVE COMPONENTS.

FORWARD COMMUNICATIONS, INCLUDING RECOMMENDED CHANGES, REGARDING THIS REGULATION AND COPIES OF SUPPLEMENTAL INSTRUCTIONS ISSUED, THROUGH APPROPRIATE CHANNELS TO: DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY, ATTENTION: DIRECTOR COUNTERINTELLIGENCE AND INVESTIGATIVE PROGRAMS, ROOM 3C-267, THE PENTAGON, WASHINGTON, D.C. 20301-2200.

THIS REGULATION IS BEING PUBLISHED IN TITLE 32, CODE OF FEDERAL REGULATIONS (CFR). DOD COMPONENTS MAY OBTAIN COPIES OF THIS REGULATION THROUGH THEIR OWN PUBLICATIONS CHANNELS. FEDERAL AGENCIES AND THE PUBLIC MAY OBTAIN COPIES FROM THE U.S. DEPARTMENT OF COMMERCE, NATIONAL TECHNICAL INFORMATION SERVICE, 5285 PORT ROYAL ROAD, SPRINGFIELD, VA 22161.

/s/
CRAIG ALDERMAN, JR.
DEPUTY

INTRODUCTION

I. REISSUANCE AND PURPOSE

The DCAA Personnel Security Manual is the official Agency publication for (1) transmitting the DoD Personnel Security Program Regulation, DoD 5200.2-R, and all changes thereto, to all DCAA field elements; (2) providing detailed operating procedures and guidance to the DoD regulation; and (3) providing a consolidated implementation of other DoD directives related to personnel security, but not incorporated in the above cited regulation.

II. SCOPE

a. The portion of this manual printed in **SOLID CAPITAL LETTERS** is DoD 5200.2-R, DoD Personnel Security Program Regulation, including all changes.

b. The portion of this manual in bold print supplements the DoD regulation only where it is necessary to adapt these requirements to the DCAA organizational structure and operational conditions. Where no adaptation is considered necessary, refer and adhere to portions printed in **SOLID CAPITAL LETTERS** in this manual.

c. Regional operating instructions issued to supplement the requirements of this manual to the organizational structure and operational conditions of the regions will be forwarded within 120 days to CPS for approval prior to implementation.

III. FORMAT

The manual is to be maintained in loose leaf form. Revisions will be issued as replacement pages for existing pages, or as new pages to cover material not previously issued. Revised pages will be dated in the upper right corner; e.g., "CH1, Jan 1999."

IV. DISTRIBUTION

a. The DCAA Personnel Security Program Manual is distributed to CPS, the Director, Field Detachment, and regional directors' offices, and through these offices, to each DCAA office. Normal distribution is one copy to each office.

b. While the manual is intended primarily for use by Agency officials directly responsible for the application and retention of DCAA employees in sensitive positions and granting such employees access to classified information, it should be available to all Agency employees who are required to be generally familiar with its contents.

V. IMPLEMENTATION

This manual has been designed to minimize the necessity for its users to refer to other publications for technical or procedural guidance, and to achieve maximum uniformity in local implementation. Therefore, as indicated in II.c, above, proposed regional implementing instructions will be forwarded to the Agency Headquarters, ATTN: CPS, for review prior to publication.

VI. CANCELLATION

DCAA Regulation 5210.1 dated 2 November 1992 is hereby canceled. DCAA Manual 5210.1, Personnel Security Program, dated January 1989, and its changes 1, 2, 3, 4, and 5, dated 6 July 1989, 2 October 1991, 5 November 1993, 9 September 1993, and 6 December 1994, respectively, are hereby canceled. All changes to the parent document, DoD 5200.2-R, up to and including Change 3 of 1 November 1995, have also been included. Change 3 to 5200.2-R, and changes in implementing DCAA guidance, are highlighted by vertical lines in the margins of this manual.

DEPARTMENT OF DEFENSE PERSONNEL SECURITY
PROGRAM REGULATION

INDEX

CHAPTER I

Section 1

REFERENCES

<u>Paragraph</u>	<u>Page</u>
1-100 References.....	I-1

Section 2

PURPOSE AND APPLICABILITY

1-200 Purpose.....	I-2
1-201 Applicability.....	I-3

Section 3

DEFINITIONS

1-300 Access.....	I-3
1-301 Adverse Action.....	I-3
1-302 Background Investigation (BI).....	I-4
1-303 Classified Information.....	I-4
1-304 Defense Clearance and Investigations Index (DCII).....	I-4
1-305 DoD Component.....	I-4
1-306 Entrance National Agency Check (ENTNAC).....	I-4
1-307 Head of DoD Component.....	I-4
1-308 Immigrant Alien.....	I-4
1-309 Interim Security Clearance.....	I-4
1-310 Limited Access Authorization.....	I-5
1-311 Minor Derogatory Information.....	I-5
1-312 National Agency Check (NAC).....	I-5
1-313 National Agency Check Plus Written Inquiries (NACI).....	I-5
1-314 National Security.....	I-5
1-315 Need-to-know.....	I-5
1-316 Periodic Reinvestigation (PR).....	I-5
1-317 Personnel Security Investigation (PSI).....	I-5
1-318 Scope.....	I-6
1-319 Security Clearance.....	I-6
1-320 Senior Officer of the Intelligence Community (SOIC).....	I-6
1-321 Sensitive Position.....	I-6
1-322 Significant Derogatory Information.....	I-6
1-323 Special Access Program.....	I-6
1-324 Special Background Investigation (SBI).....	I-7
1-325 Special Investigative Inquiry (SII).....	I-7
1-326 Service.....	I-7
1-327 Unfavorable Administrative Action.....	I-7
1-328 Unfavorable Personnel Security Determination.....	I-7

<u>Paragraph</u>	<u>Page</u>
1-329 United States Citizen (Native Born).....	I-7
1-330 Alien.....	I-7
1-331 Appointment.....	I-8
1-332 Controlled Information.....	I-8
1-333 Eligibility.....	I-8
1-334 Emergency Waiver.....	I-8
1-335 Sensitive Compartmented Information (SCI).....	I-8
1-336 Security Information System (SIS).....	I-8
1-337 Security Specialists.....	I-8
1-338 Glossary of Terms.....	I-8

1-332 commander, activity commander, Head of an Organization

CHAPTER II

POLICIES

Section 1

STANDARDS FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES

2-100 General.....	II-1
2-101 Clearance and Sensitive Position Standard.....	II-1
2-102 Military Service Standard.....	II-1

Section 2

CRITERIA FOR APPLICATION OF SECURITY STANDARDS

2-200 Criteria for Application of Security Standards.....	II-1
---	------

Section 3

TYPES AND SCOPE OF PERSONNEL SECURITY INVESTIGATIONS

2-300 General.....	II-3
2-301 National Agency Check.....	II-3
2-302 National Agency Check Plus Written Inquiries.....	II-3
2-303 DoD National Agency Check Plus Written Inquiries.....	II-4
2-304 Background Investigation.....	II-4
2-305 Special Background Investigation.....	II-4
2-306 Special Investigative Inquiry.....	II-4
2-307 Periodic Reinvestigation.....	II-5
2-308 Personal Interview.....	II-5
2-309 Expanded Investigation.....	II-6

Section 4

AUTHORIZED PERSONNEL SECURITY INVESTIGATIVE AGENCIES

2-400 General.....	II-6
2-401 Subversive Affiliations.....	II-7
2-402 Suitability Information.....	II-7
2-403 Hostage Situations.....	II-9
2-404 Overseas Personnel Security Investigations.....	II-10

Section 5

LIMITATIONS AND RESTRICTIONS

Paragraph	Page
2-500 Authorized Requesters and Personnel Security Determination Authorities.....	II-10
2-501 Limit Investigations and Access.....	II-10
2-502 Collection of Investigative Data.....	II-10
2-503 Privacy Act Notification.....	II-11
2-504 Restrictions on Investigators.....	II-11
2-505 Polygraph Restrictions.....	II-12

CHAPTER III

PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS

Section 1

SENSITIVE POSITIONS

3-100 Designation of Sensitive Positions.....	III-1
3-101 Criteria for Security Designation of Positions.....	III-1
3-102 Authority to Designate Sensitive Positions.....	III-2
3-103 Limitation of Sensitive Positions.....	III-2
3-104 Billet Control System for TOP SECRET.....	III-2

Section 2

CIVILIAN EMPLOYMENT

3-200 General.....	III-3
3-201 Nonsensitive Positions.....	III-3
3-202 Noncritical-sensitive Positions.....	III-4
3-203 Critical-sensitive Positions.....	III-4
3-204 Exceptions.....	III-5
3-205 Mobilization of DoD Civilian Retirees.....	III-6

Section 3

MILITARY APPOINTMENT, ENLISTMENT, AND INDUCTION

3-300 General.....	III-7
3-301 Entrance Investigation.....	III-7
3-302 Reserve Components and National Guard.....	III-7
3-303 Exceptions for Certain Commissioned Officers of Reserve Components.....	III-7
3-304 Mobilization of Military Retirees.....	III-8

Section 4

SECURITY CLEARANCE

3-400 General.....	III-8
3-401 Investigative Requirements for Clearance.....	III-8

<u>Paragraph</u>	<u>Page</u>
3-402 Access to Classified Information by Non-United States Citizens.....	III-10
3-403 Access by Persons Outside the Executive Branch.....	III-13
3-404 Restrictions on Issuance of Personnel Security Clearances.....	III-14
3-405 Dual Citizenship.....	III-15
3-406 One-Time Access.....	III-15
3-407 Access by Retired Flag and/or General Officers.....	III-17

Section 5

SPECIAL ACCESS PROGRAMS

3-500 General.....	III-17
3-501 Sensitive Compartmented Information (SCI).....	III-18
3-502 Single Integrated Operation Plan--Extremely Sensitive Information (SIOP-ESI).....	III-18
3-503 Presidential Support Activities.....	III-19
3-504 Nuclear Weapon Personnel Reliability Program (PRP).....	III-20
3-505 North Atlantic Treaty Organization (NATO) Classified Information.....	III-22
3-506 Other Special Access Programs.....	III-22

Section 6

CERTAIN POSITIONS NOT NECESSARILY REQUIRING ACCESS TO CLASSIFIED INFORMATION

3-600 General.....	III-22
3-601 Access to Restricted Areas, Sensitive Information or Equipment Not Involving Access to Classified Information....	III-23
3-602 Nonappropriated Fund Employees.....	III-23
3-603 Customs Inspectors.....	III-24
3-604 Red Cross/United Service Organizations Personnel.....	III-24
3-605 Officials Authorized to Issue Security Clearances.....	III-24
3-606 Personnel Security Clearance Adjudication Officials.....	III-24
3-607 Persons Requiring DoD Building Passes.....	III-24
3-608 Foreign National Employees Overseas Not Requiring Access to Classified Information.....	III-24
3-609 Special Agents and Investigative Support Personnel.....	III-25
3-610 Persons Requiring Access to Chemical Agents.....	III-25
3-611 Education and Orientation Personnel.....	III-25
3-612 Contract Guards.....	III-25
3-613 Transportation of Arms, Ammunition, and Explosives (AAE).....	III-25
3-614 Personnel Occupying Information Systems Positions Designated ADP-I, ADP-II & ADP-III.....	III-25
3-615 Others.....	III-26

Section 7

REINVESTIGATION

3-700 General.....	III-26
--------------------	--------

<u>Paragraph</u>	<u>Page</u>
3-701 Allegations Related to Disqualification.....	III-26
3-702 Access to Sensitive Compartmented Information.....	III-27
3-703 Critical-sensitive Positions.....	III-27
3-704 Presidential Support Duties.....	III-27
3-705 NATO Staff.....	III-27
3-706 Extraordinarily Sensitive Duties.....	III-27
3-707 Foreign Nationals Employed by DoD Organizations Overseas.....	III-27
3-708 Persons Accessing Very Sensitive Information Classified Secret.....	III-28
3-709 Access to Top Secret Information.....	III-28
3-710 Personnel Occupying Computer Positions Designated ADP-I.	III-28

Section 8

AUTHORITY TO WAIVE INVESTIGATIVE REQUIREMENTS

3-800 Authorized Officials.....	III-28
---------------------------------	--------

CHAPTER IV

RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS

4-100 General.....	IV-1
4-101 Prior Personnel Security Investigations.....	IV-1
4-102 Prior Personnel Security Determinations Made by DoD Authorities.....	IV-1
4-103 Investigations Conducted and Clearances Granted by Other Agencies of the Federal Government.....	IV-3

CHAPTER V

REQUESTING PERSONNEL SECURITY INVESTIGATIONS

5-100 General.....	V-1
5-101 Authorized Requesters.....	V-1
5-102 Criteria for Requesting Investigations.....	V-2
5-103 Request Procedures.....	V-2
5-104 Priority Requests.....	V-2
5-105 Personal Data Provided by the Subject of the Investigation.....	V-3

CHAPTER VI

ADJUDICATION

6-100 General.....	VI-1
6-101 Central Adjudication.....	VI-1
6-102 Evaluation of Personnel Security Information.....	VI-3
6-103 Adjudicative Record.....	VI-3

CHAPTER VII

ISSUING CLEARANCE AND GRANTING ACCESS

<u>Paragraph</u>	<u>Page</u>
7-100 General.....	VII-1
7-101 Issuing Clearance.....	VII-1
7-102 Granting Access.....	VII-3
7-103 Administrative Withdrawal.....	VII-4

CHAPTER VIII

UNFAVORABLE ADMINISTRATIVE ACTIONS

Section 1

REQUIREMENTS

8-100 General.....	VIII-1
8-101 Referral for Action.....	VIII-1
8-102 Suspension.....	VIII-2
8-103 Final Unfavorable Administrative Actions.....	VIII-3

Section 2

PROCEDURES

8-200 General.....	VIII-3
8-201 Unfavorable Administrative Action Procedures.....	VIII-4
8-202 Due Process Review.....	VIII-5
8-203 Exceptions to Policy.....	VIII-6

Section 3

REINSTATEMENT OF CIVILIAN EMPLOYEES

8-300 General.....	VIII-6
8-301 Reinstatement Benefits.....	VIII-6

CHAPTER IX

CONTINUING SECURITY RESPONSIBILITIES

Section 1

EVALUATING CONTINUED SECURITY ELIGIBILITY

9-100 General.....	IX-1
9-101 Management Responsibility.....	IX-1
9-102 Supervisory Responsibility.....	IX-2
9-103 Individual Responsibility.....	IX-4
9-104 Co-worker Responsibility.....	IX-4

Section 2

SECURITY EDUCATION

<u>Paragraph</u>	<u>Page</u>
9-200 General.....	IX-5
9-201 Initial Briefing.....	IX-5
9-202 Refresher Briefing.....	IX-6
9-203 Foreign Travel Briefing.....	IX-6
9-204 Termination Briefing.....	IX-7

CHAPTER X

SAFEGUARDING PERSONNEL SECURITY INVESTIGATIVE RECORDS

10-100	General.....	X-1
10-101	Responsibilities.....	X-1
10-102	Access Restrictions.....	X-1
10-103	Safeguarding Procedures.....	X-2
10-104	Records Disposition.....	X-3
10-105	Foreign Source Information.....	X-3

CHAPTER XI

PROGRAM MANAGEMENT

11-100	General.....	XI-1
11-101	Responsibilities.....	XI-1
11-102	Reporting Requirements.....	XI-2
11-103	Inspections.....	XI-3

CHAPTER XII

DEFENSE CLEARANCE AND INVESTIGATIONS INDEX

12-100	General.....	XII-1
12-101	Access.....	XII-1
12-102	Investigative Data.....	XII-2
12-103	Adjudicative Data.....	XII-2
12-104	Notification to Other Contributors.....	XII-3
12-105	Security Requirements for the DCII.....	XII-3
12-106	Disclosure of Information.....	XII-4

APPENDICES

Appendix A	-	References (continued).....	A-1
Appendix B	-	Investigative Scope.....	B-1
Appendix C	-	Request Procedures.....	C-1
Appendix D	-	Tables for Requesting Investigations.....	D-1
Appendix E	-	Reporting of Nonderogatory Cases.....	E-1
Appendix F	-	DoD Security Clearance and/or SCI Access Determination Authorities.....	F-1
Appendix G	-	Guidelines for Conducting Prenomination Personal Interviews.....	G-1

	<u>Page</u>
Appendix H - (left blank for future use)	
Appendix I - Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.....	I-1
Appendix J - Overseas Investigations.....	J-1
Appendix K - ADP Position Categories and Criteria for Designating Positions.....	K-1
Appendix L - Sample Notifications for Adverse Personnel Security Determinations.....	L-1
Appendix M - Structure and Functioning of the Personnel Security Appeal Board.....	M-1
Appendix N - Conduct of a Personal Appearance Before an Administrative Judge (AJ).....	N-1

ENCLOSURES

Enclosure 1 Executive Order 10450.....	1-1
Enclosure 2 Critical-Sensitive Positions (Regions).....	2-1
Enclosure 3 Appointment and Investigation Procedures.....	3-1
Section 1 Procedures for processing applicants with no prior Federal service or who had a break in Federal service for more than two years.....	3-1
Section 2 Processing applicants transferring from another Federal agency or reinstatement to Federal employment with less than two year break in Federal service.....	3-6
Section 3 Processing tentative selectees for regional GM-14 and above critical-sensitive positions who do not have background investigations...	3-9
Section 4 DCAA employees being considered for assignment/reassignment to positions of higher sensitivity	3-10
Section 5 Hiring foreign national employees in DCAA overseas offices.....	3-11
Section 6 Security Processing of Individuals for Special Access Programs (SAPs).....	3-12
Section 7 Disposition of Security Clearance and Eligibility Certificates.....	3-13
Enclosure 4 Briefings Outline.....	4-1
Enclosure 5 DoD Directive 5240.6, Counterintelligence Awareness and Briefing Program.....	5-1
Enclosure 6 Foreign Contact/Travel Guide for DCAA Personnel.....	6-1
Enclosure 7 List of Forms.....	7-1

750.2

DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM REGULATION

CHAPTER I

GENERAL PROVISIONS

Section 1

REFERENCES

1-100 REFERENCES

- (A) DOD 5200.2-R, "PERSONNEL SECURITY PROGRAM," JANUARY 1987, AUTHORIZED BY DOD DIRECTIVE 5200.2, MAY 6, 1992
- (B) DOD 5220.22-R, "INDUSTRIAL SECURITY REGULATION," DECEMBER 1985, AUTHORIZED BY DOD DIRECTIVE 5220.22, DECEMBER 8, 1980
- (C) DOD DIRECTIVE 5220.6, "DEFENSE INDUSTRIAL PERSONNEL SECURITY CLEARANCE REVIEW PROGRAM," FEBRUARY 2, 1992
- (D) THROUGH (OO), SEE APPENDIX A
- a. DoD 5200.2-R, DoD Personnel Security Program (SOLID CAPITAL LETTERS in this manual)
- b. DCAA Regulation 5210.1, DCAA Personnel Security Program
- c. DoD Directive 5240.6, Counterintelligence Awareness and Briefing Program (Enclosure 5 of this manual)
- d. DCAA Regulation 3020.4, Protection of DCAA Personnel and Resources Against Terrorist Acts
- e. DCAA Regulation 5205.10, Special Access Programs
- f. DCAA Instruction 5205.11, Procedures for Implementing Audit Effort of Special Access Programs
- g. DCAA Manual 5205.1, Information Security Program
- h. DCAA Regulation 5210.9, Nomination, Screening, Investigation, Selection, and Continuing Evaluation of DCAA Personnel for Assignment to Presidential Support Activities
- i. DCAA Regulation C-5210.12, United States Security Authority for North Atlantic Treaty Organization Affairs
- j. DCAA Regulation 5210.3, Access to and Dissemination of Restricted Data
- k. DCAA Regulation 5240.1, Department of Defense Counterintelligence
- l. DCAA Regulation 5220.1, DoD Industrial Security Program
- m. DoD 5400.7-R, DoD Freedom of Information Act Program.
- n. DCAA Instruction 5410.8, DCAA Freedom of Information Act Program
- o. DCAA Instruction 5410.10, DCAA Privacy Act Program
- p. Office of the Assistant Secretary of Defense (Comptroller) Administrative Instruction No. 30, Building Security for the Pentagon
- q. DCAA Manual 5015.1, Files Maintenance and Disposition Manual
- r. DCAA Manual 1400.1, Personnel Management Manual
- s. DCAA Regulation 5210.7, DCAA Polygraph Program
- t. DCAA Regulation 5205.3, Security Surveys and Inspections
- u. DCAA Regulation 5200.7, Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense
- v. DCAA Pamphlet 5205.13, DCAA SAP Security Guide
- w. DoD Directive 5230.24, Distribution Statements on Technical Documents, 18 March 1987

x. Memorandums:

1. OASD(C3I), 9 June 1992, Subject: Supervisory Review for Periodic Reinvestigations (DCAA MRD No. 92-CPS-152, 26 June 1992)
2. OASD(C3I), 9 April 1993, Subject: Elimination of Technical Fingerprint Check for TOP SECRET and SECRET Periodic Reinvestigations (PRs) (DCAA MRD No. 93-CPS-074, 16 April 1993)
3. WHS, 13 September 1993, Subject: Initiation of WHS Collateral Operations, Ref DMRD 986
4. WHS, 14 September 1993, Subject: Processing of DD Forms 1879 and OPM SFs 85P and 86 for Collateral Security Clearances and/or Sensitive Position Occupancy Determinations
5. DIA, 23 September 1993, Subject: Processing of Requests for Personnel Security Investigations for Sensitive Compartmented Information Access
6. DIA, 29 September 1993, Subject: DIA SCI Processing Guidance
7. WHS, 13 December 1993, Subject: Personnel Security Clearance Upgrades
8. WHS, 21 December 1993, Subject: Completing OPM SF 85P (Questionnaire for Public Trust Positions) and SF 86 (Questionnaire for Sensitive Positions) (DCAA MRD to attention of RSOs, 23 December 1993 - no number assigned)
9. DCAA MRD No. 94-CPS-029(R), dated 2 March 1994, subject: Evaluating Continued Security Eligibility
10. WHS, 4 March 1994, Access Levels
11. WHS, 23 March 1994, Access Levels
12. WHS, 29 April 1994, Subject: Psychiatric Evaluations Procedures (DCAA MRD No. 94-CPS-081(R), 17 May 1994)
13. WHS, 24 May 1994, Subject: Clearance for Summer Hires, Seasonal Employees, and Unsalariated Interns
14. OASD(C3I) memorandum, dated 19 October 1993, subject: Resubmission of Fingerprint Cards to OPM (DCAA MRD No. 95-CPS-131(R), 27 October 1995)
15. DCAA MRD No. 95-CPS-141(R), dated 21 November 1995, subject: Indicating Classified Access on Requests for Investigation

Section 2

PURPOSE AND APPLICABILITY

1-200 PURPOSE

A. TO ESTABLISH POLICIES AND PROCEDURES TO ENSURE THAT ACCEPTANCE AND RETENTION OF PERSONNEL IN THE ARMED FORCES, ACCEPTANCE AND RETENTION OF CIVILIAN EMPLOYEES IN THE DEPARTMENT OF DEFENSE (DOD), AND GRANTING MEMBERS OF THE ARMED FORCES, DOD CIVILIAN EMPLOYEES, DOD CONTRACTORS, AND OTHER AFFILIATED PERSONS ACCESS TO CLASSIFIED INFORMATION ARE CLEARLY CONSISTENT WITH THE INTERESTS OF NATIONAL SECURITY.

B. THIS REGULATION:

- (1) ESTABLISHES DOD PERSONNEL SECURITY POLICIES AND PROCEDURES;
- (2) SETS FORTH THE STANDARDS, CRITERIA AND GUIDELINES UPON WHICH PERSONNEL SECURITY DETERMINATIONS SHALL BE BASED;

(3) PRESCRIBES THE KINDS AND SCOPES OF PERSONNEL SECURITY INVESTIGATIONS REQUIRED;

(4) DETAILS THE EVALUATION AND ADVERSE ACTION PROCEDURES BY WHICH PERSONNEL SECURITY DETERMINATIONS SHALL BE MADE; AND

(5) ASSIGNS OVERALL PROGRAM MANAGEMENT RESPONSIBILITIES.

1-201 APPLICABILITY

A. THIS REGULATION IMPLEMENTS THE DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM AND TAKES PRECEDENCE OVER ALL OTHER DEPARTMENTAL ISSUANCES AFFECTING THAT PROGRAM. This Manual is applicable to all DCAA personnel and organizational elements, i.e., Headquarters (including PD, DCAI, TSC) and the regions (including Regional Personnel Offices and PAOs).

B. ALL PROVISIONS OF THIS REGULATION APPLY TO DOD CIVILIAN PERSONNEL, MEMBERS OF THE ARMED FORCES, EXCLUDING THE COAST GUARD IN PEACETIME, CONTRACTOR PERSONNEL AND OTHER PERSONNEL WHO ARE AFFILIATED WITH THE DEPARTMENT OF DEFENSE EXCEPT THAT THE UNFAVORABLE ADMINISTRATIVE ACTION PROCEDURES PERTAINING TO CONTRACTOR PERSONNEL REQUIRING ACCESS TO CLASSIFIED INFORMATION ARE CONTAINED IN DOD 5220.22-R (REFERENCE (B)) AND IN DOD DIRECTIVE 5220.6 (REFERENCE (C)). Security clearance procedures for persons performing contractual services for DCAA are contained in DoD 5220.22-R (reference 1-100(B)) and DCAA Regulation 5220.1 (reference 1-100.m).

C. THE POLICIES AND PROCEDURES WHICH GOVERN THE NATIONAL SECURITY AGENCY ARE PRESCRIBED BY PUBLIC LAWS 88-290 AND 86-36, EXECUTIVE ORDERS 10450 AND 12333, DOD DIRECTIVE 5210.45, DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 1/14 (REFERENCES (E), (F), (G), (I), AND (L) RESPECTIVELY), AND REGULATIONS OF THE NATIONAL SECURITY AGENCY.

D. UNDER COMBAT CONDITIONS OR OTHER MILITARY EXIGENCIES, AN AUTHORITY IN PARAGRAPH A, APPENDIX F, MAY WAIVE SUCH PROVISIONS OF THIS REGULATION AS THE CIRCUMSTANCES WARRANT.

Section 3

DEFINITIONS

1-300 ACCESS

THE ABILITY AND OPPORTUNITY TO OBTAIN KNOWLEDGE OF CLASSIFIED INFORMATION. AN INDIVIDUAL, IN FACT, MAY HAVE ACCESS TO CLASSIFIED INFORMATION BY BEING IN A PLACE WHERE SUCH INFORMATION IS KEPT, IF THE SECURITY MEASURES THAT ARE IN FORCE DO NOT PREVENT HIM FROM GAINING KNOWLEDGE OF SUCH INFORMATION.

1-301 ADVERSE ACTION

A REMOVAL FROM EMPLOYMENT, SUSPENSION FROM EMPLOYMENT OF MORE THAN 14 DAYS, REDUCTION IN GRADE, REDUCTION IN PAY, OR FURLOUGH OF 30 DAYS OR LESS.

1-302 BACKGROUND INVESTIGATION (BI)

A PERSONNEL SECURITY INVESTIGATION CONSISTING OF BOTH RECORD REVIEWS AND INTERVIEWS WITH SOURCES OF INFORMATION AS PRESCRIBED IN PARAGRAPH 3, APPENDIX B, THIS REGULATION, COVERING THE MOST RECENT 5 YEARS OF AN INDIVIDUAL'S LIFE OR SINCE THE 18TH BIRTHDAY, WHICHEVER IS SHORTER, PROVIDED THAT AT LEAST THE LAST 2 YEARS ARE COVERED AND THAT NO INVESTIGATION WILL BE CONDUCTED PRIOR TO AN INDIVIDUAL'S 16TH BIRTHDAY.

1-303 CLASSIFIED INFORMATION

OFFICIAL INFORMATION OR MATERIAL THAT REQUIRES PROTECTION IN THE INTERESTS OF NATIONAL SECURITY AND THAT IS CLASSIFIED FOR SUCH PURPOSE BY APPROPRIATE CLASSIFYING AUTHORITY IN ACCORDANCE WITH THE PROVISIONS OF EXECUTIVE ORDER 12356 (REFERENCE (J)).

1-304 DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII)

THE DCII IS THE SINGLE, AUTOMATED, CENTRAL DOD REPOSITORY WHICH IDENTIFIES INVESTIGATIONS CONDUCTED BY DOD INVESTIGATIVE AGENCIES, AND PERSONNEL SECURITY DETERMINATIONS MADE BY DOD ADJUDICATIVE AUTHORITIES. [CH2 to DoD 5200.2-R, 7/14/93]

1-305 DOD COMPONENT

INCLUDES THE OFFICE OF THE SECRETARY OF DEFENSE; THE MILITARY DEPARTMENTS; CHAIRMAN OF THE JOINT CHIEFS OF STAFF AND THE JOINT STAFF; DIRECTORS OF DEFENSE AGENCIES AND THE UNIFIED AND SPECIFIED COMMANDS.

1-306 ENTRANCE NATIONAL AGENCY CHECK (ENTNAC)

A PERSONNEL SECURITY INVESTIGATION SCOPED AND CONDUCTED IN THE SAME MANNER AS A NATIONAL AGENCY CHECK EXCEPT THAT A TECHNICAL FINGERPRINT SEARCH OF THE FILES OF THE FEDERAL BUREAU OF INVESTIGATION IS NOT CONDUCTED.

1-307 HEAD OF DOD COMPONENT

THE SECRETARY OF DEFENSE; THE SECRETARIES OF THE MILITARY DEPARTMENTS; THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF; AND THE COMMANDERS OF UNIFIED AND SPECIFIED COMMANDS; AND THE DIRECTORS OF DEFENSE AGENCIES. [CH2 to DoD 5200.2-R, 7/14/93]

1-308 IMMIGRANT ALIEN

ANY ALIEN LAWFULLY ADMITTED INTO THE UNITED STATES UNDER AN IMMIGRATION VISA FOR PERMANENT RESIDENCE.

1-309 INTERIM SECURITY CLEARANCE

A SECURITY CLEARANCE BASED ON THE COMPLETION OF MINIMUM INVESTIGATIVE REQUIREMENTS, WHICH IS GRANTED ON A TEMPORARY BASIS, PENDING THE COMPLETION OF THE FULL INVESTIGATIVE REQUIREMENTS.

1-310 LIMITED ACCESS AUTHORIZATION

AUTHORIZATION FOR ACCESS TO CONFIDENTIAL OR SECRET INFORMATION GRANTED TO NON-UNITED STATES CITIZENS AND IMMIGRANT ALIENS, WHICH IS LIMITED TO ONLY THAT INFORMATION NECESSARY TO THE SUCCESSFUL ACCOMPLISHMENT OF THEIR ASSIGNED DUTIES AND BASED ON A BACKGROUND INVESTIGATION SCOPED FOR 10 YEARS (PARAGRAPH 3, APPENDIX B).

1-311 MINOR DEROGATORY INFORMATION

INFORMATION THAT, BY ITSELF, IS NOT OF SUFFICIENT IMPORTANCE OR MAGNITUDE TO JUSTIFY AN UNFAVORABLE ADMINISTRATIVE ACTION IS A PERSONNEL SECURITY DETERMINATION.

1-312 NATIONAL AGENCY CHECK (NAC)

A PERSONNEL SECURITY INVESTIGATION CONSISTING OF A RECORDS REVIEW OF CERTAIN NATIONAL AGENCIES AS PRESCRIBED IN PARAGRAPH 1, APPENDIX B, THIS REGULATION, INCLUDING A TECHNICAL FINGERPRINT SEARCH OF THE FILES OF THE FEDERAL BUREAU OF INVESTIGATION (FBI).

1-313 NATIONAL AGENCY CHECK PLUS WRITTEN INQUIRIES (NACI)

A PERSONNEL SECURITY INVESTIGATION CONDUCTED BY THE OFFICE OF PERSONNEL MANAGEMENT, COMBINING A NAC AND WRITTEN INQUIRIES TO LAW ENFORCEMENT AGENCIES, FORMER EMPLOYERS AND SUPERVISORS, REFERENCES AND SCHOOLS.

1-314 NATIONAL SECURITY

NATIONAL SECURITY MEANS THE NATIONAL DEFENSE AND FOREIGN RELATIONS OF THE UNITED STATES.

1-315 NEED-TO-KNOW

A DETERMINATION MADE BY A POSSESSOR OF CLASSIFIED INFORMATION THAT A PROSPECTIVE RECIPIENT, IN THE INTEREST OF NATIONAL SECURITY, HAS A REQUIREMENT FOR ACCESS TO, KNOWLEDGE, OR POSSESSION OF THE CLASSIFIED INFORMATION IN ORDER TO PERFORM TASKS OR SERVICES ESSENTIAL TO THE FULFILLMENT OF AN OFFICIAL UNITED STATES GOVERNMENT PROGRAM. KNOWLEDGE, POSSESSION OF, OR ACCESS TO, CLASSIFIED INFORMATION SHALL NOT BE AFFORDED TO ANY INDIVIDUAL SOLELY BY VIRTUE OF THE INDIVIDUAL'S OFFICE, POSITION, OR SECURITY CLEARANCE.

1-316 PERIODIC REINVESTIGATION (PR)

AN INVESTIGATION CONDUCTED EVERY FIVE YEARS FOR THE PURPOSE OF UPDATING A PREVIOUSLY COMPLETED BACKGROUND INVESTIGATION, SPECIAL BACKGROUND INVESTIGATION, SINGLE SCOPE BACKGROUND INVESTIGATION OR PR ON PERSONS OCCUPYING POSITIONS REFERRED TO IN PARAGRAPHS 3-700 THROUGH 3-710. INVESTIGATIVE REQUIREMENTS ARE AS PRESCRIBED IN PARAGRAPH 5, APPENDIX B, OF THIS REGULATION. THE PERIOD OF INVESTIGATION WILL NOT NORMALLY EXCEED THE MOST RECENT 5-YEAR PERIOD. [CH2 to DoD 5200.2-R, 7/14/93]

1-317 PERSONNEL SECURITY INVESTIGATION (PSI)

ANY INVESTIGATION REQUIRED FOR THE PURPOSE OF DETERMINING THE ELIGIBILITY

OF DOD MILITARY AND CIVILIAN PERSONNEL, CONTRACTOR EMPLOYEES, CONSULTANTS, AND OTHER PERSONS AFFILIATED WITH THE DEPARTMENT OF DEFENSE, FOR ACCESS TO CLASSIFIED INFORMATION, ACCEPTANCE OR RETENTION IN THE ARMED FORCES, ASSIGNMENT OR RETENTION IN SENSITIVE DUTIES, OR OTHER DESIGNATED DUTIES REQUIRING SUCH INVESTIGATION. PSIs INCLUDE INVESTIGATIONS OF AFFILIATIONS WITH SUBVERSIVE ORGANIZATIONS, SUITABILITY INFORMATION, OR HOSTAGE SITUATIONS (SEE PARAGRAPH 2-403) CONDUCTED FOR THE PURPOSE OF MAKING PERSONNEL SECURITY DETERMINATIONS. THEY ALSO INCLUDE INVESTIGATIONS OF ALLEGATIONS THAT ARISE SUBSEQUENT TO ADJUDICATIVE ACTION AND REQUIRE RESOLUTION TO DETERMINE AN INDIVIDUAL'S CURRENT ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT OR RETENTION IN A SENSITIVE POSITION.

1-318 SCOPE

THE TIME PERIOD TO BE COVERED AND THE SOURCES OF INFORMATION TO BE CONTACTED DURING THE PRESCRIBED COURSE OF A PSI.

1-319 SECURITY CLEARANCE

A DETERMINATION THAT A PERSON IS ELIGIBLE UNDER THE STANDARDS OF THIS REGULATION FOR ACCESS TO CLASSIFIED INFORMATION.

1-320 SENIOR OFFICER OF THE INTELLIGENCE COMMUNITY (SOIC)

THE DOD SENIOR OFFICERS OF THE INTELLIGENCE COMMUNITY INCLUDE: THE DIRECTOR, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE; DIRECTOR, DEFENSE INTELLIGENCE AGENCY; ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE, U.S. ARMY; ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE, U.S. AIR FORCE; AND THE DIRECTOR OF NAVAL INTELLIGENCE, U.S. NAVY.

1-321 SENSITIVE POSITION

ANY POSITION SO DESIGNATED WITHIN THE DEPARTMENT OF DEFENSE, THE OCCUPANT OF WHICH COULD BRING ABOUT, BY VIRTUE OF THE NATURE OF THE POSITION, A MATERIALLY ADVERSE EFFECT ON THE NATIONAL SECURITY. ALL CIVILIAN POSITIONS ARE EITHER CRITICAL-SENSITIVE, NONCRITICAL-SENSITIVE, OR NONSENSITIVE AS DESCRIBED IN PARAGRAPH 3-101.

1-322 SIGNIFICANT DEROGATORY INFORMATION

INFORMATION THAT COULD, IN ITSELF, JUSTIFY AN UNFAVORABLE ADMINISTRATIVE ACTION, OR PROMPT AN ADJUDICATOR TO SEEK ADDITIONAL INVESTIGATION OR CLARIFICATION.

1-323 SPECIAL ACCESS PROGRAM

ANY PROGRAM IMPOSING "NEED-TO-KNOW" OR ACCESS CONTROLS BEYOND THOSE NORMALLY PROVIDED FOR ACCESS TO CONFIDENTIAL, SECRET, OR TOP SECRET INFORMATION. SUCH A PROGRAM MAY INCLUDE, BUT NOT BE LIMITED TO, SPECIAL CLEARANCE, ADJUDICATION, INVESTIGATIVE REQUIREMENTS, MATERIAL DISSEMINATION RESTRICTIONS, OR SPECIAL LISTS OF PERSONS DETERMINED TO HAVE A NEED-TO-KNOW.

1-324 SPECIAL BACKGROUND INVESTIGATION (SBI)

A PERSONNEL SECURITY INVESTIGATION CONSISTING OF ALL OF THE COMPONENTS OF A BI PLUS CERTAIN ADDITIONAL INVESTIGATIVE REQUIREMENTS AS PRESCRIBED IN PARAGRAPH 4, APPENDIX B, THIS REGULATION. THE PERIOD OF INVESTIGATION FOR AN SBI IS THE LAST 15 YEARS OR SINCE THE 18TH BIRTHDAY, WHICHEVER IS SHORTER, PROVIDED THAT THE LAST 2 FULL YEARS ARE COVERED AND THAT NO INVESTIGATION WILL BE CONDUCTED PRIOR TO AN INDIVIDUAL'S 16TH BIRTHDAY.

1-325 SPECIAL INVESTIGATIVE INQUIRY (SII)

A SUPPLEMENTAL PERSONNEL SECURITY INVESTIGATION OF LIMITED SCOPE CONDUCTED TO PROVE OR DISPROVE RELEVANT ALLEGATIONS THAT HAVE ARISEN CONCERNING A PERSON UPON WHOM A PERSONNEL SECURITY DETERMINATION HAS BEEN PREVIOUSLY MADE AND WHO, AT THE TIME OF THE ALLEGATION, HOLDS A SECURITY CLEARANCE OR OTHERWISE OCCUPIES A POSITION THAT REQUIRES A PERSONNEL SECURITY DETERMINATION UNDER THE PROVISIONS OF THIS REGULATION.

1-326 SERVICE

HONORABLE ACTIVE DUTY (INCLUDING ATTENDANCE AT THE MILITARY ACADEMIES), MEMBERSHIP IN ROTC SCHOLARSHIP PROGRAM, ARMY AND AIR FORCE NATIONAL GUARD, MILITARY RESERVE FORCE (INCLUDING ACTIVE STATUS AND READY RESERVE), CIVILIAN EMPLOYMENT IN GOVERNMENT SERVICE, OR CIVILIAN EMPLOYMENT WITH A DOD CONTRACTOR OR AS A CONSULTANT INVOLVING ACCESS UNDER THE DOD INDUSTRIAL SECURITY PROGRAM. CONTINUITY OF SERVICE IS MAINTAINED WITH CHANGE FROM ONE STATUS TO ANOTHER AS LONG AS THERE IS NO SINGLE BREAK IN SERVICE GREATER THAN 12 MONTHS.

1-327 UNFAVORABLE ADMINISTRATIVE ACTION

ADVERSE ACTION TAKEN AS THE RESULT OF PERSONNEL SECURITY DETERMINATIONS AND UNFAVORABLE PERSONNEL SECURITY DETERMINATIONS AS DEFINED IN THIS REGULATION.

1-328 UNFAVORABLE PERSONNEL SECURITY DETERMINATION

A DENIAL OR REVOCATION OF CLEARANCE FOR ACCESS TO CLASSIFIED INFORMATION; DENIAL OR REVOCATION OF ACCESS TO CLASSIFIED INFORMATION; DENIAL OR REVOCATION OF A SPECIAL ACCESS AUTHORIZATION (INCLUDING ACCESS TO SCI); NONAPPOINTMENT TO OR NONSELECTION FOR APPOINTMENT TO A SENSITIVE POSITION; NONAPPOINTMENT TO OR NONSELECTION FOR ANY OTHER POSITION REQUIRING A TRUSTWORTHINESS DETERMINATION UNDER THIS REGULATION; REASSIGNMENT TO A POSITION OF LESSER SENSITIVITY OR TO A NONSENSITIVE POSITION; AND NONACCEPTANCE FOR OR DISCHARGE FROM THE ARMED FORCES WHEN ANY OF THE FOREGOING ACTIONS ARE BASED ON DEROGATORY INFORMATION OF PERSONNEL SECURITY SIGNIFICANCE.

1-329 UNITED STATES CITIZEN (NATIVE BORN)

A PERSON BORN IN ONE OF THE 50 UNITED STATES, PUERTO RICO, GUAM, AMERICAN SAMOA, NORTHERN MARIANA ISLANDS, U.S. VIRGIN ISLANDS; OR PANAMA CANAL ZONE (IF THE FATHER OR MOTHER (OR BOTH) WAS OR IS, A CITIZEN OF THE UNITED STATES).

1-330 Alien

Any person not a citizen or permanent resident of the United States.

1-331 Appointment

Any personnel action which has the effect of adding or returning an individual to the civilian rolls of DCAA, whether by initial appointment, transfer from another Federal agency, or by reinstatement to the Federal service.

I-332 is removed. Act. Under Head of Org. as used through this manual, if not otherwise defined, is intended to refer to those individuals designated as the Agency Security Officer.

1-332 Controlled Information

As used in this Manual, that information which bears a distribution limitation statement from DoD Directive 5230.24 (reference 1-100.w), or that information which is being marked "For Official Use Only" in accordance with Chapter IV of DoD 5400.7-R (reference 1-100.m).

1-333 Eligibility

A security status based on favorable adjudication of a personnel security investigation indicating that an individual is deemed trustworthy for employment in a sensitive position and/or may be granted a security clearance for access to classified information up to the level required in the performance of official duties.

1-334 Emergency Waiver

A temporary waiver of preappointment investigative requirements granted when appropriate authority has determined that the delay in appointment or reassignment, pending completion of required investigation, would be harmful to the national security.

1-335 Sensitive Compartmented Information (SCI)

Classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the Director of Central Intelligence.

1-336 Security Information System (SIS)

A DCAA automated system for maintaining personnel security data and monitoring various personnel security actions.

1-337 Security Specialists

For the purpose of this manual, security specialists means CPS, FD, and regional office security personnel authorized to perform specific security duties in conjunction with the DCAA personnel security program. This does not include SCOs, ASCOs, or document custodians.

1-338 Glossary of Terms

ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ASO	Agency Security Officer
ASCO	Alternate Security Control Officer
BI	Background Investigation
CAF	Consolidated Adjudications Facility

1-338 Glossary of Terms continued

C/E Cert	Access and Eligibility Certificate
CI	Character Investigation
CPO	Operating Personnel Office, Headquarters, DCAA
CPS	Security Branch, Headquarters, DCAA
CS	Critical-Sensitive
DASD(IS)	Deputy Assistant Secretary of Defense (Intelligence and Security)
DCAA	Defense Contract Audit Agency
DCII	Defense Clearance and Investigations Index
DIA CCF	Defense Intelligence Agency Central Clearance Facility
DIS	Defense Investigative Service
DoD	Department of Defense
DUSD(P)	Deputy Under Secretary of Defense for Policy
ENTRAC	Entrance National Agency Check
EO	Executive Order
FAO	Field Audit Office
FD	Field Detachment
FDSO	Field Detachment Security Officer
FBI	Federal Bureau of Investigations
IRS	Internal Revenue Service
LAC	Local Agency Check
LoI	Letter of Intent
MFR	Memorandum for Record
NAC	National Agency Check
NACI	National Agency Check with Written Inquiries
NCS	Noncritical-Sensitive
NS	Nonsensitive
OASD(CIASCM)	Office of the Assistant Secretary of Defense (Counterintelligence and Security Countermeasures)
OPM	Office of Personnel Management
OPF	Official Personnel Folder
PR	Periodic Reinvestigation
RPO	Regional Personnel Officer
RSO	Regional Security Officer
SAP(s)	Special Access Program(s)
SBI	Special Background Investigation
SCI	Sensitive Compartmented Information
SCO	Security Control Officer
SI	Subject Interview
SII	Special Investigative Inquiry
SIS	Security Information System
SOR	Statement of Reasons
SSBI	Single Scope Background Investigation
USOPM-PIPC	U.S. Office of Personnel Management - Federal Investigations Processing Center
WHS	Washington Headquarters Services
WHS CAF	Washington Headquarters Services Consolidated Adjudications Facility

CHAPTER II

POLICIES

Section 1

STANDARDS FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES

2-100 GENERAL

ONLY UNITED STATES CITIZENS SHALL BE GRANTED A PERSONNEL SECURITY CLEARANCE, ASSIGNED TO SENSITIVE DUTIES, OR GRANTED ACCESS TO CLASSIFIED INFORMATION UNLESS AN AUTHORITY DESIGNATED IN APPENDIX F HAS DETERMINED THAT, BASED ON ALL AVAILABLE INFORMATION, THERE ARE COMPELLING REASONS IN FURTHERANCE OF THE DEPARTMENT OF DEFENSE MISSION, INCLUDING SPECIAL EXPERTISE, TO ASSIGN AN INDIVIDUAL WHO IS NOT A CITIZEN TO SENSITIVE DUTIES OR GRANT A LIMITED ACCESS AUTHORIZATION TO CLASSIFIED INFORMATION. NON-U.S. CITIZENS MAY BE EMPLOYED IN THE COMPETITIVE SERVICE IN SENSITIVE CIVILIAN POSITIONS ONLY WHEN SPECIFICALLY APPROVED BY THE OFFICE OF PERSONNEL MANAGEMENT, PURSUANT TO E.O. 11935 (REFERENCE (K)). EXCEPTIONS TO THESE REQUIREMENTS SHALL BE PERMITTED ONLY FOR COMPELLING NATIONAL SECURITY REASONS.

2-101 CLEARANCE AND SENSITIVE POSITION STANDARD

THE PERSONNEL SECURITY STANDARD THAT MUST BE APPLIED TO DETERMINE WHETHER A PERSON IS ELIGIBLE FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES IS WHETHER, BASED ON ALL AVAILABLE INFORMATION, THE PERSON'S LOYALTY, RELIABILITY, AND TRUSTWORTHINESS ARE SUCH THAT ENTRUSTING THE PERSON WITH CLASSIFIED INFORMATION OR ASSIGNING THE PERSON TO SENSITIVE DUTIES IS CLEARLY CONSISTENT WITH THE INTERESTS OF NATIONAL SECURITY.

2-102 MILITARY SERVICE STANDARD

THE PERSONNEL SECURITY STANDARD THAT MUST BE APPLIED IN DETERMINING WHETHER A PERSON IS SUITABLE UNDER NATIONAL SECURITY CRITERIA FOR APPOINTMENT, ENLISTMENT, INDUCTION, OR RETENTION IN THE ARMED FORCES IS THAT, BASED ON ALL AVAILABLE INFORMATION, THERE IS NO REASONABLE BASIS FOR DOUBTING THE PERSON'S LOYALTY TO THE GOVERNMENT OF THE UNITED STATES.

Section 2

CRITERIA FOR APPLICATION OF SECURITY STANDARDS

2-200 CRITERIA FOR APPLICATION OF SECURITY STANDARDS

THE ULTIMATE DECISION IN APPLYING EITHER OF THE SECURITY STANDARDS SET FORTH IN PARAGRAPH 2-101 AND 2-102 ABOVE MUST BE AN OVERALL COMMON SENSE DETERMINATION BASED UPON ALL AVAILABLE FACTS. THE CRITERIA FOR DETERMINING ELIGIBILITY FOR A CLEARANCE UNDER THE SECURITY STANDARD SHALL INCLUDE, BUT NOT BE LIMITED TO THE FOLLOWING:

A. COMMISSION OF ANY ACT OF SABOTAGE, ESPIONAGE, TREASON, TERRORISM, ANARCHY, SEDITION, OR ATTEMPTS THEREAT OR PREPARATION THEREFOR, OR CONSPIRING WITH OR AIDING OR ABETTING ANOTHER TO COMMIT OR ATTEMPT TO COMMIT ANY SUCH ACT.

B. ESTABLISHING OR CONTINUING A SYMPATHETIC ASSOCIATION WITH A SABOTEUR, SPY, TRAITOR, SEDITIONIST, ANARCHIST, TERRORIST, REVOLUTIONIST, OR WITH AN ESPIONAGE OR OTHER SECRET AGENT OR SIMILAR REPRESENTATIVE OF A FOREIGN NATION WHOSE INTERESTS MAY BE INIMICAL TO THE INTERESTS OF THE UNITED STATES, OR WITH ANY PERSON WHO ADVOCATES THE USE OF FORCE OR VIOLENCE TO OVERTHROW THE GOVERNMENT OF THE UNITED STATES OR TO ALTER THE FORM OF GOVERNMENT OF THE UNITED STATES BY UNCONSTITUTIONAL MEANS.

C. ADVOCACY OR USE OF FORCE OR VIOLENCE TO OVERTHROW THE GOVERNMENT OF THE UNITED STATES OR TO ALTER THE FORM OF GOVERNMENT OF THE UNITED STATES BY UNCONSTITUTIONAL MEANS.

D. KNOWING MEMBERSHIP WITH THE SPECIFIC INTENT OF FURTHERING THE AIMS OF, OR ADHERENCE TO AND ACTIVE PARTICIPATION IN ANY FOREIGN OR DOMESTIC ORGANIZATION, ASSOCIATION, MOVEMENT, GROUP OR COMBINATION OF PERSONS (HEREAFTER REFERRED TO AS ORGANIZATIONS) WHICH UNLAWFULLY ADVOCATES OR PRACTICES THE COMMISSION OF ACTS OF FORCE OR VIOLENCE TO PREVENT OTHERS FROM EXERCISING THEIR RIGHTS UNDER THE CONSTITUTION OR LAWS OF THE U.S. OR ANY STATE OF WHICH SEEKS TO OVERTHROW THE GOVERNMENT OF THE U.S. OR ANY STATE OR SUBDIVISION THEREOF BY UNLAWFUL MEANS.

E. UNAUTHORIZED DISCLOSURE TO ANY PERSON OF CLASSIFIED INFORMATION, OR OF OTHER INFORMATION, DISCLOSURE OF WHICH IS PROHIBITED BY STATUTE, EXECUTIVE ORDER OR REGULATION.

F. PERFORMING OR ATTEMPTING TO PERFORM ONE'S DUTIES, ACCEPTANCE AND ACTIVE MAINTENANCE OF DUAL CITIZENSHIP, OR OTHER ACTS CONDUCTED IN A MANNER WHICH SERVE OR WHICH COULD BE EXPECTED TO SERVE THE INTERESTS OF ANOTHER GOVERNMENT IN PREFERENCE TO THE INTERESTS OF THE U.S.

G. DISREGARD OF PUBLIC LAW, STATUTES, EXECUTIVE ORDERS OR REGULATIONS INCLUDING VIOLATION OF SECURITY REGULATIONS OR PRACTICES.

H. CRIMINAL OR DISHONEST CONDUCT.

I. ACTS OF OMISSION OR COMMISSION THAT INDICATE POOR JUDGMENT, UNRELIABILITY OR UNTRUSTWORTHINESS.

J. ANY BEHAVIOR OR ILLNESS, INCLUDING ANY MENTAL CONDITION, WHICH, IN THE OPINION OF COMPETENT MEDICAL AUTHORITY, MAY CAUSE A DEFECT IN JUDGMENT OR RELIABILITY WITH DUE REGARD TO THE TRANSIENT OR CONTINUING EFFECT OF THE ILLNESS AND THE MEDICAL FINDINGS IN SUCH CASE.

K. VULNERABILITY TO COERCION, INFLUENCE, OR PRESSURE THAT MAY CAUSE CONDUCT CONTRARY TO THE NATIONAL INTEREST. THIS MAY BE (1) THE PRESENCE OF IMMEDIATE FAMILY MEMBERS OR OTHER PERSONS TO WHOM THE APPLICANT IS BONDED BY AFFECTION OR OBLIGATION IN A NATION (OR AREAS UNDER ITS DOMINATION) WHOSE INTERESTS MAY BE INIMICAL TO THOSE OF THE U.S., OR (2) ANY OTHER CIRCUMSTANCES THAT COULD CAUSE THE APPLICANT TO BE VULNERABLE.

L. EXCESSIVE INDEBTEDNESS, RECURRING FINANCIAL DIFFICULTIES, OR UNEXPLAINED AFFLUENCE.

M. HABITUAL OR EPISODIC USE OF INTOXICANTS TO EXCESS.

N. ILLEGAL OR IMPROPER USE, POSSESSION, TRANSFER, SALE OR ADDICTION TO ANY CONTROLLED OR PSYCHOACTIVE SUBSTANCE, NARCOTIC, CANNABIS OR OTHER DANGEROUS DRUG.

O. ANY KNOWING AND WILLFUL FALSIFICATION, COVER-UP, CONCEALMENT, MISREPRESENTATION, OR OMISSION OF A MATERIAL FACT FROM ANY WRITTEN OR ORAL STATEMENT, DOCUMENT, FORM OR OTHER REPRESENTATION OR DEVICE USED BY THE DEPARTMENT OF DEFENSE OR ANY OTHER FEDERAL AGENCY.

P. FAILING OR REFUSING TO ANSWER OR TO AUTHORIZE OTHERS TO ANSWER QUESTIONS OR PROVIDE INFORMATION REQUIRED BY A CONGRESSIONAL COMMITTEE, COURT, OR AGENCY IN THE COURSE OF AN OFFICIAL INQUIRY WHENEVER SUCH ANSWERS OR INFORMATION CONCERN RELEVANT AND MATERIAL MATTERS PERTINENT TO AN EVALUATION OF THE INDIVIDUAL'S TRUSTWORTHINESS, RELIABILITY, AND JUDGMENT.

Q. ACTS OF SEXUAL MISCONDUCT OR PERVERSION INDICATIVE OR MORAL TURPITUDE, POOR JUDGMENT, OR LACK OF REGARD FOR THE LAWS OF SOCIETY.

Section 3

TYPES AND SCOPE OF PERSONNEL SECURITY INVESTIGATIONS

2-300 GENERAL

THE TYPES OF PERSONNEL SECURITY INVESTIGATIONS AUTHORIZED BELOW VARY IN SCOPE OF INVESTIGATIVE EFFORT REQUIRED TO MEET THE PURPOSE OF THE PARTICULAR INVESTIGATION. NO OTHER TYPES ARE AUTHORIZED. THE SCOPE OF A PSI MAY BE NEITHER RAISED NOR LOWERED WITHOUT THE APPROVAL OF THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY.

2-301 NATIONAL AGENCY CHECK

ESSENTIALLY, A NAC IS A RECORDS CHECK OF DESIGNATED AGENCIES OF THE FEDERAL GOVERNMENT THAT MAINTAIN RECORD SYSTEMS CONTAINING INFORMATION RELEVANT TO MAKING A PERSONNEL SECURITY DETERMINATION. AN ENTNAC IS A NAC (SCOPE AS OUTLINED IN PARAGRAPH 1, APPENDIX B) CONDUCTED ON INDUCTEES AND FIRST-TERM ENLISTEES, BUT LACKING A TECHNICAL FINGERPRINT SEARCH. A NAC IS ALSO AN INTEGRAL PART OF EACH BI, SBI, AND PERIODIC REINVESTIGATION (PR). CHAPTER III PRESCRIBES WHEN A NAC IS REQUIRED.

2-302 NATIONAL AGENCY CHECK PLUS WRITTEN INQUIRIES

THE OFFICE OF PERSONNEL MANAGEMENT (OPM) CONDUCTS A NAC PLUS WRITTEN INQUIRIES (NACI) ON CIVILIAN EMPLOYEES FOR ALL DEPARTMENTS AND AGENCIES OF THE FEDERAL GOVERNMENT, PURSUANT TO E.O. 10450 (REFERENCE (G)). NACIS ARE CONSIDERED TO MEET THE INVESTIGATIVE REQUIREMENTS OF THIS REGULATION FOR A NONSENSITIVE OR NONCRITICAL SENSITIVE POSITION AND/OR UP TO A SECRET CLEARANCE AND, IN ADDITION TO THE NAC, INCLUDE COVERAGE OF LAW ENFORCEMENT AGENCIES, FORMER EMPLOYERS AND SUPERVISORS, REFERENCES, AND SCHOOLS COVERING THE LAST 5 YEARS.

2-307 PERIODIC REINVESTIGATION

AS REFERRED TO IN PARAGRAPH 3-700 AND OTHER NATIONAL DIRECTIVES, CERTAIN CATEGORIES OF DUTIES, CLEARANCE, AND ACCESS REQUIRE THE CONDUCT OF A PR EVERY FIVE YEARS ACCORDING TO THE SCOPE OUTLINED IN PARAGRAPH 5, APPENDIX B. THE PR SCOPE APPLIES TO MILITARY, CIVILIAN, CONTRACTOR, AND FOREIGN NATIONAL PERSONNEL.

2-308 PERSONAL INTERVIEW

INVESTIGATIVE EXPERIENCE OVER THE YEARS HAS DEMONSTRATED THAT, GIVEN NORMAL CIRCUMSTANCES, THE SUBJECT OF A PERSONNEL SECURITY INVESTIGATION IS THE BEST SOURCE OF ACCURATE AND RELEVANT INFORMATION CONCERNING THE MATTERS UNDER CONSIDERATION. FURTHER, RESTRICTIONS IMPOSED BY THE PRIVACY ACT OF 1974 (REFERENCE (M)) DICTATE THAT FEDERAL INVESTIGATIVE AGENCIES COLLECT INFORMATION TO THE GREATEST EXTENT PRACTICABLE DIRECTLY FROM THE SUBJECT WHEN THE INFORMATION MAY RESULT IN ADVERSE DETERMINATIONS ABOUT AN INDIVIDUAL'S RIGHTS, BENEFITS, AND PRIVILEGES UNDER FEDERAL PROGRAMS. ACCORDINGLY, PERSONAL INTERVIEWS ARE AN INTEGRAL PART OF THE DOD PERSONNEL SECURITY PROGRAM AND SHALL BE CONDUCTED IN ACCORDANCE WITH THE REQUIREMENTS SET FORTH IN THE FOLLOWING PARAGRAPHS OF THIS SECTION.

A. BI/PR. A PERSONAL INTERVIEW SHALL BE CONDUCTED BY A TRAINED DIS AGENT AS PART OF EACH BI AND PR.

B. RESOLVING ADVERSE INFORMATION. A PERSONAL INTERVIEW OF THE SUBJECT SHALL BE CONDUCTED BY A DIS AGENT (OR, WHEN AUTHORIZED, BY INVESTIGATIVE PERSONNEL OF OTHER DOD INVESTIGATIVE ORGANIZATIONS DESIGNATED IN THIS REGULATION TO CONDUCT PERSONNEL SECURITY INVESTIGATIONS), WHEN NECESSARY, AS PART OF EACH SPECIAL INVESTIGATIVE INQUIRY, AS WELL AS DURING THE COURSE OF INITIAL OR EXPANDED INVESTIGATIONS, TO RESOLVE OR CLARIFY ANY INFORMATION WHICH MAY IMPUGN THE SUBJECT'S MORAL CHARACTER, THREATEN THE SUBJECT'S FUTURE FEDERAL EMPLOYMENT, RAISE THE QUESTION OF SUBJECT'S SECURITY CLEARABILITY, OR BE OTHERWISE STIGMATIZING.

C. HOSTAGE SITUATION. A PERSONAL INTERVIEW SHALL BE CONDUCTED BY A DIS AGENT (OR, WHEN AUTHORIZED, BY INVESTIGATIVE PERSONNEL OF OTHER DOD INVESTIGATIVE ORGANIZATIONS DESIGNATED IN THIS REGULATION TO CONDUCT PERSONNEL SECURITY INVESTIGATIONS) IN THOSE INSTANCES IN WHICH AN INDIVIDUAL HAS IMMEDIATE FAMILY MEMBERS OR OTHER PERSONS BOUND BY TIES OF AFFECTION OR OBLIGATION WHO RESIDE IN A NATION WHOSE INTERESTS ARE INIMICAL TO THE INTERESTS OF THE UNITED STATES. (SEE PARAGRAPH 2-403.)

D. APPLICANTS/POTENTIAL NOMINEES FOR DOD MILITARY OR CIVILIAN POSITIONS REQUIRING ACCESS TO SCI OR OTHER POSITIONS REQUIRING AN SBI. A PERSONAL INTERVIEW OF THE INDIVIDUAL CONCERNED SHALL BE CONDUCTED, TO THE EXTENT FEASIBLE, AS PART OF THE SELECTION PROCESS FOR APPLICANTS/POTENTIAL NOMINEES FOR POSITIONS REQUIRING ACCESS TO SCI OR COMPLETION OF AN SBI. THE INTERVIEW SHALL BE CONDUCTED BY A DESIGNEE OF THE COMPONENT TO WHICH THE APPLICANT OR POTENTIAL NOMINEE IS ASSIGNED. CLERICAL PERSONNEL ARE NOT AUTHORIZED TO CONDUCT THESE INTERVIEWS. SUCH INTERVIEWS SHALL BE CONDUCTED UTILIZING RESOURCES IN THE ORDER OF PRIORITY INDICATED BELOW:

(1) EXISTING PERSONNEL SECURITY SCREENING SYSTEMS (E.G., AIR FORCE ASSESSMENT SCREENING PROGRAM, NAVAL SECURITY GROUP PERSONNEL SECURITY INTERVIEW PROGRAM, U.S. ARMY PERSONNEL SECURITY SCREENING PROGRAM); OR

2-303 DOD NATIONAL AGENCY CHECK PLUS WRITTEN INQUIRIES

DIS WILL CONDUCT A DNACI, CONSISTING OF THE SCOPE CONTAINED IN PARAGRAPH 2, APPENDIX B, FOR DOD MILITARY AND CONTRACTOR PERSONNEL FOR ACCESS TO SECRET INFORMATION. CHAPTER III PRESCRIBES WHEN A DNACI IS REQUIRED.

2-304 BACKGROUND INVESTIGATION

THE BI IS THE PRINCIPAL TYPE OF INVESTIGATION CONDUCTED WHEN AN INDIVIDUAL REQUIRES TOP SECRET CLEARANCE OR IS TO BE ASSIGNED TO A CRITICAL SENSITIVE POSITION. THE BI NORMALLY COVERS A 5-YEAR PERIOD AND CONSISTS OF A SUBJECT INTERVIEW, NAC, LACS, CREDIT CHECKS, DEVELOPED CHARACTER REFERENCES (3), EMPLOYMENT RECORDS CHECKS, EMPLOYMENT REFERENCES (3), AND SELECT SCOPING AS REQUIRED TO RESOLVE UNFAVORABLE OR QUESTIONABLE INFORMATION. (SEE PARAGRAPH 3, APPENDIX B.) CHAPTER III PRESCRIBES WHEN A BI IS REQUIRED.

2-305 SPECIAL BACKGROUND INVESTIGATION

A. AN SBI IS ESSENTIALLY A BI PROVIDING ADDITIONAL COVERAGE BOTH IN PERIOD OF TIME AS WELL AS SOURCES OF INFORMATION, SCOPED IN ACCORDANCE WITH THE PROVISIONS OF DCID 1/14 (REFERENCE (L)) BUT WITHOUT THE PERSONAL INTERVIEW. WHILE THE KIND OF COVERAGE PROVIDED FOR BY THE SBI DETERMINES ELIGIBILITY FOR ACCESS TO SCI, DOD HAS ADOPTED THIS COVERAGE FOR CERTAIN OTHER SPECIAL ACCESS PROGRAMS. CHAPTER III PRESCRIBES WHEN AN SBI IS REQUIRED.

B. THE OPM, FBI, CENTRAL INTELLIGENCE AGENCY (CIA), SECRET SERVICE, AND THE DEPARTMENT OF STATE CONDUCT SPECIALLY SCOPED BIs UNDER THE PROVISIONS OF DCID 1/14. ANY INVESTIGATION CONDUCTED BY ONE OF THE ABOVE-CITED AGENCIES UNDER DCID 1/14 STANDARDS IS CONSIDERED TO MEET THE SBI INVESTIGATIVE REQUIREMENTS OF THIS REGULATION.

C. THE DETAILED SCOPE OF AN SBI IS SET FORTH IN PARAGRAPH 4, APPENDIX B.

2-306 SPECIAL INVESTIGATIVE INQUIRY

A. A SPECIAL INVESTIGATIVE INQUIRY IS A PERSONNEL SECURITY INVESTIGATION CONDUCTED TO PROVE OR DISPROVE ALLEGATIONS RELATING TO THE CRITERIA OUTLINED IN PARAGRAPH 2-200 OF THIS REGULATION, EXCEPT CURRENT CRIMINAL ACTIVITIES (SEE PARAGRAPH 2-402.D), THAT HAVE ARISEN CONCERNING AN INDIVIDUAL UPON WHOM A PERSONNEL SECURITY DETERMINATION HAS BEEN PREVIOUSLY MADE AND WHO, AT THE TIME OF THE ALLEGATION, HOLDS A SECURITY CLEARANCE OR OTHERWISE OCCUPIES A POSITION THAT REQUIRES A TRUSTWORTHINESS DETERMINATION.

B. SPECIAL INVESTIGATIVE INQUIRIES ARE SCOPED AS NECESSARY TO ADDRESS THE SPECIFIC MATTERS REQUIRING RESOLUTION IN THE CASE CONCERNED AND GENERALLY CONSIST OF RECORD CHECKS AND/OR INTERVIEWS WITH POTENTIALLY KNOWLEDGEABLE PERSONS. AN SII MAY INCLUDE AN INTERVIEW WITH THE SUBJECT OF THE INVESTIGATION WHEN NECESSARY TO RESOLVE CONFLICTING INFORMATION AND/OR TO PROVIDE AN OPPORTUNITY TO REFUTE OR MITIGATE ADVERSE INFORMATION.

C. IN THOSE CASES WHEN THERE IS A DISAGREEMENT BETWEEN DEFENSE INVESTIGATIVE SERVICE (DIS) AND THE REQUESTER AS TO THE APPROPRIATE SCOPE OF THE INVESTIGATION, THE MATTER MAY BE REFERRED TO THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY FOR RESOLUTION.

(2) COMMANDER OF THE NOMINATING ORGANIZATION OR SUCH OFFICIAL AS HE OR SHE HAS DESIGNATED IN WRITING (E.G., DEPUTY COMMANDER, EXECUTIVE OFFICER, SECURITY OFFICER, SECURITY MANAGER, S-2, COUNTERINTELLIGENCE SPECIALIST, PERSONNEL SECURITY SPECIALIST, OR PERSONNEL OFFICER) Within DCAA, Security Specialists in the Headquarters, PD, or regions will conduct SCI interviews in accordance with this paragraph.; OR

(3) AGENTS OF INVESTIGATIVE AGENCIES IN DIRECT SUPPORT OF THE COMPONENT CONCERNED.

E. ADMINISTRATIVE PROCEDURES

(1) THE PERSONAL INTERVIEW REQUIRED BY PARAGRAPH D., ABOVE, SHALL BE CONDUCTED IN ACCORDANCE WITH APPENDIX G.

(2) FOR THOSE INVESTIGATIONS REQUESTED SUBSEQUENT TO THE PERSONAL INTERVIEW REQUIREMENTS OF PARAGRAPH D., ABOVE, THE FOLLOWING PROCEDURES APPLY:

(A) THE DD FORM 1879 (REQUEST FOR PERSONNEL SECURITY INVESTIGATION) SHALL BE ANNOTATED UNDER ITEM 20 (REMARKS) WITH THE STATEMENT "PERSONAL INTERVIEW CONDUCTED BY (CITE THE DUTY ASSIGNMENT OF THE DESIGNATED OFFICIAL (E.G., COMMANDER, SECURITY OFFICER, PERSONNEL SECURITY SPECIALIST, ETC.))" IN ALL CASES IN WHICH AN SBI IS SUBSEQUENTLY REQUESTED.

(B) UNFAVORABLE INFORMATION DEVELOPED THROUGH THE PERSONAL INTERVIEW REQUIRED BY PARAGRAPH D., ABOVE, WILL BE DETAILED IN A WRITTEN REPORT ATTACHED TO THE DD FORM 1879 TO INCLUDE FULL IDENTIFICATION OF THE INTERVIEWER. FAILURE TO PROVIDE SUCH INFORMATION MAY RESULT IN CONDUCT OF AN INCOMPLETE INVESTIGATION BY DIS.

(C) WHENEVER IT IS DETERMINED THAT IT IS NOT FEASIBLE TO CONDUCT THE PERSONAL INTERVIEW REQUIRED BY PARAGRAPH D. ABOVE, PRIOR TO REQUESTING THE SBI, THE DD FORM 1879 SHALL BE ANNOTATED UNDER ITEM 20 CITING THE REASON FOR NOT CONDUCTING THE INTERVIEW.

2-309 EXPANDED INVESTIGATION

IF ADVERSE OR QUESTIONABLE INFORMATION RELEVANT TO A SECURITY DETERMINATION IS DEVELOPED DURING THE CONDUCT OF A PERSONNEL SECURITY INVESTIGATION, REGARDLESS OF TYPE, THE INVESTIGATION SHALL BE EXPANDED, CONSISTENT WITH THE RESTRICTIONS IN PARAGRAPH 2-504, TO THE EXTENT NECESSARY TO SUBSTANTIATE OR DISPROVE THE ADVERSE OR QUESTIONABLE INFORMATION.

Section 4

AUTHORIZED PERSONNEL SECURITY INVESTIGATIVE AGENCIES

2-400 GENERAL

THE DIS PROVIDES A SINGLE CENTRALLY DIRECTED PERSONNEL SECURITY INVESTIGATIVE SERVICE TO CONDUCT PERSONNEL SECURITY INVESTIGATIONS WITHIN THE 50 STATES, DISTRICT OF COLUMBIA, AND COMMONWEALTH OF PUERTO RICO FOR DOD COMPONENTS, EXCEPT AS PROVIDED FOR IN DOD DIRECTIVE 5100.23 (REFERENCE (N)). DIS WILL REQUEST THE MILITARY DEPARTMENTS OR OTHER APPROPRIATE FEDERAL AGENCIES

TO ACCOMPLISH DOD INVESTIGATIVE REQUIREMENTS IN OTHER GEOGRAPHIC AREAS BEYOND THEIR JURISDICTION. NO OTHER DOD COMPONENT SHALL CONDUCT PERSONNEL SECURITY INVESTIGATIONS UNLESS SPECIFICALLY AUTHORIZED BY THE DEPUTY ASSISTANT SECRETARY OF DEFENSE (INTELLIGENCE AND SECURITY). IN CERTAIN INSTANCES PROVIDED FOR BELOW, THE DIS SHALL REFER AN INVESTIGATION TO OTHER INVESTIGATIVE AGENCIES.

2-401 SUBVERSIVE AFFILIATIONS

A. GENERAL. IN THE CONTEXT OF DOD INVESTIGATIVE POLICY, SUBVERSION REFERS ONLY TO SUCH CONDUCT AS IS FORBIDDEN BY THE LAWS OF THE UNITED STATES. SPECIFICALLY, THIS IS LIMITED TO INFORMATION CONCERNING THE ACTIVITIES OF INDIVIDUALS OR GROUPS THAT INVOLVE OR WILL INVOLVE THE VIOLATION OF FEDERAL LAW, FOR THE PURPOSE OF:

(1) OVERTHROWING THE GOVERNMENT OF THE UNITED STATES OR THE GOVERNMENT OF A STATE;

(2) SUBSTANTIALLY IMPAIRING FOR THE PURPOSE OF INFLUENCING U.S. GOVERNMENT POLICIES OR DECISIONS:

(A) THE FUNCTIONS OF THE GOVERNMENT OF THE UNITED STATES, OR

(B) THE FUNCTIONS OF THE GOVERNMENT OF A STATE;

(3) DEPRIVING PERSONS OF THEIR CIVIL RIGHTS UNDER THE CONSTITUTION OR LAWS OF THE UNITED STATES.

B. MILITARY DEPARTMENT/FBI JURISDICTION. ALLEGATIONS OF ACTIVITIES COVERED BY CRITERIA A. THROUGH F. OF PARAGRAPH 2-200 OF THIS REGULATION ARE IN THE EXCLUSIVE INVESTIGATIVE DOMAIN OF EITHER THE COUNTERINTELLIGENCE AGENCIES OF THE MILITARY DEPARTMENTS OR THE FBI, DEPENDING ON THE CIRCUMSTANCES OF THE CASE AND THE PROVISIONS OF THE AGREEMENT GOVERNING THE CONDUCT OF DEFENSE DEPARTMENT COUNTERINTELLIGENCE ACTIVITIES IN CONJUNCTION WITH THE FBI (REFERENCE (O)). WHENEVER ALLEGATIONS OF THIS NATURE ARE DEVELOPED, WHETHER BEFORE OR AFTER A SECURITY CLEARANCE HAS BEEN ISSUED OR DURING THE COURSE OF A PERSONNEL SECURITY INVESTIGATION CONDUCTED BY DIS, THEY SHALL BE REFERRED IMMEDIATELY TO EITHER THE FBI OR TO A MILITARY DEPARTMENT COUNTERINTELLIGENCE AGENCY AS APPROPRIATE. In accordance with DCAA Regulation 5240.1 (reference 1-100.k), all allegations of a nature referenced in this paragraph will be reported through the RSO to the ASO.

C. DIS JURISDICTION. ALLEGATIONS OF ACTIVITIES LIMITED TO THOSE SET FORTH IN CRITERION G. THROUGH Q. OF PARAGRAPH 2-200 OF THIS REGULATION SHALL BE INVESTIGATED BY DIS. Security specialists will initiate SIIs and furnish the ASO a copy when allegations under this section are received.

2-402 SUITABILITY INFORMATION

A. GENERAL. MOST DEROGATORY INFORMATION DEVELOPED THROUGH PERSONNEL SECURITY INVESTIGATIONS OF DOD MILITARY OR CIVILIAN PERSONNEL IS SO-CALLED SUITABILITY INFORMATION, THAT IS, INFORMATION PERTAINING TO ACTIVITIES OR SITUATIONS COVERED BY CRITERIA G. THROUGH Q. OF PARAGRAPH 2-200 OF THIS REGULATION. ALMOST ALL UNFAVORABLE PERSONNEL SECURITY DETERMINATIONS MADE BY

DOD AUTHORITIES ARE BASED ON DEROGATORY SUITABILITY INFORMATION, ALTHOUGH SUCH INFORMATION IS OFTEN USED AS A BASIS FOR UNFAVORABLE ADMINISTRATIVE ACTIONS NOT OF A SECURITY NATURE, SUCH AS ACTION UNDER THE UNIFORM CODE OF MILITARY JUSTICE OR REMOVAL FROM FEDERAL EMPLOYMENT UNDER OPM REGULATIONS.

B. PRE-CLEARANCE INVESTIGATION. DEROGATORY SUITABILITY INFORMATION, EXCEPT THAT COVERED IN D. BELOW, DEVELOPED DURING THE COURSE OF A PERSONNEL SECURITY INVESTIGATION, PRIOR TO THE ISSUANCE OF AN INDIVIDUAL'S PERSONNEL SECURITY CLEARANCE, SHALL BE INVESTIGATED BY DIS TO THE EXTENT NECESSARY TO CONFIRM OR REFUTE ITS APPLICABILITY TO CRITERIA G. THROUGH Q. OF PARAGRAPH 2-200.

C. POSTADJUDICATIVE INVESTIGATION. DEROGATORY SUITABILITY ALLEGATIONS, EXCEPT THOSE COVERED BY D. BELOW, ARISING SUBSEQUENT TO CLEARANCE REQUIRING INVESTIGATION TO RESOLVE AND TO DETERMINE THE INDIVIDUAL'S ELIGIBILITY FOR CONTINUED ACCESS TO CLASSIFIED INFORMATION, REINSTATEMENT OF CLEARANCE/ACCESS, OR RETENTION IN A SENSITIVE POSITION SHALL BE REFERRED TO DIS TO CONDUCT A SPECIAL INVESTIGATIVE INQUIRY. REINVESTIGATION OF INDIVIDUALS FOR ADJUDICATIVE RECONSIDERATION DUE TO THE PASSAGE OF TIME OR EVIDENCE OF FAVORABLE BEHAVIOR SHALL ALSO BE REFERRED TO DIS FOR INVESTIGATION. IN SUCH CASES, COMPLETION OF THE APPROPRIATE STATEMENT OF PERSONAL HISTORY BY THE INDIVIDUAL CONSTITUTES CONSENT TO BE INVESTIGATED. INDIVIDUAL CONSENT OR COMPLETION OF A STATEMENT OF PERSONAL HISTORY IS NOT REQUIRED WHEN PARAGRAPH 3-701 APPLIES. POSTADJUDICATION INVESTIGATION OF ALLEGATIONS OF A SUITABILITY NATURE REQUIRED TO SUPPORT OTHER TYPES OF UNFAVORABLE PERSONNEL SECURITY DETERMINATIONS OR DISCIPLINARY PROCEDURES INDEPENDENT OF A PERSONNEL SECURITY DETERMINATION SHALL BE HANDLED IN ACCORDANCE WITH APPLICABLE COMPONENT ADMINISTRATIVE REGULATIONS. THESE LATTER CATEGORIES OF ALLEGATIONS LIE OUTSIDE THE DOD PERSONNEL SECURITY PROGRAM AND ARE NOT A PROPER INVESTIGATIVE FUNCTION FOR DEPARTMENTAL COUNTERINTELLIGENCE ORGANIZATIONS, COMPONENT PERSONNEL SECURITY AUTHORITIES, OR DIS.

D. ALLEGATIONS OF CRIMINAL ACTIVITY. ALLEGATIONS OF POSSIBLE CRIMINAL CONDUCT ARISING DURING A PERSONNEL SECURITY INVESTIGATION SHALL BE REFERRED TO THE APPROPRIATE DEPARTMENT OF DEFENSE CRIMINAL INVESTIGATIVE AGENCY, MILITARY DEPARTMENT OR CIVILIAN JURISDICTION UNLESS THE LIMITATIONS IN PARAGRAPH 2-402D(1) THROUGH 2-402D(3) BELOW, APPLY. WHERE THE ALLEGATION CONCERNS A POTENTIAL VIOLATION OF THE UNIFORM CODE OF MILITARY JUSTICE, MILITARY DEPARTMENT INVESTIGATIVE AGENCIES HAVE PRIMARY INVESTIGATIVE JURISDICTION. THE FOLLOWING LIMITATIONS APPLY TO REFERRALS TO ALL LAW ENFORCEMENT AGENCIES, BOTH MILITARY AND CIVILIAN. Allegations under this paragraph, which may come to the attention of RSOs or the FDSO, will be referred to the ASO who will coordinate with the Agency counsel as necessary.

(1) ALLEGATIONS SHALL NOT BE REFERRED OR REPORTED TO LAW ENFORCEMENT AGENCIES WHERE AGREEMENTS WITH THE AGENCY OR IN CASES WHERE THERE IS NO AGREEMENT, PAST EXPERIENCE INDICATES THAT THE JURISDICTION DOES NOT HAVE A SUBSTANTIAL INTEREST IN PROSECUTION OF THE OFFENSE OR IN RECEIVING REPORTS OF THE OFFENSE EITHER DUE TO THE TYPE OR OFFENSE INVOLVED OR THE CIRCUMSTANCES UNDER WHICH IT OCCURRED.

(2) ALLEGATIONS ABOUT PRIVATE CONSENSUAL SEXUAL ACTS WITH ADULTS SHALL NOT BE REFERRED OR REPORTED TO LAW ENFORCEMENT AGENCIES OR TO MILITARY DEPARTMENTS (OTHER THAN CONSOLIDATED ADJUDICATION FACILITIES) FOR ANY PURPOSE. THAT LIMITATION DOES NOT APPLY TO ALLEGATIONS THAT AN INDIVIDUAL ATTEMPTED, SOLICITED, OR COMMITTED A CRIMINAL OFFENSE IN THE FOLLOWING CIRCUMSTANCES:

- (A) BY USING FORCE, COERCION, OR INTIMIDATION.
- (B) WITH A PERSON UNDER 17 YEARS OF AGE.
- (C) OPENLY IN PUBLIC VIEW.
- (D) FOR COMPENSATION OR WITH AN OFFER OF COMPENSATION TO ANOTHER INDIVIDUAL.
- (E) WHILE ON ACTIVE DUTY IN, OR ON DUTY IN A RESERVE COMPONENT OF, THE ARMED FORCES OF THE UNITED STATES AND

- 1 ABOARD A MILITARY VESSEL OR AIRCRAFT; OR
- 2 WITH A SUBORDINATE IN CIRCUMSTANCES THAT VIOLATE CUSTOMARY MILITARY SUPERIOR-SUBORDINATE RELATIONSHIPS.

EXCEPTIONS TO THAT LIMITATION WILL BE MADE ONLY WITH THE SPECIFIC WRITTEN AUTHORIZATION OF THE GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE, OR HIS OR HER DESIGNEE.

(3) INFORMATION ABOUT AN INDIVIDUAL'S SEXUAL ORIENTATION OR STATEMENTS BY AN INDIVIDUAL THAT HE OR SHE IS A HOMOSEXUAL OR BISEXUAL, OR WORDS TO THAT EFFECT, SHALL NOT BE REFERRED OR REPORTED TO LAW ENFORCEMENT AGENCIES OR TO MILITARY DEPARTMENTS (OTHER THAN CONSOLIDATED ADJUDICATION FACILITIES) FOR ANY PURPOSE. IF INVESTIGATIVE REPORTS CONTAINING SUCH INFORMATION ARE REFERRED TO LAW ENFORCEMENT AGENCIES OR MILITARY DEPARTMENTS FOR OTHER REASONS, INFORMATION SUBJECT TO THE LIMITATIONS IN THIS PARAGRAPH WILL BE REMOVED.

2-403 HOSTAGE SITUATIONS

A. GENERAL. A HOSTAGE SITUATION EXISTS WHEN A MEMBER OF SUBJECT'S IMMEDIATE FAMILY OR SUCH OTHER PERSON TO WHOM THE INDIVIDUAL IS BOUND BY OBLIGATION OR AFFECTION RESIDES IN A COUNTRY WHOSE INTERESTS ARE INIMICAL TO THE INTERESTS OF THE UNITED STATES. THE RATIONALE UNDERLYING THIS CATEGORY OF INVESTIGATION IS BASED ON THE POSSIBILITY THAT AN INDIVIDUAL IN SUCH A SITUATION MIGHT BE COERCED, INFLUENCED, OR PRESSURED TO ACT CONTRARY TO THE INTERESTS OF NATIONAL SECURITY. In such cases, DCAA applicants and employees must be requested to provide information about the above individual(s) who are living in such a country. The data will be provided on SF 86, as indicated in section 1.D, Enclosure 3.

B. DIS JURISDICTION. IN THE ABSENCE OF EVIDENCE OF ANY COERCION, INFLUENCE OR PRESSURE, HOSTAGE INVESTIGATIONS ARE EXCLUSIVELY A PERSONNEL SECURITY MATTER, RATHER THAN COUNTERINTELLIGENCE, AND ALL SUCH INVESTIGATIONS SHALL BE CONDUCTED BY DIS.

C. MILITARY DEPARTMENT AND/OR FBI JURISDICTION. SHOULD INDICATIONS BE DEVELOPED THAT HOSTILE INTELLIGENCE IS TAKING ANY ACTION SPECIFICALLY DIRECTED AGAINST THE INDIVIDUAL CONCERNED--OR SHOULD THERE EXIST ANY OTHER EVIDENCE THAT THE INDIVIDUAL IS ACTUALLY BEING COERCED, INFLUENCED, OR PRESSURED BY AN ELEMENT INIMICAL TO THE INTERESTS OF NATIONAL SECURITY--THEN THE CASE BECOMES A COUNTERINTELLIGENCE MATTER (OUTSIDE OF INVESTIGATIVE JURISDICTION OF DIS) TO BE REFERRED TO THE APPROPRIATE MILITARY DEPARTMENT OR THE FBI FOR INVESTIGATION.

MARCH 1996

2-404 OVERSEAS PERSONNEL SECURITY INVESTIGATIONS

PERSONNEL SECURITY INVESTIGATIONS REQUIRING INVESTIGATION OVERSEAS SHALL BE CONDUCTED UNDER THE DIRECTION AND CONTROL OF DIS BY THE APPROPRIATE MILITARY DEPARTMENT INVESTIGATIVE ORGANIZATION. ONLY POSTADJUDICATION INVESTIGATIONS INVOLVING AN OVERSEAS SUBJECT MAY BE REFERRED BY THE REQUESTER DIRECTLY TO THE MILITARY DEPARTMENT INVESTIGATIVE ORGANIZATION HAVING INVESTIGATIVE RESPONSIBILITY IN THE OVERSEAS AREA CONCERNED (SEE APPENDIX J) WITH A COPY OF THE INVESTIGATIVE REQUEST SENT TO DIS. IN SUCH CASES, THE MILITARY DEPARTMENT INVESTIGATIVE AGENCY WILL COMPLETE THE INVESTIGATION, FORWARD THE COMPLETED REPORT OF INVESTIGATION DIRECTLY TO DIS, WITH A COPY TO THE REQUESTER.

SECTION 5**LIMITATIONS AND RESTRICTIONS****2-500 AUTHORIZED REQUESTERS AND PERSONNEL SECURITY DETERMINATION AUTHORITIES**

PERSONNEL SECURITY INVESTIGATIONS MAY BE REQUESTED AND PERSONNEL SECURITY CLEARANCES (INCLUDING SPECIAL ACCESS AUTHORIZATIONS AS INDICATED) GRANTED ONLY BY THOSE AUTHORITIES DESIGNATED IN PARAGRAPH 5-101 AND APPENDIX F. For authorized requesters of personnel security investigations, see paragraph 5-101. The WHS CAF adjudicates personnel security investigations and issues security clearances for DCAA personnel.

2-501 LIMIT INVESTIGATIONS AND ACCESS

THE NUMBER OF PERSONS CLEARED FOR ACCESS TO CLASSIFIED INFORMATION SHALL BE KEPT TO A MINIMUM, CONSISTENT WITH THE REQUIREMENTS OF OPERATIONS. SPECIAL ATTENTION SHALL BE GIVEN TO ELIMINATING UNNECESSARY CLEARANCES AND REQUESTS FOR PERSONNEL SECURITY INVESTIGATIONS. Heads of principal staff elements, the Agency Security Officer, Headquarters Security Specialists (for Headquarters), security officers for regional offices and FD, PAO managers in field audit offices (through their regional security officers), and Managers, DCAI and TSC will sign requests for security clearances and ensure that clearances are requested only for those employees whose duties require access to classified information. Clearance requests must be appropriately justified, with duration of need specified on DCAA Form 5210-31. Security specialists will ensure that managers periodically reevaluate the need for clearances within their areas, and initiate withdrawal actions by obtaining Security Termination Statements (DCAA Form 5210-3) when access is no longer required, in accordance with paragraph 9-204 of this manual, and section 10-105 of DCAA Manual 5205.1 (reference 1-100.g).

2-502 COLLECTION OF INVESTIGATIVE DATA

TO THE GREATEST EXTENT PRACTICABLE, PERSONAL INFORMATION RELEVANT TO PERSONNEL SECURITY DETERMINATIONS SHALL BE OBTAINED DIRECTLY FROM THE SUBJECT OF A PERSONNEL SECURITY INVESTIGATION. SUCH ADDITIONAL INFORMATION REQUIRED TO MAKE THE NECESSARY PERSONNEL SECURITY DETERMINATION SHALL BE OBTAINED AS APPROPRIATE FROM KNOWLEDGEABLE PERSONAL SOURCES, PARTICULARLY SUBJECT'S PEERS, AND THROUGH CHECKS OF RELEVANT RECORDS INCLUDING SCHOOL, EMPLOYMENT, CREDIT, MEDICAL, AND LAW ENFORCEMENT RECORDS. In addition to the provisions of this section, refer and adhere to provisions of DCAA Regulation 5200.7, Acquisition

of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense (reference 1-100.u).

2-503 PRIVACY ACT NOTIFICATION

WHENEVER PERSONAL INFORMATION IS SOLICITED FROM AN INDIVIDUAL PREPARATORY TO THE INITIATION OF A PERSONNEL SECURITY INVESTIGATION, THE INDIVIDUAL MUST BE INFORMED OF (1) THE AUTHORITY (STATUTE OR EXECUTIVE ORDER THAT AUTHORIZED SOLICITATION); (2) THE PRINCIPAL PURPOSE OR PURPOSES FOR WHICH THE INFORMATION IS TO BE USED; (3) THE ROUTINE USES TO BE MADE OF THE INFORMATION; (4) WHETHER FURNISHING SUCH INFORMATION IS MANDATORY OR VOLUNTARY; (5) THE EFFECT ON THE INDIVIDUAL, IF ANY, OF NOT PROVIDING THE INFORMATION AND (6) THAT SUBSEQUENT USE OF THE DATA MAY BE EMPLOYED AS PART OF AN APERIODIC, RANDOM PROCESS TO SCREEN AND EVALUATE CONTINUED ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION.

2-504 RESTRICTIONS ON INVESTIGATORS

INVESTIGATIONS SHALL BE CARRIED OUT INSOFAR AS POSSIBLE TO COLLECT ONLY AS MUCH INFORMATION AS IS RELEVANT AND NECESSARY FOR A PROPER PERSONNEL SECURITY DETERMINATION. QUESTIONS CONCERNING PERSONAL AND DOMESTIC AFFAIRS, NATIONAL ORIGIN, FINANCIAL MATTERS, AND THE STATUS OF PHYSICAL HEALTH SHOULD BE AVOIDED UNLESS THE QUESTION IS RELEVANT TO THE CRITERIA OF PARAGRAPH 2-200 OF THIS REGULATION. SIMILARLY, THE PROBING OF A PERSON'S THOUGHTS OR BELIEFS AND QUESTIONS ABOUT CONDUCT THAT HAVE NO PERSONNEL SECURITY IMPLICATIONS ARE UNWARRANTED. WHEN CONDUCTING INVESTIGATIONS UNDER THE PROVISIONS OF THIS REGULATION, INVESTIGATORS SHALL:

A. INVESTIGATE ONLY CASES OR PERSONS ASSIGNED WITHIN THEIR OFFICIAL DUTIES.

B. INTERVIEW SOURCES ONLY WHERE THE INTERVIEW CAN TAKE PLACE IN REASONABLY PRIVATE SURROUNDINGS.

C. ALWAYS PRESENT CREDENTIALS AND INFORM SOURCES OF THE REASONS FOR THE INVESTIGATION. INFORM SOURCES OF THE SUBJECT'S ACCESSIBILITY TO THE INFORMATION TO BE PROVIDED AND TO THE IDENTITY OF THE SOURCES PROVIDING THE INFORMATION. RESTRICTIONS ON INVESTIGATORS RELATING TO PRIVACY ACT ADVISEMENTS TO SUBJECTS OF PERSONNEL SECURITY INVESTIGATIONS ARE OUTLINED IN PARAGRAPH 2-503.

D. FURNISH ONLY NECESSARY IDENTITY DATA TO A SOURCE, AND REFRAIN FROM ASKING QUESTIONS IN SUCH A MANNER AS TO INDICATE THAT THE INVESTIGATOR IS IN POSSESSION OF DEROGATORY INFORMATION CONCERNING THE SUBJECT OF THE INVESTIGATION.

E. REFRAIN FROM USING, UNDER ANY CIRCUMSTANCES, COVERT OR SURREPTITIOUS INVESTIGATIVE METHODS, DEVICES, OR TECHNIQUES INCLUDING MAIL COVERS, PHYSICAL OR PHOTOGRAPHIC SURVEILLANCE, VOICE ANALYZERS, INSPECTION OF TRASH, PAID INFORMANTS, WIRETAP, OR EAVESDROPPING DEVICES.

F. REFRAIN FROM ACCEPTING ANY CASE IN WHICH THE INVESTIGATOR KNOWS OF CIRCUMSTANCES THAT MIGHT ADVERSELY AFFECT HIS FAIRNESS, IMPARTIALITY, OR OBJECTIVITY.

G. REFRAIN, UNDER ANY CIRCUMSTANCES, FROM CONDUCTING PHYSICAL SEARCHES OF SUBJECT OR HIS PROPERTY.

H. REFRAIN FROM ATTEMPTING TO EVALUATE MATERIAL CONTAINED IN MEDICAL FILES. MEDICAL FILES SHALL BE EVALUATED FOR PERSONNEL SECURITY PROGRAM PURPOSES ONLY BY SUCH PERSONNEL AS ARE DESIGNATED BY DOD MEDICAL AUTHORITIES. HOWEVER, REVIEW AND COLLECTION OF MEDICAL RECORD INFORMATION MAY BE ACCOMPLISHED BY AUTHORIZED INVESTIGATIVE PERSONNEL.

2-505 POLYGRAPH RESTRICTIONS

THE POLYGRAPH MAY BE USED AS A PERSONNEL SECURITY SCREENING MEASURE ONLY IN THOSE LIMITED INSTANCES AUTHORIZED BY THE SECRETARY OF DEFENSE IN DOD DIRECTIVE 5210.48, (REFERENCE (P)). Polygraph will be used within DCAA in accordance with provisions of DCAA Regulation 5210.7 (reference 1-100.s).

CHAPTER III
PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS

Section 1

SENSITIVE POSITIONS

3-100 DESIGNATION OF SENSITIVE POSITIONS

CERTAIN CIVILIAN POSITIONS WITHIN THE DEPARTMENT OF DEFENSE ENTAIL DUTIES OF SUCH A SENSITIVE NATURE, INCLUDING ACCESS TO CLASSIFIED INFORMATION, THAT THE MISCONDUCT, MALFEASANCE, OR NONFEASANCE OF AN INCUMBENT IN AN ANY SUCH POSITION COULD RESULT IN AN UNACCEPTABLY ADVERSE IMPACT UPON THE NATIONAL SECURITY. THESE POSITIONS ARE REFERRED TO IN THIS REGULATION AS SENSITIVE POSITIONS. IT IS VITAL TO THE NATIONAL SECURITY THAT GREAT CARE BE EXERCISED IN THE SELECTION OF INDIVIDUALS TO FILL SUCH POSITIONS. SIMILARLY, IT IS IMPORTANT THAT ONLY POSITIONS WHICH TRULY MEET ONE OR MORE OF THE CRITERIA SET FORTH IN PARAGRAPH 3-101 BE DESIGNATED AS SENSITIVE. Redesignation of any position without the prior approval of the ASO is prohibited. Under no circumstances will a position be temporarily redesignated at a lower sensitivity level in order to fill it prior to completion of the required investigation.

3-101 CRITERIA FOR SECURITY DESIGNATION OF POSITIONS

EACH CIVILIAN POSITION WITHIN THE DEPARTMENT OF DEFENSE SHALL BE CATEGORIZED, WITH RESPECT TO SECURITY SENSITIVITY, AS EITHER NONSENSITIVE, NONCRITICAL-SENSITIVE, OR CRITICAL-SENSITIVE.

A. THE CRITERIA TO BE APPLIED IN DESIGNATING A POSITION AS SENSITIVE ARE:

(1) CRITICAL-SENSITIVE

(A) ACCESS TO TOP SECRET INFORMATION.

(B) DEVELOPMENT OR APPROVAL OF PLANS, POLICIES, OR PROGRAMS THAT AFFECT THE OVERALL OPERATIONS OF THE DEPARTMENT OF DEFENSE OR OF A DOD COMPONENT.

(C) DEVELOPMENT OR APPROVAL OF WAR PLANS, PLANS OR PARTICULARS OF FUTURE MAJOR OR SPECIAL OPERATIONS OF WAR, OR CRITICAL AND EXTREMELY IMPORTANT ITEMS OF WAR.

(D) INVESTIGATIVE AND CERTAIN INVESTIGATIVE SUPPORT DUTIES, THE ISSUANCE OF PERSONNEL SECURITY CLEARANCES OR ACCESS AUTHORIZATIONS, OR THE MAKING OF PERSONNEL SECURITY DETERMINATIONS.

(E) FIDUCIARY, PUBLIC CONTACT, OR OTHER DUTIES DEMANDING THE HIGHEST DEGREE OF PUBLIC TRUST.

(F) DUTIES FALLING UNDER SPECIAL ACCESS PROGRAMS.

(G) CATEGORY I AUTOMATED DATA PROCESSING (ADP) POSITIONS.

(H) ANY OTHER POSITION SO DESIGNATED BY THE HEAD OF THE COMPONENT OR DESIGNEE.

(2) NONCRITICAL-SENSITIVE

(A) ACCESS TO SECRET OR CONFIDENTIAL INFORMATION.

(B) SECURITY POLICE/PROVOST MARSHAL-TYPE DUTIES INVOLVING THE ENFORCEMENT OF LAW AND SECURITY DUTIES INVOLVING THE PROTECTION AND SAFEGUARDING OF DOD PERSONNEL AND PROPERTY.

(C) CATEGORY II AUTOMATED DATA PROCESSING POSITIONS.

(D) DUTIES INVOLVING EDUCATION AND ORIENTATION OF DOD PERSONNEL.

(E) DUTIES INVOLVING THE DESIGN, OPERATION, OR MAINTENANCE OF INTRUSION DETECTION SYSTEMS DEPLOYED TO SAFEGUARD DOD PERSONNEL AND PROPERTY.

(F) ANY OTHER POSITION SO DESIGNATED BY THE HEAD OF THE COMPONENT OR DESIGNEE.

B. ALL OTHER POSITIONS SHALL BE DESIGNATED AS NONSENSITIVE.

3-102 AUTHORITY TO DESIGNATE SENSITIVE POSITIONS

THE AUTHORITY TO DESIGNATE SENSITIVE POSITIONS IS LIMITED TO THOSE AUTHORITIES DESIGNATED IN PARAGRAPH G, APPENDIX F. THESE AUTHORITIES SHALL DESIGNATE EACH POSITION WITHIN THEIR JURISDICTION AS TO ITS SECURITY SENSITIVITY AND MAINTAIN THESE DESIGNATIONS CURRENT VIS-A-VIS THE SPECIFIC DUTIES OF EACH POSITION. The ASO and CPS security specialists are authorized to designate sensitivity for all positions.

3-103 LIMITATION OF SENSITIVE POSITIONS

IT IS THE RESPONSIBILITY OF THOSE AUTHORITIES AUTHORIZED TO DESIGNATE SENSITIVE POSITIONS TO INSURE THAT (1) ONLY THOSE POSITIONS ARE DESIGNATED AS SENSITIVE THAT MEET THE CRITERIA OF PARAGRAPH 3-101 ABOVE AND (2) THAT THE DESIGNATION OF SENSITIVE POSITIONS IS HELD TO A MINIMUM CONSISTENT WITH MISSION REQUIREMENTS. DESIGNATING AUTHORITIES SHALL MAINTAIN AN ACCOUNTING OF THE NUMBER OF SENSITIVE POSITIONS BY CATEGORY, I.E., CRITICAL OR NONCRITICAL-SENSITIVE. SUCH INFORMATION WILL BE INCLUDED IN ANNUAL REPORT REQUIRED IN CHAPTER XI. (This reporting requirement, the Annual Personnel Security Program Management Data Report, RCN:DD-POL(A)1749, was canceled by OASD(C3I) by memorandum dated 6 September 1991.)

3-104 BILLET CONTROL SYSTEM FOR TOP SECRET

A. TO STANDARDIZE AND CONTROL THE ISSUANCE OF TOP SECRET CLEARANCES WITHIN THE DEPARTMENT OF DEFENSE, A SPECIFIC DESIGNATED BILLET MUST BE ESTABLISHED AND MAINTAINED FOR ALL DOD MILITARY AND CIVILIAN POSITIONS REQUIRING ACCESS TO TOP SECRET INFORMATION. ONLY PERSONS OCCUPYING THESE BILLET POSITIONS WILL BE AUTHORIZED A TOP SECRET CLEARANCE. IF AN INDIVIDUAL DEPARTS FROM A TOP SECRET BILLET TO A BILLET/POSITION INVOLVING A LOWER LEVEL CLEARANCE, THE TOP SECRET CLEARANCE WILL BE ADMINISTRATIVELY RESCINDED. THIS TOP SECRET BILLET

REQUIREMENT IS IN ADDITION TO THE EXISTING BILLET STRUCTURE MAINTAINED FOR SCI ACCESS. The ASO is responsible for establishing and maintaining Top Secret billets. Billets have been established by title for both Headquarters and regional personnel, and a block of billets has been established for FD personnel. Only persons occupying these positions will be authorized a Top Secret clearance. When an individual no longer requires access to Top Secret, the clearance will be downgraded or administratively withdrawn and the individual's name will be removed from the billet.

B. EACH REQUEST TO DIS FOR A BI OR SBI THAT INVOLVES ACCESS TO TOP SECRET OR SCI INFORMATION WILL REQUIRE INCLUSION OF THE APPROPRIATE BILLET REFERENCE ON THE REQUEST FOR INVESTIGATION. EACH COMPONENT HEAD SHOULD INCORPORATE, TO THE EXTENT FEASIBLE, THE TOP SECRET BILLET STRUCTURE INTO THE COMPONENT MANPOWER UNIT MANNING DOCUMENT. SUCH A PROCEDURE SHOULD MINIMIZE THE TIME AND EFFORT REQUIRED TO MAINTAIN SUCH A BILLET STRUCTURE. Security specialists requesting investigations on employees who require a Top Secret clearance will obtain a billet control number from CPS to include on DD Form 1879 prior to its submission to DIS.

C. A REPORT ON THE NUMBER OF ESTABLISHED TOP SECRET BILLETS WILL BE SUBMITTED EACH YEAR TO THE DUSD(P) AS PART OF THE ANNUAL CLEARANCE REPORT REFERRED TO IN CHAPTER XI. (This reporting requirement, the Annual Personnel Security Program Management Data Report, RCN:DD-POL(A)1749, was canceled by OASD(C3I) by memorandum dated 6 September 1991.)

Section 2

CIVILIAN EMPLOYMENT

3-200 GENERAL

THE APPOINTMENT OF EACH CIVILIAN EMPLOYEE IN ANY DOD COMPONENT IS SUBJECT TO INVESTIGATION, EXCEPT FOR REAPPOINTMENT WHEN THE BREAK IN EMPLOYMENT IS LESS THAN 12 MONTHS. THE TYPE OF INVESTIGATION REQUIRED IS SET FORTH IN THIS SECTION ACCORDING TO POSITION SENSITIVITY.

The Agency Security Officer will be notified of all reassignments which result in a change of position sensitivity.

3-201 NONSENSITIVE POSITIONS

IN ACCORDANCE WITH THE OPM FEDERAL PERSONNEL MANUAL (REFERENCE (CC)), A NACI SHALL BE REQUESTED NOT LATER THAN 3 WORKING DAYS AFTER A PERSON IS APPOINTED TO A NONSENSITIVE POSITION. ALTHOUGH THERE IS NORMALLY NO INVESTIGATION REQUIREMENT FOR PER DIEM, INTERMITTENT, TEMPORARY OR SEASONAL EMPLOYEES IN NONSENSITIVE POSITIONS PROVIDED SUCH EMPLOYMENT DOES NOT EXCEED AN AGGREGATE OF 120 DAYS IN EITHER A SINGLE CONTINUOUS OR SERIES OF APPOINTMENTS, A NAC MAY BE REQUESTED OF DIS WHERE DEEMED APPROPRIATE BY THE EMPLOYING ACTIVITY. Appointments to nonsensitive positions may be made without preliminary investigation. Following such appointments, a request for a NACI will be initiated as prescribed in this paragraph, within seven days of appointment. Security investigations are not required for appointments to nonsensitive positions limited in tenure to a total of 120 days or less. Individuals whose appointments to limited tenure positions are subsequently extended beyond 120 days, or who are to be transferred to a sensitive position, are subject to the investigative

MARCH 1996

requirements set forth in this manual. Such cases will be processed in accordance with the applicable provisions of Chapter III and Enclosure 3 of this manual.

3-202 NONCRITICAL-SENSITIVE POSITIONS

A. A NACI SHALL BE REQUESTED AND THE NAC PORTION FAVORABLY COMPLETED BEFORE A PERSON IS APPOINTED TO A NONCRITICAL-SENSITIVE POSITION (FOR EXCEPTIONS SEE PARAGRAPH 3-204). AN ENTNAC, NAC OR DNACI CONDUCTED DURING MILITARY OR CONTRACTOR EMPLOYMENT MAY ALSO BE USED FOR APPOINTMENT PROVIDED A NACI HAS BEEN REQUESTED FROM OPM AND THERE IS NO MORE THAN 12 MONTHS BREAK IN SERVICE SINCE COMPLETION OF THE INVESTIGATION. DCAA appointees to noncritical-sensitive positions will be subject to the investigative requirements as prescribed in this manual. No person will be appointed to a noncritical-sensitive position until, as a minimum, a NAC has been completed with satisfactory results. However, in the event of an emergency, an exception is permitted, in that such a position may be filled for a limited period by an individual on whom a NACI has been requested but not completed, providing that the appropriate official has granted an employment waiver and the provisions of paragraph 3-204 below have been met. This same procedure applies to individuals from temporary services who will not have access to classified information, except that a request for NAC will be submitted to DIS using SF 85P and FD 258.

B. SEASONAL EMPLOYEES (INCLUDING SUMMER HIRES) NORMALLY DO NOT REQUIRE ACCESS TO CLASSIFIED INFORMATION. FOR THOSE REQUIRING ACCESS TO CLASSIFIED INFORMATION, THE APPROPRIATE INVESTIGATION IS REQUIRED. THE REQUEST FOR THE NAC (OR NACI) SHOULD BE SUBMITTED TO DIS BY ENTERING "SH" (SUMMER HIRE) IN RED LETTERS APPROXIMATELY ONE INCH HIGH ON THE DD FORM 398-2, PERSONNEL SECURITY QUESTIONNAIRE (NATIONAL AGENCY CHECKLIST). ADDITIONALLY, TO ENSURE EXPEDITED PROCESSING BY DIS, SUMMER HIRE REQUESTS SHOULD BE ASSEMBLED AND FORWARDED TO DIS IN BUNDLES, WHEN APPROPRIATE. The position descriptions for seasonal employees (including summer hires) in DCAA are designated as noncritical-sensitive if the incumbent is assigned duties which involve access to sensitive information (which includes audit reports issued by the Agency). Although the expedited NAC required by this section is not necessary, provided that such employees will not have access to classified information, a NACI will be initiated in accordance with section 3-202.A, and exceptions processed in accordance with section 3-204.A of this manual.

C. An applicant for noncritical-sensitive position who occupies a non-sensitive position, and has a previous NACI conducted for a nonsensitive position, will be required to complete SF 86 if access will be required, or SF 85P if no access will be required. A new investigation will not be initiated unless the prior NACI is no longer current or complete, or the completed SF 85P or 86 presents issues that postdate prior adjudication.

3-203 CRITICAL-SENSITIVE POSITIONS

A BI SHALL BE FAVORABLY COMPLETED PRIOR TO APPOINTMENT TO CRITICAL-SENSITIVE POSITIONS (FOR EXCEPTIONS SEE PARAGRAPH 3-204). CERTAIN CRITICAL-SENSITIVE POSITIONS REQUIRE A PREAPPOINTMENT SBI IN ACCORDANCE WITH SECTION 5 OF THIS CHAPTER. PREAPPOINTMENT BIs AND SBIs WILL BE CONDUCTED BY DIS.

a. Enclosure 2 is a list of critical-sensitive positions in the Regions. A list of critical-sensitive positions in Headquarters is maintained in CPS. No person will be appointed to a critical-sensitive position prior to a

favorably completed SSBI. An exception is that, in an emergency, the position may be occupied pending completion of a SSBI provided a previous NAC or NACI has been completed and favorably adjudicated, and the Assistant Director, Resources, has granted an employment waiver in accordance with the provisions of paragraph 3-204 below have been met.

b. An incumbent employee on whom a SSBI has not been completed, and who is occupying a position at the time it is designated critical-sensitive, may continue to occupy such a position pending completion of a SSBI, provided a favorable NAC or NACI has been completed. A request for a SSBI must be submitted to DIS immediately after redesignation of an encumbered position.

3-204 EXCEPTIONS

Prior to granting exceptions in accordance with this paragraph, inquiries of previous employer(s) (i.e., supervisor or personnel office), college professors or references, as appropriate, will be conducted. The results of the inquiries will assist personnel management specialists in making a suitability decision and security specialists in making a recommendation to waive or not waive the investigative requirement. A favorable review of employment applications, security questionnaires, and all inquiries will be completed by a security specialist prior to recommending a waiver of required security investigation.

A. NONCRITICAL-SENSITIVE. IN AN EMERGENCY, A NONCRITICAL-SENSITIVE POSITION MAY BE OCCUPIED PENDING THE COMPLETION OF THE NACI IF THE HEAD OF THE REQUESTING ORGANIZATION FINDS THAT THE DELAY IN APPOINTMENT WOULD BE HARMFUL TO THE NATIONAL SECURITY AND SUCH FINDING IS REDUCED TO WRITING AND MADE PART OF THE RECORD. IN SUCH INSTANCES, THE POSITION MAY BE FILLED ONLY AFTER THE NACI HAS BEEN REQUESTED. The Assistant Director, Resources, for Headquarters positions, regional directors for regional positions, and Director, Field Detachment for FD positions may approve waivers (DCAA Form 5210-43) in accordance with provisions of this paragraph. The head of a principal staff element and division chiefs (for Headquarters) and the Regional Resources Manager (for regions) are authorized to request waivers. The responsible security officer will mail the request for a NACI investigation to the USOPM-FIPC before emergency appointments are made, by waiver, to noncritical-sensitive positions.

B. CRITICAL-SENSITIVE. IN AN EMERGENCY, A CRITICAL-SENSITIVE POSITION MAY BE OCCUPIED PENDING COMPLETION OF THE BI (OR SBI, AS APPROPRIATE) IF THE HEAD OF THE REQUESTING ORGANIZATION FINDS THAT THE DELAY IN APPOINTMENT WOULD BE HARMFUL TO THE NATIONAL SECURITY AND SUCH FINDING IS REDUCED TO WRITING AND MADE A PART OF THE RECORD. IN SUCH INSTANCES, THE POSITION MAY BE FILLED ONLY WHEN THE NAC PORTION OF THE BI (OR SBI) OR A PREVIOUS VALID NACI, NAC OR ENTNAC HAS BEEN COMPLETED AND FAVORABLY ADJUDICATED. Only the Assistant Director, Resources, may sign a waiver (DCAA Form 5210-43) based on a request by the head of a principal staff element, a division chief, the Director, Field Detachment, or a regional director. (This authority may be exercised by anyone designated in writing to act in the capacity of the above officials, however, it may not be further delegated.) The NAC portion of the SSBI or a previous favorable NAC or NACI (provided there has been no break in service of more than 24 months since investigation) will be verified and favorably adjudicated prior to submitting the waiver for signature by the Assistant Director, Resources. In cases when a NAC must be completed before a waiver is considered, security specialists should ensure the earliest receipt of NAC results by marking item 6 of DD Form 1879 to

reflect that advance notification be forwarded to WHS. In all cases, the request for SSBI must be mailed to DIS before the Assistant Director, Resources will consider a waiver request.

c. Effects of an employment waiver. The granting of an employment waiver will be for the purpose of appointment only. Under no circumstances will any person be given access to classified information until the ASO has issued an interim security clearance or the WHS CAF has issued a final security clearance. Approved waivers (DCAA Forms 5210-43) of preappointment security investigations will be filed on the left side of the official personnel folders of the appointees concerned.

d. Guidelines for conducting employment inquiries on applicants

1. If the applicant is employed, contact the current employer; if unemployed, contact the most recent employer. Contact one or two additional references to assess the applicant's loyalty and trustworthiness. For applicants currently employed with the Federal Government, contact the current supervisor.

2. If the applicant is currently a college student or recently graduated, conduct at least two inquiries to include a college professor and/or references. Inquiries of students employed in temporary positions during the previous four months need not be made.

3. If an applicant requests that inquiry not be made of their current employer, the applicant should be contacted and asked to reconsider this request. The applicant should be advised that we must obtain information about their character, reputation, and fitness prior to considering them for a sensitive position within the Agency. The applicant should understand that we will be required to waive the USOPM and DoD investigative requirements to hire them and that cannot be done without current information to make a suitability and security determination.

4. If the applicant insists that contact not be made with their current employer, but still wishes to be considered for a sensitive position, a waiver will not be further considered. The employee should be told that an investigation must be favorably completed prior to appointment and that inquiries will be made by USOPM to the current employer during the investigation. If this procedure is unacceptable to the applicant, consideration for employment should be discontinued.

3-205 MOBILIZATION OF DOD CIVILIAN RETIREES

THE REQUIREMENTS CONTAINED IN PARAGRAPH 3-200 OF THIS SECTION, REGARDING THE TYPE OF INVESTIGATION REQUIRED BY POSITION SENSITIVITY FOR DOD CIVILIAN RETIREES TEMPORARY APPOINTMENT WHEN THE BREAK IN EMPLOYMENT IS GREATER THAN 12 MONTHS, SHOULD EITHER BE EXPEDITED OR WAIVED FOR THE PURPOSES OF MOBILIZING SELECTED REEMPLOYED ANNUITANTS UNDER THE PROVISIONS OF TITLE 5, UNITED STATES CODE, DEPENDING UPON THE DEGREE OF SENSITIVITY OF THE POSITION TO WHICH ASSIGNED. PARTICULAR PRIORITY SHOULD BE AFFORDED TO NEWLY ASSIGNED PERSONNEL ASSIGNED TO THE DEFENSE INTELLIGENCE AND SECURITY AGENCIES WITH RESPECT TO GRANTING SECURITY CLEARANCES IN AN EXPEDITIOUS MANNER UNDER PARAGRAPH 3-200 OF THIS SECTION.

Section 3

MILITARY APPOINTMENT, ENLISTMENT, AND INDUCTION

3-300 GENERAL

THE APPOINTMENT, ENLISTMENT, AND INDUCTION OF EACH MEMBER OF THE ARMED FORCES OR THEIR RESERVE COMPONENTS SHALL BE SUBJECT TO THE FAVORABLE COMPLETION OF A PERSONNEL SECURITY INVESTIGATION. THE TYPES OF INVESTIGATION REQUIRED ARE SET FORTH IN THIS SECTION.

3-301 ENTRANCE INVESTIGATION

A. AN ENTNAC SHALL BE CONDUCTED ON EACH ENLISTED MEMBER OF THE ARMED FORCES AT THE TIME OF INITIAL ENTRY INTO THE SERVICE. A DNACI SHALL BE CONDUCTED ON EACH COMMISSIONED OFFICER, EXCEPT AS PERMITTED BY PARAGRAPH 3-303 OF THIS SECTION, WARRANT OFFICER, CADET, MIDSHIPMAN, AND RESERVE OFFICERS TRAINING CANDIDATE, AT THE TIME OF APPOINTMENT. A FULL NAC SHALL BE CONDUCTED UPON REENTRY OF ANY OF THE ABOVE WHEN THERE HAS BEEN A BREAK IN SERVICE GREATER THAN 12 MONTHS.

B. IF AN OFFICER OR WARRANT OFFICER CANDIDATE HAS BEEN THE SUBJECT OF A FAVORABLE NAC OR ENTNAC AND THERE HAS NOT BEEN A BREAK IN SERVICE OF MORE THAN 12 MONTHS, A NEW NAC IS NOT AUTHORIZED. THIS INCLUDES ROTC GRADUATES WHO DELAY ENTRY ONTO ACTIVE DUTY PENDING COMPLETION OF THEIR STUDIES.

C. ALL DEROGATORY INFORMATION REVEALED DURING THE ENLISTMENT OR APPOINTMENT PROCESS THAT RESULTS IN A MORAL WAIVER WILL BE FULLY EXPLAINED ON A WRITTEN SUMMARY ATTACHED TO THE DD FORM 398-2.

3-302 RESERVE COMPONENTS AND NATIONAL GUARD

RESERVE COMPONENT AND NATIONAL GUARD PERSONNEL NOT ON ACTIVE DUTY ARE SUBJECT TO THE INVESTIGATIVE REQUIREMENTS OF THIS CHAPTER.

3-303 EXCEPTIONS FOR CERTAIN COMMISSIONED OFFICERS OF RESERVE COMPONENTS

THE REQUIREMENTS FOR ENTRANCE INVESTIGATION SHALL BE RIGIDLY ADHERED TO EXCEPT AS FOLLOWS. HEALTH PROFESSIONALS, CHAPLAINS, AND ATTORNEYS MAY BE COMMISSIONED IN THE RESERVE COMPONENTS PRIOR TO COMPLETION OF A DNACI PROVIDED THAT:

A. A DNACI IS INITIATED AT THE TIME AN APPLICATION FOR A COMMISSION IS RECEIVED; AND

B. THE APPLYING HEALTH PROFESSIONAL, CHAPLAIN, OR ATTORNEY AGREES IN WRITING THAT, IF THE RESULTS OF THE INVESTIGATION ARE UNFAVORABLE, HE OR SHE WILL BE SUBJECT TO DISCHARGE IF FOUND TO BE INELIGIBLE TO HOLD A COMMISSION. UNDER THIS EXCEPTION, COMMISSIONS IN RESERVE COMPONENTS OTHER THAN THE NATIONAL GUARD MAY BE TENDERED TO IMMIGRANT ALIEN HEALTH PROFESSIONALS, CHAPLAINS, AND ATTORNEYS.

3-304 MOBILIZATION OF MILITARY RETIREES

THE REQUIREMENTS CONTAINED IN PARAGRAPH 3-301 OF THIS SECTION, REGARDING A FULL NAC UPON REENTRY TO ACTIVE DUTY OF ANY OFFICER OR ENLISTED REGULAR/ RESERVE MILITARY RETIREE OR INDIVIDUAL READY RESERVE WHO HAS BEEN SEPARATED FROM SERVICE FOR A PERIOD OF GREATER THAN 12 MONTHS, SHOULD BE WAIVED FOR THE PURPOSES OF PARTIAL OR FULL MOBILIZATION UNDER PROVISIONS OF TITLE 10, (TITLE 14, PERTAINING TO THE US COAST GUARD AS AN ELEMENT OF THE NAVY) UNITED STATES CODE, TO INCLUDE THE PERIOD OF PRESCRIBED SERVICE REFRESHER TRAINING. PARTICULAR PRIORITY SHOULD BE AFFORDED TO MILITARY RETIREES MOBILIZED AND ASSIGNED TO THE DEFENSE INTELLIGENCE AND SECURITY AGENCIES COMMUNITIES.

Section 4

SECURITY CLEARANCE

3-400 GENERAL

A. THE AUTHORITIES DESIGNATED IN PARAGRAPH A, APPENDIX F ARE THE ONLY AUTHORITIES AUTHORIZED TO GRANT, DENY OR REVOKE DOD PERSONNEL SECURITY CLEARANCES. THE GRANTING OF SUCH CLEARANCES SHALL BE LIMITED TO ONLY THOSE PERSONS WHO REQUIRE ACCESS TO CLASSIFIED INFORMATION FOR MISSION ACCOMPLISHMENT.

B. MILITARY, DOD CIVILIAN, AND CONTRACTOR PERSONNEL WHO ARE EMPLOYED BY OR SERVING IN A CONSULTANT CAPACITY TO THE DOD, MAY BE CONSIDERED FOR ACCESS TO CLASSIFIED INFORMATION ONLY WHEN SUCH ACCESS IS REQUIRED IN CONNECTION WITH OFFICIAL DUTIES. SUCH INDIVIDUALS MAY BE GRANTED EITHER A FINAL OR INTERIM PERSONNEL SECURITY CLEARANCE PROVIDED THE INVESTIGATIVE REQUIREMENTS SET FORTH BELOW ARE COMPLIED WITH, AND PROVIDED FURTHER THAT ALL AVAILABLE INFORMATION HAS BEEN ADJUDICATED AND A FINDING MADE THAT SUCH CLEARANCE WOULD BE CLEARLY CONSISTENT WITH THE INTERESTS OF NATIONAL SECURITY.

3-401 INVESTIGATIVE REQUIREMENTS FOR CLEARANCE

A. TOP SECRET

(1) FINAL CLEARANCE:

- (A) BI
- (B) ESTABLISHED BILLET PER PARAGRAPH 3-104 (EXCEPT CONTRACTORS)

(2) INTERIM CLEARANCE:

- (A) FAVORABLE NAC, ENTNAC, DNACI, OR NACI COMPLETED
- (B) FAVORABLE REVIEW OF DD FORM 398/SF-86/SF-171/DD FORM 49
- (C) BI OR SBI HAS BEEN INITIATED
- (D) FAVORABLE REVIEW OF LOCAL PERSONNEL, BASE/MILITARY POLICE, MEDICAL, AND OTHER SECURITY RECORDS AS APPROPRIATE

- (E) ESTABLISHED BILLET PER PARAGRAPH 3-104 (EXCEPT CONTRACTORS)
- (F) PROVISIONS OF PARAGRAPH 3-204 HAVE BEEN MET REGARDING CIVILIAN PERSONNEL.

B. SECRET

- (1) FINAL CLEARANCE:
- (A) DNACI: MILITARY (EXCEPT FIRST-TERM ENLISTEES) AND CONTRACTOR EMPLOYEES
- (B) NACI: CIVILIAN EMPLOYEES
- (C) ENTNAC: FIRST-TERM ENLISTEES
- (2) INTERIM CLEARANCE:
- (A) WHEN A VALID NEED TO ACCESS SECRET INFORMATION IS ESTABLISHED, AN INTERIM SECRET CLEARANCE MAY BE ISSUED IN EVERY CASE, PROVIDED THAT THE STEPS OUTLINED IN SUBPARAGRAPHS (B) THROUGH (E) BELOW, HAVE BEEN COMPLIED WITH.
- (B) FAVORABLE REVIEW OF DD FORM 398-2/SF-85/SF-171/DD FORM 48.
- (C) NACI, DNACI, OR ENTNAC INITIATED.
- (D) FAVORABLE REVIEW OF LOCAL PERSONNEL, BASE MILITARY POLICE, MEDICAL, AND SECURITY RECORDS AS APPROPRIATE.
- (E) PROVISIONS OF PARAGRAPH 3-204 HAVE BEEN COMPLIED WITH REGARDING CIVILIAN PERSONNEL.

C. CONFIDENTIAL

- (1) FINAL CLEARANCE:
- (A) NAC OR ENTNAC: MILITARY AND CONTRACTOR EMPLOYEES (EXCEPT FOR PHILIPPINE NATIONAL MEMBERS OF THE UNITED STATES NAVY ON WHOM A BI SHALL BE FAVORABLY COMPLETED.)
- (B) NACI: CIVILIAN EMPLOYEES (EXCEPT FOR SUMMER HIRES WHO MAY BE GRANTED A FINAL CLEARANCE ON THE BASIS OF A NAC).
- (2) INTERIM CLEARANCE
- (A) FAVORABLE REVIEW OF DD FORM 398-2/SF 85/SF 171/DD FORM 48.
- (B) NAC, ENTNAC OR NACI INITIATED.
- (C) FAVORABLE REVIEW OF LOCAL PERSONNEL, BASE MILITARY POLICE, MEDICAL, AND SECURITY RECORDS AS APPROPRIATE.

(D) PROVISIONS OF PARAGRAPH 3-204 HAVE BEEN COMPLIED WITH REGARDING CIVILIAN PERSONNEL.

D. VALIDITY OF PREVIOUSLY GRANTED CLEARANCES:

CLEARANCES GRANTED UNDER LESS STRINGENT INVESTIGATIVE REQUIREMENTS RETAIN THEIR VALIDITY; HOWEVER, IF A HIGHER DEGREE OF CLEARANCE IS REQUIRED, INVESTIGATIVE REQUIREMENTS OF THIS DIRECTIVE WILL BE FOLLOWED.

3-402 ACCESS TO CLASSIFIED INFORMATION BY NON-U.S. CITIZENS

A. ONLY U.S. CITIZENS ARE ELIGIBLE FOR A SECURITY CLEARANCE. EVERY EFFORT SHALL BE MADE TO ENSURE THAT NON-U.S. CITIZENS ARE NOT EMPLOYED IN DUTIES THAT MAY REQUIRE ACCESS TO CLASSIFIED INFORMATION. HOWEVER, COMPELLING REASONS MAY EXIST TO GRANT ACCESS TO CLASSIFIED INFORMATION TO AN IMMIGRANT ALIEN OR A FOREIGN NATIONAL. SUCH INDIVIDUALS MAY BE GRANTED A "LIMITED ACCESS AUTHORIZATION" (LAA) IN THOSE RARE CIRCUMSTANCES WHERE A NON-U. S. CITIZEN POSSESSES A UNIQUE OR UNUSUAL SKILL OR EXPERTISE THAT IS URGENTLY NEEDED IN PURSUIT OF A SPECIFIC DOD REQUIREMENT INVOLVING ACCESS TO SPECIFIED CLASSIFIED INFORMATION FOR WHICH A CLEARED OR CLEARABLE U.S. CITIZEN IS NOT AVAILABLE.

B. LIMITATIONS

(1) LAAs SHALL BE LIMITED ONLY TO INDIVIDUALS WHO HAVE A SPECIAL SKILL OR TECHNICAL EXPERTISE ESSENTIAL TO THE FULFILLMENT OF A DOD REQUIREMENT THAT CANNOT REASONABLY BE FILLED BY A U.S. CITIZEN.

(2) LAAs SHALL NOT BE GRANTED TO PERSONNEL WHO PERFORM ROUTINE ADMINISTRATIVE OR OTHER SUPPORT DUTIES, SUCH AS SECRETARIES, CLERKS, DRIVERS, OR MECHANICS, UNLESS IT HAS BEEN CLEARLY ESTABLISHED THAT THOSE DUTIES CANNOT BE PERFORMED BY A U.S. CITIZEN.

(3) PERSONNEL GRANTED LAAs SHALL NOT BE PERMITTED UNCONTROLLED ACCESS TO AREAS WHERE CLASSIFIED INFORMATION IS STORED OR DISCUSSED. CLASSIFIED INFORMATION SHALL BE MAINTAINED IN A LOCATION THAT WILL BE UNDER THE CONTINUOUS CONTROL AND SUPERVISION OF AN APPROPRIATELY CLEARED U.S. CITIZEN.

(4) LAA PERSONNEL SHALL NOT BE DESIGNATED AS A COURIER OR ESCORT FOR CLASSIFIED MATERIAL OUTSIDE THE LOCATION IN WHICH ACCESS IS PERMITTED UNLESS THEY ARE ACCOMPANIED BY AN APPROPRIATELY CLEARED U.S. PERSON.

C. AUTHORIZED ACCESS LEVELS

(1) LAAs MAY BE GRANTED ONLY AT THE SECRET AND CONFIDENTIAL LEVEL. LAAs FOR TOP SECRET ARE PROHIBITED. INTERIM ACCESS IS NOT AUTHORIZED PENDING APPROVAL OF A LAA.

(2) THE INFORMATION THE NON-U.S. CITIZEN MAY HAVE ACCESS TO MUST BE APPROVED FOR RELEASE TO THE PERSON'S COUNTRY OR COUNTRIES OF CITIZENSHIP, IN ACCORDANCE WITH DOD DIRECTIVE 5230.11 (REFERENCE (LL)).

(3) ACCESS TO CLASSIFIED INFORMATION SHALL BE LIMITED OR RELATED TO A SPECIFIC PROGRAM OR PROJECT; THE LAA SHALL BE CANCELED OR REJUSTIFIED AS DESCRIBED HEREIN UPON COMPLETION OF THE PROGRAM OR PROJECT.

(4) ACCESS TO CLASSIFIED INFORMATION OUTSIDE THE SCOPE OF THE APPROVED LAA SHALL BE CONSIDERED A COMPROMISE OF CLASSIFIED INFORMATION AND SHALL BE INVESTIGATED, IN ACCORDANCE WITH DOD 5200.1-R (REFERENCE (Q)).

D. REQUIREMENTS

(1) THE LAA GRANTING AUTHORITY (APPENDIX F) MAY CONSIDER ISSUING AN LAA ONLY AFTER A WRITTEN DETERMINATION IS MADE THAT ACCESS IS ESSENTIAL FOR A CRITICAL MISSION AND NO U.S. CITIZEN IS AVAILABLE TO PERFORM THE DUTIES.

(2) WHEN A NON-U.S. CITIZEN WHO IS NOMINATED FOR AN LAA IS A CITIZEN OF A COUNTRY WITH WHICH THE UNITED STATES HAS AN AGREEMENT PROVIDING FOR SECURITY ASSURANCES BASED ON THAT COUNTRY'S INVESTIGATIVE REQUIREMENTS, WHICH ARE COMMENSURATE WITH THE STANDARDS PROVIDED HEREIN, AN LAA MAY BE ISSUED AT THE REQUISITE LEVEL.

(3) IN ADDITION TO THE ABOVE, A FAVORABLY COMPLETED (WITHIN THE LAST 5 YEARS) AND ADJUDICATED SSBI IS REQUIRED PRIOR TO GRANTING AN LAA. IF THE SSBI CANNOT PROVIDE FULL INVESTIGATIVE COVERAGE, A POLYGRAPH EXAMINATION (IF THERE ARE NO HOST COUNTRY LEGAL PROHIBITIONS) TO RESOLVE THE REMAINING PERSONNEL SECURITY ISSUES (SEE DOD DIRECTIVE 5210.48 (REFERENCE (P))), MUST BE FAVORABLY COMPLETED BEFORE GRANTING ACCESS.

(4) IF GEOGRAPHICAL, POLITICAL OR MEDICAL SITUATIONS PREVENT THE FULL COMPLETION OF THE SSBI OR PREVENT THE POLYGRAPH EXAMINATION TO SUPPLEMENT A LESS THAN FULL SSBI, A LAA MAY BE GRANTED ONLY WITH APPROVAL OF THE ASD(C3I).

(5) IF AN LAA IS WITHDRAWN AND THE INDIVIDUAL SUBSEQUENTLY IS CONSIDERED FOR AN LAA, THE PROVISIONS OF THIS PARAGRAPH SHALL APPLY CONCERNING AN SSBI AND POLYGRAPH EXAMINATION. THE SCOPE OF THE SSBI NORMALLY SHALL COVER THE PERIOD SINCE THE PREVIOUS BACKGROUND INVESTIGATION OR 10 YEARS, WHICHEVER IS SHORTER.

(6) A PR SHALL BE CONDUCTED ON EVERY INDIVIDUAL WITH A LAA 5 YEARS FROM THE DATE OF THE LAST PR OR SSBI, AS APPROPRIATE.

(7) ALL REQUESTS FOR INITIAL LAAs SHALL CONTAIN A DETAILED JUSTIFICATION AND PLAN DESCRIBING THE FOLLOWING:

(A) THE LOCATION OF THE CLASSIFIED MATERIAL (SECURITY CONTAINERS) IN RELATIONSHIP TO THE LOCATION OF THE FOREIGN NATIONAL.

(B) THE COMPELLING REASON FOR NOT EMPLOYING A CLEARED OR CLEARABLE U.S. CITIZEN.

(C) A SYNOPSIS OF AN ANNUAL CONTINUING ASSESSMENT PROGRAM TO EVALUATE THE INDIVIDUAL'S CONTINUED TRUSTWORTHINESS AND ELIGIBILITY FOR ACCESS.

(D) A PLAN TO CONTROL ACCESS TO SECURE AREAS AND TO CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION.

E. LAA DETERMINATION AUTHORITY

(1) LAA DETERMINATIONS MAY ONLY BE MADE BY AN OFFICIAL LISTED IN PARAGRAPH B, APPENDIX F. THE DESIGNATED SINGLE AUTHORIZING OFFICIAL FOR THE

MILITARY DEPARTMENTS, THE UNIFIED COMBATANT COMMANDS, AND THE DIS PRECLUDES AN LAA DETERMINATION BY ANY OTHER OFFICIAL AT THE MAJOR COMMAND LEVEL, OR EQUIVALENT.

(2) LAA DETERMINATIONS FOR EMPLOYEES OF THE MILITARY DEPARTMENTS SHALL BE THE SOLE AUTHORITY OF THE SECRETARY OF THE MILITARY DEPARTMENT OR A SINGLE DESIGNEE SUCH AS THE SERVICE CENTRAL ADJUDICATION FACILITY. FIELD ELEMENTS MUST SUBMIT THEIR RECOMMENDATIONS FOR ACCESS TO THE DESIGNATED OFFICIAL FOR APPROVAL, ALONG WITH AFFILIATED INFORMATION IN SUPPORT OF THE ACTION.

(3) THE COMMANDER OF A UNIFIED COMBATANT COMMAND, OR SINGLE DESIGNEE (FLAG OFFICER OR CIVILIAN EQUIVALENT) RESPONSIBLE FOR IMPLEMENTATION OF THE PERSONNEL SECURITY PROGRAM, SHALL BE AUTHORIZED TO ISSUE, DENY, OR REVOKE AN LAA. LAA DETERMINATIONS BY THE UNIFIED COMBATANT COMMANDS SHALL BE REPORTED TO THE CENTRAL ADJUDICATIVE FACILITY OF THE MILITARY DEPARTMENT IN ACCORDANCE WITH THE ASSIGNED RESPONSIBILITIES IN DOD DIRECTIVE 5100.3 (REFERENCE (MM)) FOR INCLUSION IN THE DCII.

(4) ALL LAA DETERMINATIONS, FAVORABLE AND UNFAVORABLE, SHALL BE ENTERED INTO THE DCII.

(5) THE ADMINISTRATIVE ACTION PROCEDURES IN CHAPTER 8 DO NOT APPLY TO LAA DETERMINATIONS.

F. RECORD

(1) THE LAA GRANTING AUTHORITY SHALL ENSURE THAT A RECORD IS CREATED ON ISSUANCE AND MAINTAINED FOR 5 YEARS FROM THE DATE THE LAA CEASES. THE RECORD SHALL INCLUDE THE FOLLOWING:

(A) THE IDENTITY OF THE INDIVIDUAL GRANTED THE LAA, TO INCLUDE THE FULL NAME, DATE AND PLACE OF BIRTH, CURRENT CITIZENSHIP(S), ANY SSN, AND ANY NATIONAL IDENTIFYING NUMBER ISSUED BY THE INDIVIDUAL'S COUNTRY OR COUNTRIES OF CITIZENSHIP;

(B) THE INDIVIDUAL'S STATUS AS AN IMMIGRANT ALIEN OR FOREIGN NATIONAL; IF AN IMMIGRANT ALIEN, THE DATE AND PLACE SUCH STATUS WAS GRANTED;

(C) THE CLASSIFICATION LEVEL OF THE LAA; I.E., SECRET OR CONFIDENTIAL;

(D) DATE AND TYPE OF MOST RECENT BACKGROUND INVESTIGATION OR PR AND THE INVESTIGATING AGENCY.

(E) WHETHER A POLYGRAPH EXAMINATION WAS CONDUCTED; IF SO, THE DATE AND ADMINISTERING AGENCY FOR THE MOST RECENT EXAMINATION.

(F) THE NATURE AND IDENTITY OF THE CLASSIFIED PROGRAM MATERIALS TO WHICH ACCESS IS AUTHORIZED AND THE PRECISE DUTIES PERFORMED.

(G) THE COMPELLING REASONS FOR GRANTING ACCESS TO THE INFORMATION.

(2) ALL LAA SSBIs AND PRs SHALL BE CONDUCTED UNDER THE AUSPICES OF THE DIS AND SHALL COMPLY WITH THE REQUIREMENTS OF APPENDIX B. THE DIS SHALL INITIATE LEADS TO THE RESPECTIVE MILITARY DEPARTMENT INVESTIGATIVE AGENCIES OVERSEAS AS WELL AS THE DEPARTMENT OF STATE (DOS). THE RESULTS OF ALL INVESTIGATIONS, TO INCLUDE THOSE CONDUCTED BY THE DOS, SHALL BE RETURNED TO THE DIS FOR REVIEW AND ENTRY INTO THE DCII AND RETURN TO THE DESIGNATED GRANTING OFFICIAL FOR ADJUDICATION. (TO EXPEDITE MATTERS, THE INVESTIGATION MAY BE INITIATED LOCALLY PROVIDED THE NECESSARY PAPERWORK HAS BEEN SUBMITTED TO THE DIS FOR ASSIGNMENT OF A CASE CONTROL NUMBER AND INITIATION OF SUCH OTHER CHECKS AS NEEDED.)

(3) THE UNIFIED COMBATANT COMMANDS SHALL REPORT LAAs THEY ISSUE TO THE APPLICABLE DOD COMPONENT CAP FOR ENTRY INTO THE DCII. THE UNIFIED COMBATANT COMMANDS SHALL ENSURE THAT ALL INVESTIGATIVE PAPERWORK FOR THE INITIATION OF THE SSBI OR PR IS SUBMITTED TO THE DIS THROUGH THE DESIGNATED SINGLE-APPROVAL AUTHORITY RESPONSIBLE FOR ADJUDICATION AND ISSUANCE OF THE LAA.

(4) ALL LAA NOMINEES MUST AGREE TO UNDERGO A POLYGRAPH EXAMINATION AT ANY TIME DURING THE PERIOD THE LAA IS IN EFFECT, IF THERE IS NO HOST-COUNTRY LEGAL PROHIBITION.

G. ALL LAAs SHALL BE REVIEWED ANNUALLY BY THE ISSUING COMPONENT TO DETERMINE IF CONTINUED ACCESS IS IN COMPLIANCE WITH DOD POLICY. A REPORT ON ALL LAAs IN EFFECT, INCLUDING THE DATA REQUIRED IN PARAGRAPH 3-402.F.(1) SHALL BE FURNISHED TO THE DASD(I&S) WITHIN 60 DAYS AFTER THE END OF EACH FISCAL YEAR (SEE SUBSECTION 11-102 BELOW).

3-403 ACCESS BY PERSONS OUTSIDE THE EXECUTIVE BRANCH

A. ACCESS TO CLASSIFIED INFORMATION BY PERSONS OUTSIDE THE EXECUTIVE BRANCH SHALL BE ACCOMPLISHED IN ACCORDANCE WITH CHAPTER VII, DOD 5200.1-R (REFERENCE (Q)). THE INVESTIGATIVE REQUIREMENT SHALL BE THE SAME AS FOR THE APPROPRIATE LEVEL OF SECURITY CLEARANCE, EXCEPT AS INDICATED BELOW.

B. MEMBERS OF THE U.S. SENATE AND HOUSE OF REPRESENTATIVE DO NOT REQUIRE PERSONNEL SECURITY CLEARANCES. THEY MAY BE GRANTED ACCESS TO DOD CLASSIFIED INFORMATION WHICH RELATES TO MATTERS UNDER THE JURISDICTION OF THE RESPECTIVE COMMITTEES TO WHICH THEY ARE ASSIGNED AND IS NEEDED TO PERFORM THEIR DUTIES IN CONNECTION WITH SUCH ASSIGNMENTS.

C. CONGRESSIONAL STAFF MEMBERS REQUIRING ACCESS TO DOD CLASSIFIED INFORMATION SHALL BE PROCESSED FOR A SECURITY CLEARANCE IN ACCORDANCE WITH DOD DIRECTIVE 5142.1 (REFERENCE (OO)) AND THE PROVISIONS OF THIS REGULATION. THE DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (WHS) WILL INITIATE THE REQUIRED INVESTIGATION (INITIAL OR REINVESTIGATION) TO DIS, ADJUDICATE THE RESULTS AND GRANT, DENY OR REVOKE THE SECURITY CLEARANCE, AS APPROPRIATE. THE ASSISTANT SECRETARY OF DEFENSE (LEGISLATIVE AFFAIRS) WILL BE NOTIFIED BY WHS OF THE COMPLETED CLEARANCE ACTION. The ASO will coordinate with WHS should Congressional staff members require access to DoD classified information in accordance with provisions of this paragraph.

D. STATE GOVERNORS DO NOT REQUIRE PERSONNEL SECURITY CLEARANCES. THEY MAY BE GRANTED ACCESS TO SPECIFICALLY DESIGNATED CLASSIFIED INFORMATION, ON A "NEED-TO-KNOW" BASIS, BASED UPON AFFIRMATION BY THE SECRETARY OF DEFENSE OR THE

HEAD OF A DOD COMPONENT OR SINGLE DESIGNEE, THAT ACCESS, UNDER THE CIRCUMSTANCES, SERVES THE NATIONAL INTEREST. STAFF PERSONNEL OF A GOVERNOR'S OFFICE REQUIRING ACCESS TO CLASSIFIED INFORMATION SHALL BE INVESTIGATED AND CLEARED IN ACCORDANCE WITH THE PRESCRIBED PROCEDURES OF THIS REGULATION WHEN THE HEAD OF A DOD COMPONENT, OR SINGLE DESIGNEE, AFFIRMS THAT SUCH CLEARANCE SERVES THE NATIONAL INTEREST. ACCESS SHALL ALSO BE LIMITED TO SPECIFICALLY DESIGNATED CLASSIFIED INFORMATION ON A "NEED-TO-KNOW" BASIS. The ASO will coordinate with the WHS CAF when it is necessary to grant clearances to state government officials as referred to in this paragraph.

E. MEMBERS OF THE U.S. SUPREME COURT, THE FEDERAL JUDICIARY AND THE SUPREME COURTS OF THE INDIVIDUAL STATES DO NOT REQUIRE PERSONNEL SECURITY CLEARANCES. THEY MAY BE GRANTED ACCESS TO DOD CLASSIFIED INFORMATION TO THE EXTENT NECESSARY TO ADJUDICATE CASES BEING HEARD BEFORE THESE INDIVIDUAL COURTS.

F. ATTORNEYS REPRESENTING DOD MILITARY, CIVILIAN OR CONTRACTOR PERSONNEL, REQUIRING ACCESS TO DOD CLASSIFIED INFORMATION TO PROPERLY REPRESENT THEIR CLIENTS, SHALL NORMALLY BE INVESTIGATED BY DIS AND CLEARED IN ACCORDANCE WITH THE PRESCRIBED PROCEDURES IN PARAGRAPH 3-401. THIS SHALL BE DONE UPON CERTIFICATION OF THE GENERAL COUNSEL OF THE DOD COMPONENT INVOLVED IN THE LITIGATION THAT ACCESS TO SPECIFIED CLASSIFIED INFORMATION, ON THE PART OF THE ATTORNEY CONCERNED, IS NECESSARY TO ADEQUATELY REPRESENT HIS OR HER CLIENT. IN EXCEPTIONAL INSTANCES, WHEN THE EXIGENCIES OF A GIVEN SITUATION DO NOT PERMIT TIMELY COMPLIANCE WITH THE PROVISIONS OF PARAGRAPH 3-401, ACCESS MAY BE GRANTED WITH THE WRITTEN APPROVAL OF AN AUTHORITY DESIGNATED IN APPENDIX F PROVIDED THAT AS A MINIMUM: (A) A FAVORABLE NAME CHECK OF THE FBI AND THE DCII HAS BEEN COMPLETED, AND (B) A DOD NON-DISCLOSURE AGREEMENT HAS BEEN EXECUTED. IN POST-INDICTMENT CASES, AFTER A JUDGE HAS INVOKED THE SECURITY PROCEDURES OF THE CLASSIFIED INFORMATION PROCEDURES ACT (CIPA) (REFERENCE (M)), THE DEPARTMENT OF JUSTICE MAY ELECT TO CONDUCT THE NECESSARY BACKGROUND INVESTIGATION AND ISSUE THE REQUIRED SECURITY CLEARANCE, IN COORDINATION WITH THE AFFECTED DOD COMPONENT. The ASO will coordinate with the General Counsel, Defense Legal Service, the WHS CAF, and comply with this paragraph.

3-404 RESTRICTIONS ON ISSUANCE OF PERSONNEL SECURITY CLEARANCES

PERSONNEL SECURITY CLEARANCES MUST BE KEPT TO THE ABSOLUTE MINIMUM NECESSARY TO MEET MISSION REQUIREMENTS. In keeping with the intent of this paragraph, the ASO may periodically require that regions review and reevaluate the need for access to classified information by their employees. A report on such reviews will be provided upon request by the ASO.

PERSONNEL SECURITY CLEARANCES SHALL NORMALLY NOT BE ISSUED:

- A. TO PERSONS IN NONSENSITIVE POSITIONS.
- B. TO PERSONS WHOSE REGULAR DUTIES DO NOT REQUIRE AUTHORIZED ACCESS TO CLASSIFIED INFORMATION.
- C. FOR EASE OF MOVEMENT OF PERSONS WITHIN A RESTRICTED, CONTROLLED, OR INDUSTRIAL AREA, WHOSE DUTIES DO NOT REQUIRE ACCESS TO CLASSIFIED INFORMATION.
- D. TO PERSONS WHO MAY ONLY HAVE INADVERTENT ACCESS TO SENSITIVE INFORMATION OR AREAS, SUCH AS GUARDS, EMERGENCY SERVICE PERSONNEL, FIREMEN, DOCTORS, NURSES, POLICE, AMBULANCE DRIVERS, OR SIMILAR PERSONNEL.

E. TO PERSONS WORKING IN SHIPYARDS WHOSE DUTIES DO NOT REQUIRE ACCESS TO CLASSIFIED INFORMATION.

F. TO PERSONS WHO CAN BE PREVENTED FROM ACCESSING CLASSIFIED INFORMATION BY BEING ESCORTED BY CLEARED PERSONNEL.

G. TO FOOD SERVICE PERSONNEL, VENDORS AND SIMILAR COMMERCIAL SALES OR SERVICE PERSONNEL WHOSE DUTIES DO NOT REQUIRE ACCESS TO CLASSIFIED INFORMATION.

H. TO MAINTENANCE OR CLEANING PERSONNEL WHO MAY ONLY HAVE INADVERTENT ACCESS TO CLASSIFIED INFORMATION UNLESS SUCH ACCESS CANNOT BE REASONABLY PREVENTED.

I. TO PERSONS WHO PERFORM MAINTENANCE ON OFFICE EQUIPMENT, COMPUTERS, TYPEWRITERS, AND SIMILAR EQUIPMENT WHO CAN BE DENIED CLASSIFIED ACCESS BY PHYSICAL SECURITY MEASURES.

J. TO PERIMETER SECURITY PERSONNEL WHO HAVE NO ACCESS TO CLASSIFIED INFORMATION.

K. TO DRIVERS, CHAUFFEURS AND FOOD SERVICE PERSONNEL.

3-405 DUAL CITIZENSHIP

PERSONS CLAIMING BOTH U.S. AND FOREIGN CITIZENSHIP SHALL BE PROCESSED UNDER PARAGRAPH 3-401, ABOVE, AND ADJUDICATED IN ACCORDANCE WITH THE "FOREIGN PREFERENCE" STANDARD IN APPENDIX I.

3-406 ONE-TIME ACCESS

CIRCUMSTANCES MAY ARISE WHERE AN URGENT OPERATIONAL OR CONTRACTUAL EXIGENCY EXISTS FOR CLEARED DOD PERSONNEL TO HAVE ONE-TIME OR SHORT DURATION ACCESS TO CLASSIFIED INFORMATION AT A HIGHER LEVEL THAN IS AUTHORIZED BY THE EXISTING SECURITY CLEARANCE. IN MANY INSTANCES, THE PROCESSING TIME REQUIRED TO UPGRADE THE CLEARANCE WOULD PRECLUDE TIMELY ACCESS TO THE INFORMATION. IN SUCH SITUATIONS, AND ONLY FOR COMPELLING REASONS IN FURTHERANCE OF THE DOD MISSION, AN AUTHORITY REFERRED TO IN SUBPARAGRAPH A., BELOW, MAY GRANT HIGHER LEVEL ACCESS ON A TEMPORARY BASIS SUBJECT TO THE TERMS AND CONDITIONS PRESCRIBED BELOW. THIS SPECIAL AUTHORITY MAY BE REVOKED FOR ABUSE, INADEQUATE RECORD KEEPING, OR INADEQUATE SECURITY OVERSIGHT. THESE PROCEDURES DO NOT APPLY WHEN CIRCUMSTANCES EXIST WHICH WOULD PERMIT THE ROUTINE PROCESSING OF AN INDIVIDUAL FOR THE HIGHER LEVEL CLEARANCE. PROCEDURES AND CONDITIONS FOR EFFECTING EMERGENCY ONE-TIME ACCESS TO THE NEXT HIGHER CLASSIFICATION LEVEL ARE AS FOLLOWS:

A. AUTHORIZATION FOR SUCH ONE-TIME ACCESS SHALL BE GRANTED BY A FLAG OR GENERAL OFFICER, A GENERAL COURT MARTIAL CONVENING AUTHORITY OR EQUIVALENT SENIOR EXECUTIVE SERVICE MEMBER, AFTER COORDINATION WITH APPROPRIATE SECURITY OFFICIALS. Heads of principal staff elements, the Director of Field Detachment, and regional directors are the DCAA officials who have authority under this paragraph, but may exercise this authority only after direct coordination with the ASO. This authority will be exercised in strict compliance with all provisions of section 3-407.

B. THE RECIPIENT OF THE ONE-TIME ACCESS AUTHORIZATION MUST BE A U.S. CITIZEN, POSSESS A CURRENT DOD SECURITY CLEARANCE, AND THE ACCESS REQUIRED SHALL BE LIMITED TO CLASSIFIED INFORMATION ONE LEVEL HIGHER THAN THE CURRENT CLEARANCE.

C. SUCH ACCESS, ONCE GRANTED, SHALL BE CANCELED PROMPTLY WHEN NO LONGER REQUIRED, AT THE CONCLUSION OF THE AUTHORIZED PERIOD OF ACCESS, OR UPON NOTIFICATION FROM THE GRANTING AUTHORITY.

D. THE EMPLOYEE TO BE AFFORDED THE HIGHER LEVEL ACCESS SHALL HAVE BEEN CONTINUOUSLY EMPLOYED BY A DOD COMPONENT OR A CLEARED DOD CONTRACTOR FOR THE PRECEDING 24-MONTH PERIOD. HIGHER LEVEL ACCESS IS NOT AUTHORIZED FOR PART-TIME EMPLOYEES.

E. PERTINENT LOCAL RECORDS CONCERNING THE EMPLOYEE CONCERNED SHALL BE REVIEWED WITH FAVORABLE RESULTS.

F. WHENEVER POSSIBLE, ACCESS SHALL BE CONFINED TO A SINGLE INSTANCE OR AT MOST, A FEW OCCASIONS. THE APPROVAL FOR ACCESS SHALL AUTOMATICALLY EXPIRE 30 CALENDAR DAYS FROM DATE ACCESS COMMENCED. IF THE NEED FOR ACCESS IS EXPECTED TO CONTINUE FOR A PERIOD IN EXCESS OF 30 DAYS, WRITTEN APPROVAL OF THE GRANTING AUTHORITY IS REQUIRED. AT SUCH TIME AS IT IS DETERMINED THAT THE NEED FOR ACCESS IS EXPECTED TO EXTEND BEYOND 90 DAYS, THE INDIVIDUAL CONCERNED SHALL BE PROMPTLY PROCESSED FOR THE LEVEL OF CLEARANCE REQUIRED. WHEN EXTENDED ACCESS HAS BEEN APPROVED, SUCH ACCESS SHALL BE CANCELED AT OR BEFORE 90 DAYS FROM ORIGINAL DATE OF ACCESS.

G. ACCESS AT THE HIGHER LEVEL SHALL BE LIMITED TO INFORMATION UNDER THE CONTROL AND CUSTODY OF THE AUTHORIZING OFFICIAL AND SHALL BE AFFORDED UNDER THE GENERAL SUPERVISION OF A PROPERLY CLEARED EMPLOYEE. THE EMPLOYEE CHARGED WITH PROVIDING SUCH SUPERVISION SHALL BE RESPONSIBLE FOR: (1) RECORDING THE HIGHER-LEVEL INFORMATION ACTUALLY REVEALED, (2) THE DATE(S) SUCH ACCESS IS AFFORDED, AND (3) THE DAILY RETRIEVAL OF THE MATERIAL ACCESSED.

H. ACCESS AT THE NEXT HIGHER LEVEL SHALL NOT BE AUTHORIZED FOR COMSEC, SCI, NATO, OR FOREIGN GOVERNMENT INFORMATION.

I. THE EXERCISE OF THIS PROVISION SHALL BE USED SPARINGLY AND REPEAT USE WITHIN ANY 12 MONTH PERIOD ON BEHALF OF THE SAME INDIVIDUAL IS PROHIBITED. THE APPROVING AUTHORITY SHALL MAINTAIN A RECORD CONTAINING THE FOLLOWING DATA WITH RESPECT TO EACH SUCH ACCESS APPROVED:

(1) THE NAME, AND SSN OF THE EMPLOYEE AFFORDED HIGHER LEVEL ACCESS.

(2) THE LEVEL OF ACCESS AUTHORIZED.

(3) JUSTIFICATION FOR THE ACCESS, TO INCLUDE AN EXPLANATION OF THE COMPELLING REASON TO GRANT THE HIGHER LEVEL ACCESS AND SPECIFICALLY HOW THE DOD MISSION WOULD BE FURTHERED.

(4) AN UNCLASSIFIED DESCRIPTION OF THE SPECIFIC INFORMATION TO WHICH ACCESS WAS AUTHORIZED AND THE DURATION OF ACCESS ALONG WITH THE DATE(S) ACCESS WAS AFFORDED.

(5) A LISTING OF THE LOCAL RECORDS REVIEWED AND A STATEMENT THAT NO SIGNIFICANT ADVERSE INFORMATION CONCERNING THE EMPLOYEE IS KNOWN TO EXIST.

(6) THE APPROVING AUTHORITY'S SIGNATURE CERTIFYING (1) THROUGH (5), ABOVE.

(7) COPIES OF ANY PERTINENT BRIEFINGS/DEBRIEFINGS ADMINISTERED TO THE EMPLOYEE.

The authorities designated in paragraph A. above are responsible for creating and maintaining a Memorandum for Record (MFR) which meets the requirements of this section. A copy of each MFR will be provided immediately to the ASO.

3-407 ACCESS BY RETIRED FLAG AND/OR GENERAL OFFICERS

A. UPON DETERMINATION BY AN ACTIVE DUTY FLAG/GENERAL OFFICER THAT THERE ARE COMPELLING REASONS, IN FURTHERANCE OF THE DEPARTMENT OF DEFENSE MISSION, TO GRANT A RETIRED FLAG/GENERAL OFFICER ACCESS TO CLASSIFIED INFORMATION IN CONNECTION WITH A SPECIFIC DOD PROGRAM OR MISSION, FOR A PERIOD NOT GREATER THAN 90 DAYS, THE INVESTIGATIVE REQUIREMENTS OF THIS REGULATION MAY BE WAIVED. THE ACCESS SHALL BE LIMITED TO CLASSIFIED INFORMATION AT A LEVEL COMMENSURATE WITH THE SECURITY CLEARANCE HELD AT THE TIME OF RETIREMENT -- NOT INCLUDING ACCESS TO SCI.

B. THE FLAG/GENERAL OFFICER APPROVING ISSUANCE OF THE CLEARANCE SHALL, PROVIDE THE APPROPRIATE DOD COMPONENT CENTRAL CLEARANCE FACILITY A WRITTEN RECORD TO BE INCORPORATED INTO THE DCII DETAILING:

- (1) FULL IDENTIFYING DATA PERTAINING TO THE CLEARED SUBJECT;
- (2) THE CLASSIFICATION OF THE INFORMATION TO WHICH ACCESS WAS AUTHORIZED.

C. SUCH ACCESS MAY BE GRANTED ONLY AFTER THE COMPELLING REASON AND THE SPECIFIC ASPECT OF THE DOD MISSION WHICH IS SERVED BY GRANTING SUCH ACCESS HAS BEEN DETAILED AND UNDER THE CONDITION THAT THE CLASSIFIED MATERIALS INVOLVED ARE NOT REMOVED FROM THE CONFINES OF A GOVERNMENT INSTALLATION OR OTHER AREA APPROVED FOR STORAGE OF DOD CLASSIFIED INFORMATION.

Section 5

SPECIAL ACCESS PROGRAMS

3-500 GENERAL

IT IS THE POLICY OF THE DEPARTMENT OF DEFENSE TO ESTABLISH, TO THE EXTENT POSSIBLE, UNIFORM AND CONSISTENT PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS. ACCORDINGLY, INVESTIGATIONS EXCEEDING ESTABLISHED REQUIREMENTS ARE AUTHORIZED ONLY WHEN MANDATED BY STATUTE, NATIONAL REGULATIONS, OR INTERNATIONAL AGREEMENT OR EXECUTIVE ORDER 12968 OR ITS SUCCESSOR. IN THIS CONNECTION, THERE ARE CERTAIN SPECIAL ACCESS PROGRAMS (SAPs) ORIGINATING AT THE NATIONAL OR INTERNATIONAL LEVEL THAT REQUIRE PERSONNEL SECURITY INVESTIGATIONS AND PROCEDURES OF A SPECIAL NATURE. THOSE PROGRAMS AND THE SPECIAL INVESTIGATIVE REQUIREMENTS IMPOSED BY THEM ARE DESCRIBED IN THIS SECTION. A SAP IS ANY

PROGRAM DESIGNED TO CONTROL ACCESS, DISTRIBUTION, AND PROTECTION OF PARTICULARLY SENSITIVE INFORMATION ESTABLISHED PURSUANT TO E. O. 12958 (REFERENCE (J)) AND PRIOR EXECUTIVE ORDERS. DOD DIRECTIVE O-5205.7 (REFERENCE (Q)) PRESCRIBES POLICY AND PROCEDURES FOR ESTABLISHMENT, ADMINISTRATION AND REPORTING OF DEPARTMENTAL SAPs. In support of SAPs, selected Agency personnel are designated to assist in audits and are screened to ensure that applicable investigative and adjudicative actions are accomplished. Level of investigative requirements, as well as adjudicative guidelines, are determined and directed by individual SAP managers. General guidance as to DCAA requirements for participation in SAPs is contained in DCAA Regulation 5205.10 (reference 1-100.e); DCAA Instruction 5205.11 (reference 1-100.f); DCAA Pamphlet 5205.13 (reference 1-100.v); and Chapter XII and Enclosure 8 of DCAA Manual 5205.1 (reference 1-100.g). Individuals being nominated for participation in a SAP who have not been the subject of a BI, SBI, SSBI, or the equivalent conducted by other agencies of the Federal Government as defined above, will be processed for completion of a SSBI. Also, those individuals who have been the subject of a BI, SBI, SSBI, or the equivalent conducted by another agency of the Federal Government, and the investigation is more than five years old, will be processed for a Periodic Reinvestigation (PR). (See section 6, Enclosure 3).

3-501 SENSITIVE COMPARTMENTED INFORMATION (SCI)

A. THE INVESTIGATIVE REQUIREMENTS FOR ACCESS TO SCI IS AN SBI (SEE PARAGRAPH 4, APPENDIX B) INCLUDING A NAC ON THE INDIVIDUAL'S SPOUSE OR COHABITANT. WHEN CONDITIONS INDICATE, ADDITIONAL INVESTIGATION SHALL BE CONDUCTED ON THE SPOUSE OF THE INDIVIDUAL AND MEMBERS OF THE IMMEDIATE FAMILY (OR OTHER PERSONS TO WHOM THE INDIVIDUAL IS BOUND BY AFFECTION OR OBLIGATION) TO THE EXTENT NECESSARY TO PERMIT A DETERMINATION BY THE ADJUDICATION AGENCY THAT THE PERSONNEL SECURITY STANDARDS OF DCID 1/14 (REFERENCE (1)) ARE MET.

B. A PREVIOUS INVESTIGATION CONDUCTED WITHIN THE PAST FIVE YEARS WHICH SUBSTANTIALLY MEETS THE INVESTIGATIVE REQUIREMENTS PRESCRIBED BY THIS SECTION MAY SERVE AS A BASIS FOR GRANTING ACCESS APPROVAL PROVIDED THAT THERE HAS BEEN NO BREAK IN THE INDIVIDUAL'S MILITARY SERVICE, DOD CIVILIAN EMPLOYMENT, OR ACCESS TO CLASSIFIED INFORMATION UNDER THE INDUSTRIAL SECURITY PROGRAM GREATER THAN 24 MONTHS. THE INDIVIDUAL SHALL SUBMIT ONE COPY OF AN UPDATED PSQ COVERING THE PERIOD SINCE THE COMPLETION OF THE LAST SBI AND/OR SSBI AND CERTIFY ANY SUBSTANTIVE CHANGES THAT MAY HAVE OCCURRED.

C. IN ACCORDANCE WITH DCID 1/14 (REFERENCE (L)), A TOP SECRET SECURITY CLEARANCE SHALL NOT BE A PREREQUISITE FOR ACCESS TO SCI. DETERMINATION OF ELIGIBILITY FOR ACCESS TO SCI UNDER REFERENCE (L) SHALL INCLUDE ELIGIBILITY FOR ACCESS TO TOP SECRET AND BELOW.

3-502 SINGLE INTEGRATED OPERATIONAL PLAN-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI)

THE INVESTIGATIVE REQUIREMENT FOR ACCESS TO SIOP-ESI IS AN SBI, INCLUDING A NAC ON THE SPOUSE AND THE INDIVIDUAL'S IMMEDIATE FAMILY WHO ARE 18 YEARS OF AGE OR OVER AND WHO ARE UNITED STATES CITIZENS OTHER THAN BY BIRTH OR WHO ARE RESIDENT ALIENS.

3-503 PRESIDENTIAL SUPPORT ACTIVITIES

A. DOD DIRECTIVE 5210.55 (REFERENCE (R)) PRESCRIBES THE POLICIES AND PROCEDURES FOR THE NOMINATION, SCREENING, SELECTION, AND CONTINUED EVALUATION OF DOD MILITARY AND CIVILIAN PERSONNEL AND CONTRACTOR EMPLOYEES ASSIGNED TO OR UTILIZED IN PRESIDENTIAL SUPPORT ACTIVITIES. THE TYPE OF INVESTIGATION OF INDIVIDUALS ASSIGNED TO PRESIDENTIAL SUPPORT ACTIVITIES VARIES ACCORDING TO WHETHER THE PERSON INVESTIGATED QUALIFIES FOR CATEGORY ONE OR CATEGORY TWO AS INDICATED BELOW: In addition to the above provisions, see DCAA Regulation 5210.9 (reference 1-100.h).

(1) CATEGORY ONE

(A) PERSONNEL ASSIGNED ON A PERMANENT OR FULL-TIME BASIS TO DUTIES IN DIRECT SUPPORT OF THE PRESIDENT (INCLUDING THE OFFICE STAFF OF THE DIRECTOR, WHITE HOUSE MILITARY OFFICE, AND ALL INDIVIDUALS UNDER HIS CONTROL):

1 PRESIDENTIAL AIR CREW AND ASSOCIATED MAINTENANCE AND SECURITY PERSONNEL.

2 PERSONNEL ASSIGNED TO THE WHITE HOUSE COMMUNICATIONS ACTIVITIES AND THE PRESIDENTIAL RETREAT.

3 WHITE HOUSE TRANSPORTATION PERSONNEL.

4 PRESIDENTIAL MESS ATTENDANTS AND MEDICAL PERSONNEL.

5 OTHER INDIVIDUALS FILLING ADMINISTRATIVE POSITIONS AT THE WHITE HOUSE.

(B) PERSONNEL ASSIGNED ON A TEMPORARY OR PART-TIME BASIS TO DUTIES SUPPORTING THE PRESIDENT:

1 MILITARY SOCIAL AIDES.

2 SELECTED SECURITY, TRANSPORTATION, FLIGHT-LINE SAFETY, AND BAGGAGE PERSONNEL.

3 OTHERS WITH SIMILAR DUTIES.

(C) PERSONNEL ASSIGNED TO THE OFFICE OF THE MILITARY AIDE TO THE VICE PRESIDENT.

(2) CATEGORY TWO

(A) PERSONNEL ASSIGNED TO HONOR GUARDS, CEREMONIAL UNITS, AND MILITARY BANDS WHO PERFORM AT PRESIDENTIAL FUNCTIONS AND FACILITIES.

(B) EMPLOYEES OF CONTRACTORS WHO PROVIDE SERVICES OR CONTRACTORS EMPLOYEES WHO REQUIRE UNESCORTED ACCESS TO PRESIDENTIAL SUPPORT AREAS, ACTIVITIES, OR EQUIPMENT--INCLUDING MAINTENANCE OF THE PRESIDENTIAL RETREAT, COMMUNICATIONS, AND AIRCRAFT.

(C) INDIVIDUALS IN DESIGNATED UNITS REQUIRING A LESSER DEGREE OF ACCESS TO THE PRESIDENT OR PRESIDENTIAL SUPPORT ACTIVITIES.

B. PERSONNEL NOMINATED FOR CATEGORY ONE DUTIES MUST HAVE BEEN THE SUBJECT OF AN SBI, INCLUDING A NAC ON THE SPOUSE AND ALL MEMBERS OF THE INDIVIDUAL'S IMMEDIATE FAMILY OF 18 YEARS OF AGE OR OVER WHO ARE UNITED STATES CITIZENS OTHER THAN BY BIRTH OR WHO ARE RESIDENT ALIENS. THE SBI MUST HAVE BEEN COMPLETED WITHIN THE 12 MONTHS PRECEDING SELECTION FOR PRESIDENTIAL SUPPORT DUTIES. IF SUCH AN INDIVIDUAL MARRIES SUBSEQUENT TO THE COMPLETION OF THE SBI, THE REQUIRED SPOUSE CHECK SHALL BE MADE AT THAT TIME.

C. PERSONNEL NOMINATED FOR CATEGORY TWO DUTIES MUST HAVE BEEN THE SUBJECT OF A BI, INCLUDING A NAC ON THE SPOUSE AND ALL MEMBERS OF THE INDIVIDUAL'S IMMEDIATE FAMILY OF 18 YEARS OF AGE OR OVER WHO ARE UNITED STATES CITIZENS OTHER THAN BY BIRTH OR WHO ARE RESIDENT ALIENS. THE BI MUST HAVE BEEN COMPLETED WITHIN THE 12 MONTHS PRECEDING SELECTION FOR PRESIDENTIAL SUPPORT DUTIES. IT SHOULD BE NOTED THAT DUTIES (SEPARATE AND DISTINCT FROM THEIR PRESIDENTIAL SUPPORT RESPONSIBILITIES) OF SOME CATEGORY TWO PERSONNEL MAY MAKE IT NECESSARY FOR THEM TO HAVE SPECIAL ACCESS CLEARANCES WHICH REQUIRE AN SBI.

D. THE U.S. CITIZENSHIP OF FOREIGN-BORN IMMEDIATE FAMILY MEMBERS OF ALL PRESIDENTIAL SUPPORT NOMINEES MUST BE VERIFIED BY INVESTIGATION.

E. A LIMITED NUMBER OF CATEGORY ONE PERSONNEL HAVING ESPECIALLY SENSITIVE DUTIES HAVE BEEN DESIGNATED BY THE DIRECTOR, WHITE HOUSE MILITARY OFFICE AS "CATEGORY A." THESE PERSONNEL SHALL BE INVESTIGATED UNDER SPECIAL SCOPING IN ACCORDANCE WITH THE REQUIREMENTS OF REFERENCE (JJ).

3-504 NUCLEAR WEAPON PERSONNEL RELIABILITY PROGRAM (PRP)

A. DOD DIRECTIVE 5210.42 (REFERENCE (S)) SETS FORTH THE STANDARDS OF INDIVIDUAL RELIABILITY REQUIRED FOR PERSONNEL PERFORMING DUTIES ASSOCIATED WITH NUCLEAR WEAPONS AND NUCLEAR COMPONENTS. THE INVESTIGATIVE REQUIREMENT FOR PERSONNEL PERFORMING SUCH DUTIES IS:

(1) CRITICAL POSITION: BI. IN THE EVENT THAT IT BECOMES NECESSARY TO CONSIDER AN INDIVIDUAL FOR A CRITICAL POSITION AND THE REQUIRED BI HAS NOT BEEN COMPLETED, INTERIM CERTIFICATION MAY BE MADE UNDER CAREFULLY CONTROLLED CONDITIONS AS SET FORTH BELOW.

(A) THE INDIVIDUAL HAS HAD A FAVORABLE DNACI, NAC (OR ENTNAC) WITHIN THE PAST 5 YEARS WITHOUT A BREAK IN SERVICE OR EMPLOYMENT IN EXCESS OF 1 YEAR.

(B) THE BI HAS BEEN REQUESTED.

(C) ALL OTHER REQUIREMENTS OF THE PRP SCREENING PROCESS HAVE BEEN FULFILLED.

(D) THE INDIVIDUAL IS IDENTIFIED TO SUPERVISORY PERSONNEL AS BEING CERTIFIED ON AN INTERIM BASIS.

(E) THE INDIVIDUAL IS NOT USED IN A TWO-MAN TEAM WITH ANOTHER SUCH INDIVIDUAL.

(F) JUSTIFICATION OF THE NEED FOR INTERIM CERTIFICATION IS DOCUMENTED BY THE CERTIFYING OFFICIAL.

(G) SHOULD THE BI NOT BE COMPLETED WITHIN 150 DAYS FROM THE DATE OF THE REQUEST, THE CERTIFYING OFFICIAL SHALL QUERY THE COMPONENT CLEARANCE AUTHORITY, WHO SHALL ASCERTAIN FROM DIS THE STATUS OF THE INVESTIGATION. ON THE BASIS OF SUCH INFORMATION, THE CERTIFYING OFFICIAL SHALL DETERMINE WHETHER TO CONTINUE OR TO WITHDRAW THE INTERIM CERTIFICATION.

(2) CONTROLLED POSITION: DNACI/NACI

(A) AN ENTNAC COMPLETED FOR THE PURPOSE OF FIRST TERM ENLISTMENT OR INDUCTION INTO THE ARMED FORCES DOES NOT SATISFY THIS REQUIREMENT.

(B) INTERIM CERTIFICATION IS AUTHORIZED FOR AN INDIVIDUAL WHO HAS NOT HAD A DNACI/NACI COMPLETED WITHIN THE PAST 5 YEARS, SUBJECT TO THE FOLLOWING CONDITIONS:

1 THE INDIVIDUAL HAS HAD A FAVORABLE ENTNAC/NAC, OR HIGHER INVESTIGATION, THAT IS MORE THAN 5 YEARS OLD AND HAS NOT HAD A BREAK IN SERVICE OR EMPLOYMENT IN EXCESS OF 1 YEAR.

2 A DNACI/NACI HAS BEEN REQUESTED AT THE TIME OF INTERIM CERTIFICATION.

3 ALL OTHER REQUIREMENTS OF THE PRP SCREENING PROCESS HAVE BEEN FULFILLED.

4 SHOULD THE DNACI/NACI NOT BE COMPLETED WITHIN 90 DAYS FROM THE DATE OF THE REQUEST, THE PROCEDURES SET FORTH IN A(L)(G), ABOVE, FOR ASCERTAINING THE DELAY OF THE INVESTIGATION IN THE CASE OF A CRITICAL POSITION SHALL APPLY.

(3) ADDITIONAL REQUIREMENTS APPLY.

(A) THE INVESTIGATION UPON WHICH CERTIFICATION IS BASED MUST HAVE BEEN COMPLETED WITHIN THE LAST 5 YEARS FROM THE DATE OF INITIAL ASSIGNMENT TO A PRP POSITION AND THERE MUST NOT HAVE BEEN A BREAK IN SERVICE OR EMPLOYMENT IN EXCESS OF 1 YEAR BETWEEN COMPLETION OF THE INVESTIGATION AND INITIAL ASSIGNMENT.

(B) IN THOSE CASES IN WHICH THE INVESTIGATION WAS COMPLETED MORE THAN 5 YEARS PRIOR TO INITIAL ASSIGNMENT OR IN WHICH THERE HAS BEEN A BREAK IN SERVICE OR EMPLOYMENT IN EXCESS OF 1 YEAR SUBSEQUENT TO COMPLETION OF THE INVESTIGATION, A REINVESTIGATION IS REQUIRED.

(C) SUBSEQUENT TO INITIAL ASSIGNMENT TO THE PRP, REINVESTIGATION IS NOT REQUIRED SO LONG AS THE INDIVIDUAL REMAINS IN THE PRP.

(D) A MEDICAL EVALUATION OF THE INDIVIDUAL AS SET FORTH IN DOD DIRECTIVE 5210.42 (REFERENCE (S)).

(E) REVIEW OF THE INDIVIDUAL'S PERSONNEL FILE AND OTHER OFFICIAL RECORDS AND INFORMATION LOCALLY AVAILABLE CONCERNING BEHAVIOR OR CONDUCT WHICH IS RELEVANT TO PRP STANDARDS.

(F) A PERSONAL INTERVIEW WITH THE INDIVIDUAL FOR THE PURPOSE OF INFORMING HIM OF THE SIGNIFICANCE OF THE ASSIGNMENT, RELIABILITY STANDARDS, THE NEED FOR RELIABLE PERFORMANCE, AND OF ASCERTAINING HIS ATTITUDE WITH RESPECT TO THE PRP.

(G) SERVICE IN THE ARMY, NAVY AND AIR FORCE RESERVE DOES NOT CONSTITUTE ACTIVE SERVICE FOR PRP PURPOSES.

3-505 ACCESS TO NORTH ATLANTIC TREATY ORGANIZATION (NATO) CLASSIFIED INFORMATION

A. PERSONNEL ASSIGNED TO A NATO STAFF POSITION REQUIRING ACCESS TO NATO COSMIC (TOP SECRET), SECRET OR CONFIDENTIAL INFORMATION SHALL HAVE BEEN THE SUBJECT OF A FAVORABLY ADJUDICATED BI (10 YEAR SCOPE), DNACI/NACI OR NACI ENTNAC, CURRENT WITHIN FIVE YEARS PRIOR TO THE ASSIGNMENT, IN ACCORDANCE WITH USSAN INSTRUCTION 1-69 (REFERENCE (KK)) AND PARAGRAPH 3-705, BELOW.

B. PERSONNEL NOT ASSIGNED TO A NATO STAFF POSITION, BUT REQUIRING ACCESS TO NATO COSMIC, SECRET OR CONFIDENTIAL INFORMATION IN THE NORMAL COURSE OF THEIR DUTIES, MUST POSSESS THE EQUIVALENT FINAL U.S. SECURITY CLEARANCE BASED UPON THE APPROPRIATE PERSONNEL SECURITY INVESTIGATION (APPENDIX B) REQUIRED BY PARAGRAPH 3-401 AND 3-709 OF THIS REGULATION.

Additionally, see DCAA Regulation C-5210.12 (reference 1-100.i).

3-506 OTHER SPECIAL ACCESS PROGRAMS (SAPs)

SPECIAL INVESTIGATIVE REQUIREMENTS FOR SAPs NOT PROVIDED FOR IN THIS PARAGRAPH MAY BE ESTABLISHED ONLY AS PART OF THE WRITTEN PROGRAM APPROVAL OF THE DEPUTY SECRETARY OF DEFENSE IN ACCORDANCE WITH THE SAP APPROVAL PROCESS PRESCRIBED FOR IN DOD DIRECTIVE O-5205.7 (REFERENCE (QQ)).

Section 6

CERTAIN POSITIONS NOT NECESSARILY REQUIRING ACCESS
TO CLASSIFIED INFORMATION

3-600 GENERAL

DOD DIRECTIVE 5200.8 (REFERENCE (T)) OUTLINES THE AUTHORITY OF MILITARY COMMANDERS UNDER THE INTERNAL SECURITY ACT OF 1950 TO ISSUE ORDERS AND REGULATIONS FOR THE PROTECTION OF PROPERTY OR PLACES UNDER THEIR COMMAND. ESSENTIAL TO CARRYING OUT THIS RESPONSIBILITY IS A COMMANDER'S NEED TO PROTECT THE COMMAND AGAINST THE ACTION OF UNTRUSTWORTHY PERSONS. NORMALLY, THE INVESTIGATIVE REQUIREMENTS PRESCRIBED IN THIS REGULATION SHOULD SUFFICE TO ENABLE A COMMANDER TO DETERMINE THE TRUSTWORTHINESS OF INDIVIDUALS WHOSE DUTIES REQUIRE ACCESS TO CLASSIFIED INFORMATION OR APPOINTMENT TO POSITIONS THAT ARE SENSITIVE AND DO NOT INVOLVE SUCH ACCESS. HOWEVER, THERE ARE CERTAIN CATEGORIES OF POSITIONS OR DUTIES WHICH, ALTHOUGH NOT REQUIRING ACCESS TO CLASSIFIED INFORMATION, IF PERFORMED BY UNTRUSTWORTHY PERSONS, COULD ENABLE THEM TO JEOPARDIZE THE SECURITY OF THE COMMAND OR OTHERWISE ENDANGER THE NATIONAL SECURITY. THE INVESTIGATIVE REQUIREMENTS FOR SUCH POSITIONS OR DUTIES ARE DETAILED IN THIS SECTION.

3-601 ACCESS TO RESTRICTED AREAS, SENSITIVE INFORMATION OR EQUIPMENT NOT INVOLVING ACCESS TO CLASSIFIED INFORMATION

A. ACCESS TO RESTRICTED AREAS, SENSITIVE INFORMATION OR EQUIPMENT BY DOD MILITARY, CIVILIAN OR CONTRACTOR PERSONNEL SHALL BE LIMITED TO THOSE INDIVIDUALS WHO HAVE BEEN DETERMINED TRUSTWORTHY AS A RESULT OF THE FAVORABLE COMPLETION OF A NAC (OR ENTNAC) OR WHO ARE UNDER THE ESCORT OF APPROPRIATELY CLEARED PERSONNEL. WHERE ESCORTING SUCH PERSONS IS NOT FEASIBLE, A NAC SHALL BE CONDUCTED AND FAVORABLY REVIEWED BY THE APPROPRIATE COMPONENT AGENCY OR ACTIVITY PRIOR TO PERMITTING SUCH ACCESS. DOD COMPONENTS SHALL NOT REQUEST, AND SHALL NOT DIRECT OR PERMIT THEIR CONTRACTORS TO REQUEST, SECURITY CLEARANCES TO PERMIT ACCESS TO AREAS WHEN ACCESS TO CLASSIFIED INFORMATION IS NOT REQUIRED IN THE NORMAL COURSE OF DUTIES OR WHICH SHOULD BE PRECLUDED BY APPROPRIATE SECURITY MEASURES. IN DETERMINING TRUSTWORTHINESS UNDER THIS PARAGRAPH, THE PROVISIONS OF PARAGRAPH 2-200 AND APPENDIX I WILL BE UTILIZED.

B. IN MEETING THE REQUIREMENTS OF THIS PARAGRAPH, APPROVAL SHALL BE OBTAINED FROM ONE OF THE AUTHORITIES DESIGNATED IN PARAGRAPH A, APPENDIX F OF THIS REGULATION, FOR AUTHORITY TO REQUEST NACs ON DOD MILITARY, CIVILIAN OR CONTRACTOR EMPLOYEES. A JUSTIFICATION SHALL ACCOMPANY EACH REQUEST WHICH SHALL DETAIL THE REASONS WHY ESCORTED ACCESS WOULD NOT BETTER SERVE THE NATIONAL SECURITY. REQUESTS FOR INVESTIGATIVE REQUIREMENTS BEYOND A NAC SHALL BE FORWARDED TO THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY FOR APPROVAL.

C. NAC REQUESTS SHALL (1) BE FORWARDED TO DIS IN ACCORDANCE WITH THE PROVISIONS OF PARAGRAPH B, APPENDIX C, (2) CONTAIN A REFERENCE TO THIS PARAGRAPH ON THE DD FORM 398-2, AND (3) LIST THE AUTHORITY IN APPENDIX F WHO APPROVED THE REQUEST.

D. DETERMINATIONS TO DENY ACCESS UNDER THE PROVISIONS OF THIS PARAGRAPH MUST NOT BE EXERCISED IN AN ARBITRARY, CAPRICIOUS, OR DISCRIMINATORY MANNER AND SHALL BE THE RESPONSIBILITY OF THE MILITARY OR INSTALLATION COMMANDER AS PROVIDED FOR IN DOD DIRECTIVE 5200.8 (REFERENCE (T)).

DCAAM will comply strictly with provisions of this section in not requesting clearances for or granting access to its personnel when no access to classified information is necessary. Security specialists will coordinate with contractor security officials and/or CPS should contractors indicate a requirement for security clearance to permit access to areas when actual access to classified information is not required.

3-602 NONAPPROPRIATED FUND EMPLOYEES

EACH NONAPPROPRIATED FUND EMPLOYEE WHO IS EMPLOYED IN A POSITION OF TRUST AS DESIGNATED BY AN OFFICIAL AUTHORIZED IN PARAGRAPH H, APPENDIX F, SHALL HAVE BEEN THE SUBJECT OF A NAC COMPLETED NO LONGER THAN 12 MONTHS PRIOR TO EMPLOYMENT OR A PRIOR PERSONNEL SECURITY INVESTIGATION WITH NO BREAK IN FEDERAL SERVICE OR EMPLOYMENT GREATER THAN 12 MONTHS IN ACCORDANCE WITH DOD MANUAL 1401.1-M, (REFERENCE (U)). AN INDIVIDUAL WHO DOES NOT MEET ESTABLISHED SUITABILITY REQUIREMENTS MAY NOT BE EMPLOYED WITHOUT PRIOR APPROVAL OF THE AUTHORIZING OFFICIAL. ISSUANCE OF A CONFIDENTIAL OR SECRET CLEARANCE WILL BE BASED ON A DNACI OR NACI IN ACCORDANCE WITH PARAGRAPH 3-401.

3-603 CUSTOMS INSPECTORS

DOD EMPLOYEES APPOINTED AS CUSTOMS INSPECTORS, UNDER WAIVERS APPROVED IN ACCORDANCE WITH DOD 5030.49-R (REFERENCE (V)), SHALL HAVE UNDERGONE A FAVORABLY ADJUDICATED NAC COMPLETED WITHIN THE PAST 5 YEARS UNLESS THERE HAS BEEN A BREAK IN DOD EMPLOYMENT GREATER THAN 1 YEAR IN WHICH CASE A CURRENT NAC IS REQUIRED.

3-604 RED CROSS/UNITED SERVICE ORGANIZATIONS PERSONNEL

A FAVORABLY ADJUDICATED NAC SHALL BE ACCOMPLISHED ON RED CROSS OR UNITED SERVICE ORGANIZATIONS PERSONNEL AS PREREQUISITE FOR ASSIGNMENT WITH THE ARMED FORCES OVERSEAS (DOD DIRECTIVE 5210.25 (REFERENCE (W))).

3-605 OFFICIALS AUTHORIZED TO ISSUE SECURITY CLEARANCES

ANY PERSON AUTHORIZED TO ADJUDICATE PERSONNEL SECURITY CLEARANCES SHALL HAVE BEEN THE SUBJECT OF A FAVORABLY ADJUDICATED BI.

3-606 PERSONNEL SECURITY CLEARANCE ADJUDICATION OFFICIALS

ANY PERSON SELECTED TO SERVE WITH A BOARD, COMMITTEE, OR OTHER GROUP RESPONSIBLE FOR ADJUDICATING PERSONNEL SECURITY CASES SHALL HAVE BEEN THE SUBJECT OF A FAVORABLY ADJUDICATED BI.

3-607 PERSONS REQUIRING DOD BUILDING PASSES

PURSUANT TO DOD DIRECTIVE 5210.46 (REFERENCE (Z)), EACH PERSON DETERMINED BY THE DESIGNATED AUTHORITIES OF THE COMPONENTS CONCERNED AS HAVING AN OFFICIAL NEED FOR ACCESS TO DOD BUILDINGS IN THE NATIONAL CAPITAL REGION SHALL BE THE SUBJECT OF A FAVORABLY ADJUDICATED NAC PRIOR TO ISSUANCE OF A DOD BUILDING PASS. CONDUCT OF A BI FOR THIS PURPOSE IS PROHIBITED UNLESS APPROVED IN ADVANCE BY ODUSD(P). CPS, and affected FAOs in Mid-Atlantic Region, shall ensure that provisions of this paragraph are met prior to completing DD Form 2249, DoD Building Pass Request, and giving it to employees to take to the Pentagon. DoD Building Passes shall be requested by CPS in accordance with OASD (Comptroller) Administrative Instruction No. 30 (reference 1-100.p).

3-608 FOREIGN NATIONAL EMPLOYEES OVERSEAS NOT REQUIRING ACCESS TO CLASSIFIED INFORMATION

FOREIGN NATIONALS EMPLOYED BY DOD ORGANIZATIONS OVERSEAS, WHOSE DUTIES DO NOT REQUIRE ACCESS TO CLASSIFIED INFORMATION, SHALL BE THE SUBJECT OF THE FOLLOWING RECORD CHECKS, INITIATED BY THE APPROPRIATE MILITARY DEPARTMENT INVESTIGATIVE ORGANIZATION CONSISTENT WITH PARAGRAPH 2-404, PRIOR TO EMPLOYMENT:

A. HOST GOVERNMENT LAW ENFORCEMENT AND SECURITY AGENCY CHECKS AT THE CITY, STATE (PROVINCE), AND NATIONAL LEVEL, WHENEVER PERMISSIBLE BY THE LAWS OF THE HOST GOVERNMENT; AND

B. DCII;

C. FBI-HQ/ID (WHERE INFORMATION EXISTS REGARDING RESIDENCE BY THE FOREIGN NATIONAL IN THE UNITED STATES FOR ONE YEAR OR MORE SINCE AGE 18).

3-609 SPECIAL AGENTS AND INVESTIGATIVE SUPPORT PERSONNEL

SPECIAL AGENTS AND THOSE NONINVESTIGATIVE PERSONNEL ASSIGNED TO INVESTIGATIVE AGENCIES WHOSE OFFICIAL DUTIES REQUIRE CONTINUOUS ACCESS TO COMPLETE INVESTIGATIVE FILES AND MATERIAL REQUIRE AN SBI.

3-610 PERSONS REQUIRING ACCESS TO CHEMICAL AGENTS

PERSONNEL WHOSE DUTIES INVOLVE ACCESS TO OR SECURITY OF CHEMICAL AGENTS SHALL BE SCREENED INITIALLY FOR SUITABILITY AND RELIABILITY AND SHALL BE EVALUATED ON A CONTINUING BASIS AT THE SUPERVISORY LEVEL TO ENSURE THAT THEY CONTINUE TO MEET THE HIGH STANDARDS REQUIRED. AT A MINIMUM, ALL SUCH PERSONNEL SHALL HAVE HAD A FAVORABLY ADJUDICATED NAC COMPLETED WITHIN THE LAST 5 YEARS PRIOR TO ASSIGNMENT IN ACCORDANCE WITH THE PROVISIONS OF DOD DIRECTIVE 5210.65 (REFERENCE (Y)).

3-611 EDUCATION AND ORIENTATION PERSONNEL

PERSONS SELECTED FOR DUTIES IN CONNECTION WITH PROGRAMS INVOLVING THE EDUCATION AND ORIENTATION OF MILITARY PERSONNEL SHALL HAVE BEEN THE SUBJECT OF A FAVORABLY ADJUDICATED NAC PRIOR TO SUCH ASSIGNMENT. THIS DOES NOT INCLUDE TEACHERS/ADMINISTRATORS ASSOCIATED WITH UNIVERSITY EXTENSION COURSES CONDUCTED ON MILITARY INSTALLATIONS IN THE UNITED STATES. NON-US CITIZENS FROM A COUNTRY LISTED IN APPENDIX H SHALL BE REQUIRED TO UNDERGO A BI IF THEY ARE EMPLOYED IN A POSITION COVERED BY THIS PARAGRAPH.

3-612 CONTRACT GUARDS

ANY PERSON PERFORMING CONTRACT GUARD FUNCTIONS SHALL HAVE BEEN THE SUBJECT OF A FAVORABLY ADJUDICATED NAC PRIOR TO SUCH ASSIGNMENT.

3-613 TRANSPORTATION OF ARMS, AMMUNITION AND EXPLOSIVES (AAGE)

ANY DOD MILITARY, CIVILIAN OR CONTRACT EMPLOYEE (INCLUDING COMMERCIAL CARRIER) OPERATING A VEHICLE OR PROVIDING SECURITY TO A VEHICLE TRANSPORTING CATEGORY I, II OR CONFIDENTIAL AAGE SHALL HAVE BEEN THE SUBJECT OF A FAVORABLY ADJUDICATED NAC OR ENTNAC.

3-614 PERSONNEL OCCUPYING INFORMATION SYSTEMS POSITIONS DESIGNATED ADP-I, ADP-II & ADP-III

DOD MILITARY, CIVILIAN PERSONNEL, CONSULTANTS, AND CONTRACTOR PERSONNEL PERFORMING ON UNCLASSIFIED AUTOMATED INFORMATION SYSTEMS MAY BE ASSIGNED TO ONE OF THREE POSITION SENSITIVITY DESIGNATIONS (IN ACCORDANCE WITH APPENDIX K) AND INVESTIGATED AS FOLLOWS:

ADP-I:	BI
ADP-II:	DNACI/NACI
ADP-III:	NAC/ENTNAC

THOSE PERSONNEL FALLING IN THE ABOVE CATEGORIES WHO REQUIRE ACCESS TO CLASSIFIED INFORMATION WILL, OF COURSE, BE SUBJECT TO THE APPROPRIATE INVESTIGATIVE SCOPE CONTAINED IN PARAGRAPH 3-401, ABOVE.

3-615 OTHERS

REQUESTS FOR APPROVAL TO CONDUCT AN INVESTIGATION ON OTHER PERSONNEL, NOT PROVIDED FOR IN PARAGRAPHS 3-601 THROUGH 3-614, ABOVE, CONSIDERED TO FALL WITHIN THE GENERAL PROVISIONS OF PARAGRAPH 3-600 ABOVE, SHALL BE SUBMITTED, DETAILING THE JUSTIFICATION THEREFOR, FOR APPROVAL TO THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY. APPROVAL OF SUCH REQUESTS SHALL BE CONTINGENT UPON AN ASSURANCE THAT APPROPRIATE REVIEW PROCEDURES EXIST AND THAT ADVERSE DETERMINATIONS WILL BE MADE AT NO LOWER THAN MAJOR COMMAND LEVEL.

Section 7

REINVESTIGATION

3-700 GENERAL

DOD POLICY PROHIBITS UNAUTHORIZED AND UNNECESSARY INVESTIGATIONS. THERE ARE, HOWEVER, CERTAIN SITUATIONS AND REQUIREMENTS THAT NECESSITATE REINVESTIGATION OF AN INDIVIDUAL WHO HAS ALREADY BEEN INVESTIGATED UNDER THE PROVISIONS OF THIS REGULATION. IT IS THE POLICY TO LIMIT REINVESTIGATION OF INDIVIDUALS TO THE SCOPE CONTAINED IN PARAGRAPH 3, APPENDIX B TO MEET OVERALL SECURITY REQUIREMENTS. REINVESTIGATION, GENERALLY, IS AUTHORIZED ONLY AS FOLLOWS:

A. TO PROVE OR DISPROVE AN ALLEGATION RELATING TO THE CRITERIA SET FORTH IN PARAGRAPH 2-200 OF THIS REGULATION WITH RESPECT TO AN INDIVIDUAL HOLDING A SECURITY CLEARANCE OR ASSIGNED TO A POSITION THAT REQUIRES A TRUSTWORTHINESS DETERMINATION;

B. TO MEET THE PERIODIC REINVESTIGATION REQUIREMENTS OF THIS REGULATION WITH RESPECT TO THOSE SECURITY PROGRAMS ENUMERATED BELOW; AND

C. UPON INDIVIDUAL REQUEST, TO ASSESS THE CURRENT ELIGIBILITY OF INDIVIDUALS WHO DID NOT RECEIVE FAVORABLE ADJUDICATIVE ACTION AFTER AN INITIAL INVESTIGATION, IF A POTENTIAL CLEARANCE NEED EXISTS AND THERE ARE REASONABLE INDICATIONS THAT THE FACTORS UPON WHICH THE ADVERSE DETERMINATION WAS MADE NO LONGER EXISTS.

3-701 ALLEGATIONS RELATED TO DISQUALIFICATION

WHENEVER QUESTIONABLE BEHAVIOR PATTERNS DEVELOP, DEROGATORY INFORMATION IS DISCOVERED, OR INCONSISTENCIES ARISE RELATED TO THE DISQUALIFICATION CRITERIA OUTLINED IN PARAGRAPH 2-200 THAT COULD HAVE AN ADVERSE IMPACT ON AN INDIVIDUAL'S SECURITY STATUS, A SPECIAL INVESTIGATIVE INQUIRY (SII), PSYCHIATRIC, DRUG OR ALCOHOL EVALUATION, AS APPROPRIATE, MAY BE REQUESTED TO RESOLVE ALL RELEVANT ISSUES IN DOUBT. IF IT IS ESSENTIAL THAT ADDITIONAL RELEVANT PERSONAL DATA IS REQUIRED FROM THE INVESTIGATIVE SUBJECT, AND THE SUBJECT FAILS TO FURNISH THE REQUIRED DATA, THE SUBJECT'S EXISTING SECURITY CLEARANCE OR ASSIGNMENT TO SENSITIVE DUTIES SHALL BE TERMINATED IN ACCORDANCE WITH PARAGRAPH 8-201 OF THIS REGULATION.

3-702 ACCESS TO SENSITIVE COMPARTMENTED INFORMATION (SCI)

EACH INDIVIDUAL HAVING CURRENT ACCESS TO SCI SHALL BE THE SUBJECT OF A PR CONDUCTED ON A 5-YEAR RECURRING BASIS SCOPED AS SET FORTH IN PARAGRAPH 5, APPENDIX B.

3-703 CRITICAL-SENSITIVE POSITIONS

EACH DOD CIVILIAN EMPLOYEE OCCUPYING A CRITICAL SENSITIVE POSITION SHALL BE THE SUBJECT OF A PR CONDUCTED ON A 5-YEAR RECURRING BASIS SCOPED AS SET FORTH IN PARAGRAPH 5, APPENDIX B.

3-704 PRESIDENTIAL SUPPORT DUTIES

EACH INDIVIDUAL ASSIGNED PRESIDENTIAL SUPPORT DUTIES SHALL BE THE SUBJECT OF A PR CONDUCTED ON A 5-YEAR RECURRING BASIS SCOPED AS SET FORTH IN PARAGRAPH 5, APPENDIX B. See section 3-503 and reference h.

3-705 NATO STAFF

EACH INDIVIDUAL ASSIGNED TO A NATO STAFF POSITION REQUIRING A COSMIC CLEARANCE SHALL BE THE SUBJECT OF A PR CONDUCTED ON A 5-YEAR RECURRING BASIS SCOPED AS SET FORTH IN PARAGRAPH 5, APPENDIX B. THOSE ASSIGNED TO A NATO STAFF POSITION REQUIRING A NATO SECRET CLEARANCE SHALL BE THE SUBJECT OF A NEW NAC CONDUCTED ON A 5-YEAR RECURRING BASIS.

3-706 EXTRAORDINARILY SENSITIVE DUTIES

IN EXTREMELY LIMITED INSTANCES, EXTRAORDINARY NATIONAL SECURITY IMPLICATIONS ASSOCIATED WITH CERTAIN SCI DUTIES MAY REQUIRE VERY SPECIAL COMPARTMENTATION AND OTHER SPECIAL SECURITY MEASURES. IN SUCH INSTANCES, A COMPONENT SOIC MAY, WITH THE APPROVAL OF THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY, REQUEST PR'S AT INTERVALS OF LESS THAN 5 YEARS AS OUTLINED IN PARAGRAPH 5, APPENDIX B. SUCH REQUESTS SHALL INCLUDE FULL JUSTIFICATION AND A RECOMMENDATION AS TO THE DESIRED FREQUENCY. IN REVIEWING SUCH REQUESTS, THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY SHALL GIVE DUE CONSIDERATION TO:

A. THE POTENTIAL DAMAGE THAT MIGHT RESULT FROM THE INDIVIDUAL'S DEFECTION OR ABDUCTION.

B. THE AVAILABILITY AND PROBABLE EFFECTIVENESS OF MEANS OTHER THAN REINVESTIGATION TO EVALUATE FACTORS CONCERNING THE INDIVIDUAL'S SUITABILITY FOR CONTINUED SCI ACCESS.

The Director, Field Detachment, will coordinate all requests under this paragraph with the ASO.

3-707 FOREIGN NATIONALS EMPLOYED BY DOD ORGANIZATIONS OVERSEAS

FOREIGN NATIONALS EMPLOYED BY DOD ORGANIZATIONS OVERSEAS WHO HAVE BEEN GRANTED A "LIMITED ACCESS AUTHORIZATION" PURSUANT TO PARAGRAPH 3-402 SHALL BE THE SUBJECT OF A PR, AS SET FORTH IN PARAGRAPH 5, APPENDIX B, CONDUCTED UNDER THE AUSPICES OF DIS BY THE APPROPRIATE MILITARY DEPARTMENT OR OTHER U.S. GOVERNMENT INVESTIGATIVE AGENCY CONSISTENT WITH PARAGRAPH 2-404 AND APPENDIX J OF THIS REGULATION.

3-708 PERSONS ACCESSING VERY SENSITIVE INFORMATION CLASSIFIED SECRET

A. HEADS OF DOD COMPONENTS SHALL SUBMIT A REQUEST TO THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY FOR APPROVAL TO CONDUCT PERIODIC REINVESTIGATIONS ON PERSONS HOLDING SECRET CLEARANCES WHO ARE EXPOSED TO VERY SENSITIVE SECRET INFORMATION.

B. GENERALLY, THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY WILL ONLY APPROVE PERIODIC REINVESTIGATIONS OF PERSONS HAVING ACCESS TO SECRET INFORMATION IF THE UNAUTHORIZED DISCLOSURE OF THE INFORMATION IN QUESTION COULD REASONABLY BE EXPECTED TO:

- (1) JEOPARDIZE HUMAN LIFE OR SAFETY.
- (2) RESULT IN THE LOSS OF UNIQUE OR UNIQUELY PRODUCTIVE INTELLIGENCE SOURCES OR METHODS VITAL TO U.S. SECURITY.
- (3) COMPROMISE TECHNOLOGIES, PLANS, OR PROCEDURES VITAL TO THE STRATEGIC ADVANTAGE OF THE UNITED STATES.

C. EACH INDIVIDUAL ACCESSING VERY SENSITIVE SECRET INFORMATION WHO HAS BEEN DESIGNATED BY AN AUTHORITY LISTED IN PARAGRAPH A, APPENDIX F AS REQUIRING PERIODIC REINVESTIGATION, SHALL BE THE SUBJECT OF A PR CONDUCTED ON A 5-YEAR RECURRING BASIS SCOPED AS STATED IN PARAGRAPH 5, APPENDIX B.

3-709 ACCESS TO TOP SECRET INFORMATION

EACH INDIVIDUAL HAVING CURRENT ACCESS TO TOP SECRET INFORMATION SHALL BE THE SUBJECT OF A PR CONDUCTED ON A 5-YEAR RECURRING BASIS SCOPED AS OUTLINED IN PARAGRAPH 5, APPENDIX B.

3-710 PERSONNEL OCCUPYING COMPUTER POSITIONS DESIGNATED ADP-I

ALL DOD MILITARY, CIVILIANS, CONSULTANTS, AND CONTRACTOR PERSONNEL OCCUPYING COMPUTER POSITIONS DESIGNATED ADP-I, SHALL BE THE SUBJECT OF A PR CONDUCTED ON A 5-YEAR RECURRING BASIS AS SET FORTH IN PARAGRAPH 5, APPENDIX B.

Section 8

AUTHORITY TO WAIVE INVESTIGATIVE REQUIREMENTS

3-800 AUTHORIZED OFFICIALS

ONLY AN OFFICIAL DESIGNATED IN PARAGRAPH G, APPENDIX F, IS EMPOWERED TO WAIVE THE INVESTIGATIVE REQUIREMENTS FOR APPOINTMENT TO A SENSITIVE POSITION, ASSIGNMENT TO SENSITIVE DUTIES OR ACCESS TO CLASSIFIED INFORMATION PENDING COMPLETION OF THE INVESTIGATION REQUIRED BY THIS CHAPTER. SUCH WAIVER SHALL BE BASED UPON CERTIFICATION IN WRITING BY THE DESIGNATED OFFICIAL THAT SUCH ACTION IS NECESSARY TO THE ACCOMPLISHMENT OF A DOD MISSION. A MINOR INVESTIGATIVE ELEMENT THAT HAS NOT BEEN MET SHOULD NOT PRECLUDE FAVORABLE ADJUDICATION--NOR SHOULD THIS REQUIRE A WAIVER WHEN ALL OTHER INFORMATION DEVELOPED ON AN INDIVIDUAL DURING THE COURSE OF A PRESCRIBED INVESTIGATION IS FAVORABLE.

Within DCAA, only the following officials may waive investigative requirements when no access to classified information will be needed:

a. Critical-sensitive Positions

Assistant Director, Resources, for all Headquarters, FD, and regional positions.

b. Noncritical-sensitive Positions

Assistant Director, Resources, for all Headquarters positions (except FD);

Regional directors for all field positions; and
Director, Field Detachment for FD positions.

The certification in writing required by this paragraph will be an appropriately completed DCAA Form 5210-43, Waiver of Required Preappointment Security Investigation.

CHAPTER IV

RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS

4-100 GENERAL

INVESTIGATIONS CONDUCTED BY DOD ORGANIZATIONS OR ANOTHER AGENCY OF THE FEDERAL GOVERNMENT SHALL NOT BE DUPLICATED WHEN THOSE INVESTIGATIONS MEET THE SCOPE AND STANDARDS FOR THE LEVEL OF THE CLEARANCE OR ACCESS REQUIRED. THE DOD COMPONENTS THAT GRANT ACCESS (SCI OR SAP) OR ISSUE SECURITY CLEARANCES (TOP SECRET, SECRET, AND CONFIDENTIAL) TO CIVILIAN AND/OR MILITARY OR CONTRACTOR EMPLOYEES ARE RESPONSIBLE FOR DETERMINING WHETHER SUCH INDIVIDUALS HAVE BEEN PREVIOUSLY CLEARED OR INVESTIGATED BY THE U.S. GOVERNMENT. ANY PREVIOUSLY GRANTED SECURITY CLEARANCE OR ACCESS, WHICH IS BASED UPON A CURRENT INVESTIGATION OF A SCOPE THAT MEETS OR EXCEEDS THAT NECESSARY FOR THE CLEARANCE OR ACCESS REQUIRED, SHALL PROVIDE THE BASIS FOR ISSUANCE OF A NEW CLEARANCE AND/OR ACCESS WITHOUT FURTHER INVESTIGATION OR ADJUDICATION. PREVIOUSLY CONDUCTED INVESTIGATIONS AND PREVIOUSLY RENDERED PERSONNEL SECURITY DETERMINATIONS SHALL BE ACCEPTED WITHIN THE DEPARTMENT OF DEFENSE, IN ACCORDANCE WITH THE POLICY IN SECTIONS 4-101 THROUGH 4-103 BELOW.

4-101 PRIOR PERSONNEL SECURITY INVESTIGATIONS

AS LONG AS THERE IS NO BREAK IN MILITARY SERVICE AND/OR FEDERAL EMPLOYMENT GREATER THAN 24 MONTHS, ANY PREVIOUS PERSONNEL SECURITY INVESTIGATION THAT ESSENTIALLY IS EQUIVALENT IN SCOPE TO AN INVESTIGATION REQUIRED BY THIS REGULATION WILL BE ACCEPTED WITHOUT REQUESTING ADDITIONAL INVESTIGATION. THERE IS NO TIME LIMITATION AS TO THE ACCEPTABILITY OF SUCH INVESTIGATIONS, SUBJECT TO THE PROVISIONS OF PARAGRAPHS 2-307 AND 4-102.B. OF THIS REGULATION.

4-102 PRIOR PERSONNEL SECURITY DETERMINATIONS MADE BY DOD AUTHORITIES

A. ADJUDICATIVE DETERMINATIONS FOR APPOINTMENT IN SENSITIVE POSITIONS, ASSIGNMENT TO SENSITIVE DUTIES OR ACCESS TO CLASSIFIED INFORMATION (INCLUDING THOSE PERTAINING TO SCI) MADE BY DESIGNATED DOD AUTHORITIES WILL BE MUTUALLY AND RECIPROCALLY ACCEPTED BY ALL DOD COMPONENTS WITHOUT REQUIRING ADDITIONAL INVESTIGATION, UNLESS THERE HAS BEEN A BREAK IN THE INDIVIDUAL'S MILITARY SERVICE AND/OR FEDERAL EMPLOYMENT OF GREATER THAN 24 MONTHS OR UNLESS DEROGATORY INFORMATION THAT OCCURRED SUBSEQUENT TO THE LAST PRIOR SECURITY DETERMINATION BECOMES KNOWN. A CHECK OF THE DCII OR OTHER APPROPRIATE DATA BASES SHOULD BE CONDUCTED TO ACCOMPLISH THIS TASK. Subject to the conditions set forth above, personnel employed in sensitive positions within components of the DoD shall be deemed eligible for employment in positions of the same sensitivity within DCAA, consistent with the investigation basis required for employment in critical-sensitive or noncritical-sensitive positions. Security specialists will ensure that a check of the DCII is accomplished in accordance with provisions of this paragraph whenever an applicant reflects previous employment with any DoD component on SF 171, application, or resume. The DCII check will be made a matter of record using DCAA Form 5210-46, Worksheet for Security Inquiry. See Enclosure 3, Section 2, for detailed guidance.

ADJUDICATED. Only CPS will communicate information on a DCAA employee transferring to another DoD activity in accordance with provisions of this paragraph. (See section 1, Chapter IX of this manual on responsibilities to report security eligibility information.) Should CPS be advised by another DoD activity of adverse information on an employee transferring into DCAA, CPS shall ensure that the information is forwarded to the WHS CAF for adjudication prior to requesting a security clearance.

4-103 INVESTIGATIONS CONDUCTED AND CLEARANCES GRANTED BY OTHER AGENCIES OF THE FEDERAL GOVERNMENT

A. WHENEVER A PRIOR INVESTIGATION OR PERSONNEL SECURITY DETERMINATION (INCLUDING CLEARANCE FOR ACCESS TO INFORMATION CLASSIFIED UNDER EXECUTIVE ORDER 12356 (REFERENCE (J)) OF ANOTHER AGENCY OF THE FEDERAL GOVERNMENT MEETS THE INVESTIGATIVE SCOPE AND STANDARDS OF THIS REGULATION, SUCH INVESTIGATION OR CLEARANCE MAY BE ACCEPTED FOR THE INVESTIGATIVE OR CLEARANCE PURPOSES OF THIS REGULATION, PROVIDED THAT THE EMPLOYMENT WITH THE FEDERAL AGENCY CONCERNED HAS BEEN CONTINUOUS AND THERE HAS BEEN NO BREAK LONGER THAN 24 MONTHS SINCE COMPLETION OF THE PRIOR INVESTIGATION, AND FURTHER PROVIDED THAT INQUIRY WITH THE AGENCY DISCLOSES NO REASON WHY THE CLEARANCE SHOULD NOT BE ACCEPTED. IF IT IS DETERMINED THAT THE PRIOR INVESTIGATION DOES NOT MEET THE PROVISIONS OF THIS PARAGRAPH, SUPPLEMENTAL INVESTIGATION SHALL BE REQUESTED.

The investigations listed below, conducted for civilian employment, may be accepted for initial appointment within DCAA, provided that the individual has been continuously employed in the Federal agency concerned, that there has been no break longer than 24 months since the completion of the prior investigation, and an inquiry to the previous employing agency discloses no reason why the individual should not be hired or granted a security clearance. Determinations of such investigations must be supported by information obtained from the security office, personnel office, and former supervisors and other cognizant officials when appropriate, and will be made a matter of record using any combination of inquiry forms, records of telephone conversations, and/or DCAA Form 5210-46, that fully identifies the information obtained and the source(s) of information.

1. "Records Check and Inquiry," conducted by OPM pursuant to Section 3, Part 1, Executive Order 9835, may be accepted as the equivalent of a NACI.

2. "Preappointment Loyalty Check," conducted by the OPM pursuant to Executive Order 9835, provided an FBI fingerprint check is included, may be accepted as the equivalent of a NAC. This does not include the records checks conducted by the FBI under Part VI, Executive Order 9835, since such checks are not the equivalent of a NAC. (NACI would have to be initiated postappointment.)

3. "National Agency Check," including FBI fingerprint check, conducted by OPM or DIS pursuant to Executive Order 10450. (Initiate NACI postappointment.)

4. A NACI conducted for another department or agency by the OPM, may be accepted provided that the investigation disclosed no derogatory information of the type covered by Section 3(a) of Executive 10450, as amended, or other equally questionable information.

MARCH 1996

5. Character Investigation (CI) conducted by the Internal Revenue Service (IRS), provided that an inquiry is made with the IRS Investigation Files Division, Washington, D.C., and no adverse information is contained in the file.

6. "Full Field Investigation" (Background Investigation) pursuant to Executive Order 10450 by a U.S. Government investigative agency may be accepted provided it is determined upon review of the investigative report that it meets the investigative scope prescribed in Appendix B for a BI.

(See Enclosure 3 for guidance on verification of the above investigations.)

B. A NACI CONDUCTED BY OPM SHALL BE ACCEPTED AND CONSIDERED EQUIVALENT TO A DNACI FOR THE PURPOSES OF THIS REGULATION. If NACI is verified (in accordance with this paragraph) as "resulted," and has not been reviewed and favorably adjudicated by another DoD component, a copy must be requested for forwarding to the WHS CAF for review and adjudication. See section 2, Enclosure 3, for guidance on using OFI Form 79B.

C. DEPARTMENT OF DEFENSE POLICY ON RECIPROCAL ACCEPTANCE OF CLEARANCES WITH THE NUCLEAR REGULATORY COMMISSION AND THE DEPARTMENT OF ENERGY IS SET FORTH IN DOD DIRECTIVE 5210.2 (REFERENCE (Z)). (Also, see DCAAM Regulation 5210.3 (reference 1-100.j)).

CHAPTER V

REQUESTING PERSONNEL SECURITY INVESTIGATIONS

5-100 GENERAL

REQUESTS FOR PERSONNEL SECURITY INVESTIGATIONS SHALL BE LIMITED TO THOSE REQUIRED TO ACCOMPLISH THE DEFENSE MISSION. SUCH REQUESTS SHALL BE SUBMITTED ONLY BY THE AUTHORITIES DESIGNATED IN PARAGRAPH 5-101 BELOW. THESE AUTHORITIES SHALL BE HELD RESPONSIBLE FOR DETERMINING IF PERSONS UNDER THEIR JURISDICTION REQUIRE A PERSONNEL SECURITY INVESTIGATION. PROPER PLANNING MUST BE EFFECTED TO ENSURE THAT INVESTIGATIVE REQUESTS ARE SUBMITTED SUFFICIENTLY IN ADVANCE TO ALLOW COMPLETION OF THE INVESTIGATION BEFORE THE TIME IT IS NEEDED TO GRANT THE REQUIRED CLEARANCE OR OTHERWISE MAKE THE NECESSARY PERSONNEL SECURITY DETERMINATION.

5-101 AUTHORIZED REQUESTERS

REQUESTS FOR PERSONNEL SECURITY INVESTIGATION SHALL BE ACCEPTED ONLY FROM THE REQUESTERS DESIGNATED BELOW:

A. MILITARY DEPARTMENTS

(1) ARMY

(A) CENTRAL CLEARANCE FACILITY.

(B) ALL ACTIVITY COMMANDERS.

(C) CHIEFS OF RECRUITING STATIONS.

(2) NAVY (INCLUDING MARINE CORPS)

(A) CENTRAL ADJUDICATIVE FACILITY

(B) COMMANDERS AND COMMANDING OFFICERS OF ORGANIZATIONS LISTED ON THE STANDARD NAVY DISTRIBUTION LIST.

(C) CHIEFS OF RECRUITING STATIONS.

(3) AIR FORCE

(A) AIR FORCE SECURITY CLEARANCE OFFICE.

(B) ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE.

(C) ALL ACTIVITY COMMANDERS.

(D) CHIEFS OF RECRUITING STATIONS.

B. DEFENSE AGENCIES--DIRECTORS OF SECURITY AND ACTIVITY COMMANDERS.

In accordance with this section, the ASO, the Director, PD, and regional directors are authorized to request personnel security investigations. The ASO, the Director, PD, and regional directors may delegate signatory

authority for DD Form 1879 to their security specialists if they so desire. This delegation of authority should be made in writing and filed in the appropriate file series described in DCAAM 5015.1.

C. ORGANIZATION OF THE JOINT CHIEFS OF STAFF--CHIEF, SECURITY DIVISION.

D. OFFICE OF THE SECRETARY OF DEFENSE--DIRECTOR FOR PERSONNEL AND SECURITY, WASHINGTON HEADQUARTERS SERVICES.

E. COMMANDERS OF UNIFIED AND SPECIFIED COMMANDS OR THEIR DESIGNEES.

F. SUCH OTHER REQUESTERS APPROVED BY THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY.

5-102 CRITERIA FOR REQUESTING INVESTIGATIONS

AUTHORIZED REQUESTERS SHALL USE THE TABLES SET FORTH IN APPENDIX D TO DETERMINE THE TYPE OF INVESTIGATION THAT SHALL BE REQUESTED TO MEET THE INVESTIGATIVE REQUIREMENT OF THE SPECIFIC POSITION OR DUTY CONCERNED.

5-103 REQUEST PROCEDURES

TO INSURE EFFICIENT AND EFFECTIVE COMPLETION OF REQUIRED INVESTIGATIONS, ALL REQUESTS FOR PERSONNEL SECURITY INVESTIGATIONS SHALL BE PREPARED AND FORWARDED IN ACCORDANCE WITH APPENDIX C AND THE INVESTIGATIVE JURISDICTIONAL POLICIES SET FORTH IN SECTION 4, CHAPTER II OF THIS REGULATION. All requests will be prepared and forwarded in accordance with this section and Enclosure 3, with a copy furnished to CPS. Headquarters security specialists will monitor and request investigations for regional directors, Director, Field Detachment, regional security officers, alternate regional security officers, and Field Detachment security officer.

5-104 PRIORITY REQUESTS

TO INSURE THAT PERSONNEL SECURITY INVESTIGATIONS ARE CONDUCTED IN AN ORDERLY AND EFFICIENT MANNER, REQUESTS FOR PRIORITY FOR INDIVIDUAL INVESTIGATIONS OR CATEGORIES OF INVESTIGATIONS SHALL BE KEPT TO A MINIMUM. DIS SHALL NOT ASSIGN PRIORITY TO ANY PERSONNEL SECURITY INVESTIGATION OR CATEGORIES OF INVESTIGATIONS WITHOUT WRITTEN APPROVAL OF THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY. Requests for priority handling of investigations must be endorsed by regional directors and forwarded to CPS with the following information to be conveyed to DIS:

a. The basis for priority handling, i.e., explain the urgency which warrants expediting the investigation.

b. The current geographic location of the subject of the investigation.

c. The completed, signed DD Form 1879, SF 86 or 85P, and related forms, with other relevant specifics, if any.

5-105 PERSONAL DATA PROVIDED BY THE SUBJECT OF THE INVESTIGATION

A. TO CONDUCT THE REQUIRED INVESTIGATION, IT IS NECESSARY THAT THE INVESTIGATIVE AGENCY BE PROVIDED CERTAIN RELEVANT DATA CONCERNING THE SUBJECT OF THE INVESTIGATION. THE PRIVACY ACT OF 1974 (REFERENCE (M)) REQUIRES THAT, TO THE GREATEST EXTENT PRACTICABLE, PERSONAL INFORMATION SHALL BE OBTAINED DIRECTLY FROM THE SUBJECT INDIVIDUAL WHEN THE INFORMATION MAY RESULT IN ADVERSE DETERMINATIONS AFFECTING AN INDIVIDUAL'S RIGHTS, BENEFITS, AND PRIVILEGES UNDER FEDERAL PROGRAMS.

B. ACCORDINGLY, IT IS INCUMBENT UPON THE SUBJECT OF EACH PERSONNEL SECURITY INVESTIGATION TO PROVIDE THE PERSONAL INFORMATION REQUIRED BY THIS REGULATION. AT A MINIMUM, THE INDIVIDUAL SHALL COMPLETE THE APPROPRIATE INVESTIGATIVE FORMS, PROVIDE FINGERPRINTS OF A QUALITY ACCEPTABLE TO THE FBI, AND EXECUTE A SIGNED RELEASE, AS NECESSARY, AUTHORIZING CUSTODIANS OF POLICY, CREDIT, EDUCATION, EMPLOYMENT, AND MEDICAL AND SIMILAR RECORDS, TO PROVIDE RELEVANT RECORD INFORMATION TO THE INVESTIGATIVE AGENCY. WHEN THE FBI RETURNS A FINGERPRINT CARD INDICATING THAT THE QUALITY OF THE FINGERPRINTS IS NOT ACCEPTABLE, AN ADDITIONAL SET OF FINGERPRINTS WILL BE OBTAINED FROM THE SUBJECT. IN THE EVENT THE FBI INDICATES THAT THE ADDITIONAL FINGERPRINTS ARE ALSO UNACCEPTABLE, NO FURTHER ATTEMPT TO OBTAIN MORE FINGERPRINTS NEED BE MADE; THIS ASPECT OF THE INVESTIGATION WILL THEN BE PROCESSED ON THE BASIS OF THE NAME CHECK OF THE FBI FILES. AS AN EXCEPTION, A MINIMUM OF THREE ATTEMPTS WILL BE MADE (1) FOR ALL PRESIDENTIAL SUPPORT CASES, (2) FOR SCI ACCESS NOMINATIONS IF THE REQUESTER SO INDICATES, AND (3) IN THOSE CASES IN WHICH MORE THAN MINOR DEROGATORY INFORMATION EXISTS. EACH SUBJECT OF A PERSONNEL SECURITY INVESTIGATION CONDUCTED UNDER THE PROVISIONS OF THIS REGULATION SHALL BE FURNISHED A PRIVACY ACT STATEMENT ADVISING OF (1) THE AUTHORITY FOR OBTAINING THE PERSONAL DATA, (2) THE PRINCIPAL PURPOSE(S) FOR OBTAINING IT, (3) THE ROUTINE USES, (4) WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY, (5) THE EFFECT ON THE INDIVIDUAL IF IT IS NOT PROVIDED, AND (6) THAT SUBSEQUENT USE OF THE DATA MAY BE EMPLOYED AS PART OF AN APERIODIC REVIEW PROCESS TO EVALUATE CONTINUED ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION. Contrary to the above, DIS and OPM will not generally request a second fingerprint submission. If FBI returns prints, either to OPM or DIS, which indicate "name check only" in their investigative reports, a second set of prints will normally not be obtained. DIS may request a second submission if no technical check has ever been classifiable. OPM granted DoD a waiver of the second submission requirement effective 10 October 1995; criminal history name search satisfies OPM investigative requirements. A third submission of prints is only necessary under the exception provisions of this paragraph, and as may be specifically requested by USOPM.

C. FAILURE TO RESPOND WITHIN THE TIME LIMIT PRESCRIBED BY THE REQUESTING ORGANIZATION WITH THE REQUIRED SECURITY FORMS OR REFUSAL TO PROVIDE OR PERMIT ACCESS TO THE RELEVANT INFORMATION REQUIRED BY THIS REGULATION SHALL RESULT IN TERMINATION OF THE INDIVIDUAL'S SECURITY CLEARANCE OR ASSIGNMENT TO SENSITIVE DUTIES UTILIZING THE PROCEDURES OF PARAGRAPH 8-201 OR FURTHER ADMINISTRATIVE PROCESSING OF THE INVESTIGATIVE REQUEST. Any failure or refusal by an individual to provide or permit access to relevant information required under this paragraph, shall be forwarded to CPS for referral to the WBS CAP for action under section 8-201.

MARCH 1996

CHAPTER VI

ADJUDICATION

6-100 GENERAL

A. THE STANDARD WHICH MUST BE MET FOR CLEARANCE OR ASSIGNMENT TO SENSITIVE DUTIES IS THAT, BASED ON ALL AVAILABLE INFORMATION, THE PERSON'S LOYALTY, RELIABILITY, AND TRUSTWORTHINESS ARE SUCH THAT ENTRUSTING THE PERSON WITH CLASSIFIED INFORMATION OR ASSIGNING THE PERSON TO SENSITIVE DUTIES IS CLEARLY CONSISTENT WITH THE INTERESTS OF NATIONAL SECURITY. Personnel officers are responsible for adjudicating suitability issues, as required, in accordance with 5 CFR Part 731, and for advising the requesting official in writing.

B. THE PRINCIPAL OBJECTIVE OF THE DOD PERSONNEL SECURITY ADJUDICATIVE FUNCTION, CONSEQUENTLY, IS TO ASSURE SELECTION OF PERSONS FOR SENSITIVE POSITIONS WHO MEET THIS STANDARD. THE ADJUDICATION PROCESS INVOLVES THE EFFORT TO ASSESS THE PROBABILITY OF FUTURE BEHAVIOR WHICH COULD HAVE AN EFFECT ADVERSE TO THE NATIONAL SECURITY. SINCE FEW, IF ANY, SITUATIONS ALLOW FOR POSITIVE, CONCLUSIVE EVIDENCE OF CERTAIN FUTURE CONDUCT, IT IS AN ATTEMPT TO JUDGE WHETHER THE CIRCUMSTANCES OF A PARTICULAR CASE, TAKING INTO CONSIDERATION PRIOR EXPERIENCE WITH SIMILAR CASES, REASONABLY SUGGEST A DEGREE OF PROBABILITY OF PREJUDICIAL BEHAVIOR NOT CONSISTENT WITH THE NATIONAL SECURITY. IT IS INVARIABLY A SUBJECTIVE DETERMINATION, CONSIDERING THE PAST BUT NECESSARILY ANTICIPATING THE FUTURE. RARELY IS PROOF OF TRUSTWORTHINESS AND RELIABILITY OR UNTRUSTWORTHINESS AND UNRELIABILITY BEYOND ALL REASONABLE DOUBT. Reports of investigations, that are obtained by DCAA for review prior to selection of individuals for assignment to sensitive positions, will be forwarded to CPS for further transmission to the WHS CAF or DIA CCF for adjudication.

C. ESTABLISHING RELEVANCY IS ONE OF THE KEY OBJECTIVES OF THE PERSONNEL SECURITY ADJUDICATIVE PROCESS IN EVALUATING INVESTIGATIVE MATERIAL. IT INVOLVES NEITHER THE JUDGMENT OF CRIMINAL GUILT NOR THE DETERMINATION OF GENERAL SUITABILITY FOR A GIVEN POSITION; RATHER, IT IS THE ASSESSMENT OF A PERSON'S TRUSTWORTHINESS AND FITNESS FOR A RESPONSIBILITY WHICH COULD, IF ABUSED, HAVE UNACCEPTABLE CONSEQUENCES FOR THE NATIONAL SECURITY.

D. WHILE EQUITY DEMANDS OPTIMAL UNIFORMITY IN EVALUATING INDIVIDUAL CASES, ASSURING FAIR AND CONSISTENT ASSESSMENT OF CIRCUMSTANCES FROM ONE SITUATION TO THE NEXT, EACH CASE MUST BE WEIGHED ON ITS OWN MERITS, TAKING INTO CONSIDERATION ALL RELEVANT FACTS, AND PRIOR EXPERIENCE IN SIMILAR CASES. ALL INFORMATION OF RECORD, BOTH FAVORABLE AND UNFAVORABLE, MUST BE CONSIDERED AND ASSESSED IN TERMS OF ACCURACY, COMPLETENESS, RELEVANCE, SERIOUSNESS, AND OVERALL SIGNIFICANCE. IN ALL ADJUDICATIONS THE PROTECTION OF THE NATIONAL SECURITY SHALL BE THE PARAMOUNT DETERMINANT.

6-101 CENTRAL ADJUDICATION

A. TO ENSURE UNIFORM APPLICATION OF THE REQUIREMENT OF THIS REGULATION AND TO ENSURE THAT DOD PERSONNEL SECURITY DETERMINATIONS ARE EFFECTED CONSISTENT WITH EXISTING STATUTES AND EXECUTIVE ORDERS, THE HEAD OF EACH MILITARY DEPARTMENT AND DEFENSE AGENCIES SHALL ESTABLISH A SINGLE CENTRAL ADJUDICATION FACILITY FOR HIS/HER COMPONENT. THE FUNCTION OF SUCH FACILITY SHALL BE LIMITED TO EVALUATING PERSONNEL SECURITY INVESTIGATIONS AND MAKING PERSONNEL SECURITY

DETERMINATIONS. THE CHIEF OF EACH CENTRAL ADJUDICATION FACILITY SHALL HAVE THE AUTHORITY TO ACT ON BEHALF OF THE HEAD OF THE COMPONENT CONCERNED WITH RESPECT TO PERSONNEL SECURITY DETERMINATIONS. ALL INFORMATION RELEVANT TO DETERMINING WHETHER A PERSON MEETS THE APPROPRIATE PERSONNEL SECURITY STANDARD PRESCRIBED BY THIS REGULATION SHALL BE REVIEWED AND EVALUATED BY PERSONNEL SECURITY SPECIALISTS SPECIFICALLY DESIGNATED BY THE HEAD OF THE COMPONENT CONCERNED, OR DESIGNEE. The WHS CAF (for collateral access) and the DIA CCF (for SCI access) adjudicate personnel security investigations on sensitive position employees/applicants for DCAA. All correspondence to DCAA employees, (including Letters of Intent (LoI) or Statements of Reason (SORs)), are forwarded from the WHS CAF and the DIA CCF through the ASO. The ASO monitors receipt and response by the employee. The WHS CAF uses SD Form 176 and the DIA CCF uses DIA Form 1557A to notify the ASO when final security determinations are made. CPS will issue an Access and Eligibility Certificate (C/E Cert) to record completion of investigations and clearances, and will forward C/E Certs to the security specialists for distribution in accordance with paragraph 7-101.A.

B. IN VIEW OF THE SIGNIFICANCE EACH ADJUDICATIVE DECISION CAN HAVE ON A PERSON'S CAREER AND TO ENSURE THE MAXIMUM DEGREE OF FAIRNESS AND EQUITY IN SUCH ACTIONS, A MINIMUM LEVEL OF REVIEW SHALL BE REQUIRED FOR ALL CLEARANCE/ACCESS DETERMINATIONS RELATING TO THE FOLLOWING CATEGORIES OF INVESTIGATIONS:

(1) BI/SBI/PR/ENAC/SII:

(A) FAVORABLE: COMPLETELY FAVORABLE INVESTIGATIONS SHALL BE REVIEWED AND APPROVED BY AN ADJUDICATIVE OFFICIAL IN THE CIVILIAN GRADE OF GS-7/9 OR THE MILITARY RANK OF O-3.

(B) UNFAVORABLE: INVESTIGATIONS THAT ARE NOT COMPLETELY FAVORABLE SHALL UNDERGO AT LEAST TWO LEVELS OF REVIEW BY ADJUDICATIVE OFFICIALS, THE SECOND OF WHICH MUST BE AT THE CIVILIAN GRADE OF GS-11/12 OR THE MILITARY RANK OF O-4. WHEN AN UNFAVORABLE ADMINISTRATIVE ACTION IS CONTEMPLATED UNDER PARAGRAPH 8-201, THE LETTER OF INTENT (LOI) TO DENY OR REVOKE MUST BE APPROVED AND SIGNED BY AN ADJUDICATIVE OFFICIAL AT THE CIVILIAN GRADE OF GS-13/14 OR THE MILITARY RANK OF O-5. A FINAL NOTIFICATION OF UNFAVORABLE ADMINISTRATIVE ACTION, SUBSEQUENT TO THE ISSUANCE OF THE LOI, MUST BE APPROVED AND SIGNED AT THE CIVILIAN GRADE OF GS-14/15 OR THE MILITARY RANK OF O-6.

(2) NACI/DNACI/NAC/ENTNAC:

(A) FAVORABLE: A COMPLETELY FAVORABLE INVESTIGATION MAY BE FINALLY ADJUDICATED AFTER ONE LEVEL OF REVIEW PROVIDED THAT THE DECISION MAKING AUTHORITY IS AT THE CIVILIAN GRADE OF GS-5/7 OR THE MILITARY RANK OF O-2.

(B) UNFAVORABLE: INVESTIGATIONS THAT ARE NOT COMPLETELY FAVORABLE MUST BE REVIEWED BY AN ADJUDICATIVE OFFICIAL IN THE CIVILIAN GRADE OF GS-7/9 OR THE MILITARY RANK OF O-3. WHEN AN UNFAVORABLE ADMINISTRATIVE ACTION IS CONTEMPLATED UNDER PARAGRAPH 8-201, THE LETTER OF INTENT TO DENY/REVOKE MUST BE SIGNED BY AN ADJUDICATIVE OFFICIAL AT THE CIVILIAN GRADE OF GS-11/12 OR THE MILITARY RANK OF O-4. A FINAL NOTIFICATION OF UNFAVORABLE ADMINISTRATIVE ACTION SUBSEQUENT TO THE ISSUANCE OF THE LOI MUST BE SIGNED BY AN ADJUDICATIVE OFFICIAL AT THE CIVILIAN GRADE OF GS-13 OR THE MILITARY RANK OF O-5 OR ABOVE.

C. EXCEPTIONS TO THE ABOVE POLICY MAY ONLY BE GRANTED BY THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY.

6-102 EVALUATION OF PERSONNEL SECURITY INFORMATION

A. THE CRITERIA AND ADJUDICATIVE POLICY TO BE USED IN APPLYING THE PRINCIPLES AT PARAGRAPH 6-100, ABOVE, ARE SET FORTH IN PARAGRAPH 2-200 AND APPENDIX I OF THIS REGULATION. THE ULTIMATE CONSIDERATION IN MAKING A FAVORABLE PERSONNEL SECURITY DETERMINATION IS WHETHER SUCH DETERMINATION IS CLEARLY CONSISTENT WITH THE INTERESTS OF NATIONAL SECURITY AND SHALL BE AN OVERALL COMMON SENSE EVALUATION BASED ON ALL AVAILABLE INFORMATION. SUCH A DETERMINATION SHALL INCLUDE CONSIDERATION OF THE FOLLOWING FACTORS:

- (1) THE NATURE AND SERIOUSNESS OF THE CONDUCT;
- (2) THE CIRCUMSTANCES SURROUNDING THE CONDUCT;
- (3) THE FREQUENCY AND REGENCY OF THE CONDUCT;
- (4) THE AGE OF THE INDIVIDUAL;
- (5) THE VOLUNTARINESS OF PARTICIPATION; AND
- (6) THE ABSENCE OR PRESENCE OF REHABILITATION.

B. DETAILED ADJUDICATION POLICY GUIDANCE TO ASSIST ADJUDICATORS IN DETERMINING WHETHER A PERSON IS ELIGIBLE FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES IS CONTAINED IN APPENDIX I. ADJUDICATION POLICY FOR ACCESS TO SCI IS CONTAINED IN DCID 1/14.

6-103 ADJUDICATIVE RECORD

A. EACH ADJUDICATIVE DETERMINATION, WHETHER FAVORABLE OR UNFAVORABLE, SHALL BE ENTERED INTO THE DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII) ON A DAILY BASIS, BUT IN NO CASE TO EXCEED 5 WORKING DAYS FROM THE DATE OF DETERMINATION. [CH2, DoD 5200.2-R, 7/14/93] The WHS CAF and the DIA CCF make the required entries in the DCII for DCAA personnel security determinations and clearances.

B. THE RATIONALE UNDERLYING EACH UNFAVORABLE PERSONNEL SECURITY DETERMINATION, TO INCLUDE THE APPEAL PROCESS, AND EACH FAVORABLE PERSONNEL SECURITY DETERMINATION WHERE THE INVESTIGATION OR INFORMATION UPON WHICH THE DETERMINATION WAS MADE INCLUDED SIGNIFICANT DEROGATORY INFORMATION OF THE TYPE SET FORTH IN PARAGRAPH 2-200 AND APPENDIX I OF THIS REGULATION, SHALL BE MAINTAINED IN WRITTEN OR AUTOMATED FORM AND IS SUBJECT TO THE PROVISIONS OF DOD DIRECTIVES 5400.7 (REFERENCE (AA)) AND 5400.11 (REFERENCE (BB)). THIS INFORMATION SHALL BE MAINTAINED FOR A MINIMUM OF 5 YEARS FROM THE DATE OF DETERMINATION. [CH2, DoD 5200.2-R, 7/14/93]

C. Headquarters security specialists will enter investigations and access status of each employee in the DCAA SIS CENTS for use within DCAA.

CHAPTER VII

ISSUING CLEARANCE AND GRANTING ACCESS

7-100 GENERAL

A. THE ISSUANCE OF A PERSONNEL SECURITY CLEARANCE (AS WELL AS THE FUNCTION OF DETERMINING THAT AN INDIVIDUAL IS ELIGIBLE FOR ACCESS TO SPECIAL ACCESS PROGRAM INFORMATION, OR IS SUITABLE FOR ASSIGNMENT TO SENSITIVE DUTIES OR SUCH OTHER DUTIES THAT REQUIRE A TRUSTWORTHINESS DETERMINATION) IS A FUNCTION DISTINCT FROM THAT INVOLVING THE GRANTING OF ACCESS TO CLASSIFIED INFORMATION. CLEARANCE DETERMINATIONS ARE MADE ON THE MERITS OF THE INDIVIDUAL CASE WITH RESPECT TO THE SUBJECT'S SUITABILITY FOR SECURITY CLEARANCE. ACCESS DETERMINATIONS ARE MADE SOLELY ON THE BASIS OF THE INDIVIDUAL'S NEED FOR ACCESS TO CLASSIFIED INFORMATION IN ORDER TO PERFORM OFFICIAL DUTIES. EXCEPT FOR SUSPENSION OF ACCESS PENDING FINAL ADJUDICATION OF A PERSONNEL SECURITY CLEARANCE, ACCESS MAY NOT BE FINALLY DENIED FOR CAUSE WITHOUT APPLYING THE PROVISIONS OF PARAGRAPH 8-102. Clearances will be approved on an individual basis and only after the need has been fully justified. A security clearance will not be used as a "status symbol," and no Agency employee is entitled to hold a security clearance solely on the basis of grade or position.

B. ONLY THE AUTHORITIES DESIGNATED IN PARAGRAPH A, APPENDIX F ARE AUTHORIZED TO GRANT, DENY OR REVOKE PERSONNEL SECURITY CLEARANCES OR SPECIAL ACCESS AUTHORIZATIONS (OTHER THAN SCI). ANY COMMANDER OR HEAD OF AN ORGANIZATION MAY SUSPEND ACCESS FOR CAUSE WHEN THERE EXISTS INFORMATION RAISING A SERIOUS QUESTION AS TO THE INDIVIDUAL'S ABILITY OR INTENT TO PROTECT CLASSIFIED INFORMATION, PROVIDED THAT THE PROCEDURES SET FORTH IN PARAGRAPH 8-102 OF THIS REGULATION ARE COMPLIED WITH. The WHS CAF (for collateral) and the DIA CCF (for SCI) are the authorities designated to grant, deny, or revoke personnel security clearances for DCAA personnel. Heads of principal staff elements, the Director of Field Detachment, regional directors, and the ASO may suspend access in accordance with the provisions of this paragraph and paragraph 8-102. In the absence of mitigating circumstances, the above authorities shall suspend access to classified information when an employee with a security clearance has:

1. Deliberately disclosed classified information to any unauthorized person; or
2. Committed two security violations within a one year period, one of which resulted in loss or compromise of classified information.

In these circumstances, a HPSE, RD or Director of Field Detachment taking the action will immediately notify the ASO of any suspension of access, and the ASO will request review and action by the WHS CAF or the DIA CCF, as appropriate.

C. ALL COMMANDERS AND HEADS OF DOD ORGANIZATIONS HAVE THE RESPONSIBILITY FOR DETERMINING THOSE POSITION FUNCTIONS IN THEIR JURISDICTION THAT REQUIRE ACCESS TO CLASSIFIED INFORMATION AND THE AUTHORITY TO GRANT ACCESS TO INCUMBENTS OF SUCH POSITIONS WHO HAVE BEEN CLEARED UNDER THE PROVISIONS OF THIS REGULATION. At all times, the levels and numbers of clearances will be restricted to the absolute minimum necessary to accomplish assigned missions. Even if an employee is eligible for a higher level of clearance, that individual will only be granted the level of access required to perform assigned duties.

7-101 ISSUING CLEARANCE

A. AUTHORITIES DESIGNATED IN PARAGRAPH A, APPENDIX F SHALL RECORD THE ISSUANCE, DENIAL, OR REVOCATION OF A PERSONNEL SECURITY CLEARANCE IN THE DCII (SEE PARAGRAPH 6-103, ABOVE). A RECORD OF THE CLEARANCE ISSUED SHALL ALSO BE RECORDED IN AN INDIVIDUAL'S PERSONNEL/SECURITY FILE OR OFFICIAL PERSONNEL FOLDER, AS APPROPRIATE. DCAA Form 5210-31 will be used by Headquarters, Field Detachment, FAO, and regional authorized personnel to request, specify duration of, and justify clearances. A SF 312 will be completed, or verified, and if completed, filed on the right side of the employee's official personnel folder. The WES CAF issues collateral clearances for DCAA personnel on SD Form 176, and the DIA CCF issues DIA Form 1557A for DCAA personnel requiring access to Top Secret and SCI, upon receipt of request from CPS. C/E Certs will be used by the ASO to grant access, and to document the individual's OPF, after ensuring that:

1. There is an unquestioned need for such clearance to allow an individual to perform assigned duties.
2. The individual has met all investigative requirements.
3. There is a valid classified information nondisclosure agreement.
4. U.S. citizenship has been verified and recorded on DCAA Form 5210-48.

If immediate access is necessary, access authority can be arranged by telephone between CPS and the RSO concerned. The ASO will immediately notify the WES CAF of access requirements and issue a C/E Cert so that the action will be formalized and documented properly. The RSO will include the details of the telephonic approval of the clearance on DCAA Form 5210-31 for immediate transmission to CPS. If access is for a short duration, the date(s) access is required will be recorded on the DCAA Form 5210-31 and no C/E Cert will be issued.

A DCAA Form 5210-31 does not have to be completed for SAP nominees if a proof of citizenship has been verified and there is a valid Classified Information Nondisclosure Agreement on file. In these cases, CPS will issue the C/E Cert after coordination with the SAP liaison officer and forward the certificate to the appropriate region.

C/E Certs are prepared and signed in CPS. Certificates are transmitted from there to the appropriate destination. Should a copy of the C/E Cert (formerly DCAA Form 5210-1, DCAA Form 5210-5, and DCAA Form 5210-6) be required because of the inability to locate, the RSO will reproduce, certify, and date a true copy. Initial distribution of the form is as follows:

- Original - Official Personnel Folder
- 1 Copy - Regional or Field Detachment Security Office,
as appropriate
- 1 Copy - Assigned Field Audit Office
- 1 Copy - Agency Security Office (CPS)

B. A PERSONNEL SECURITY CLEARANCE REMAINS VALID UNTIL (1) THE INDIVIDUAL IS SEPARATED FROM THE ARMED FORCES, (2) SEPARATED FROM DOD CIVILIAN EMPLOYMENT,

(3) HAS NO FURTHER OFFICIAL RELATIONSHIP WITH DOD, (4) OFFICIAL ACTION HAS BEEN TAKEN TO DENY, REVOKE OR SUSPEND THE CLEARANCE OR ACCESS, OR (5) REGULAR ACCESS TO THE LEVEL OF CLASSIFIED INFORMATION FOR WHICH THE INDIVIDUAL HOLDS A CLEARANCE IS NO LONGER NECESSARY IN THE NORMAL COURSE OF HIS OR HER DUTIES. IF AN INDIVIDUAL RESUMES THE ORIGINAL STATUS OF (1), (2), (3), OR (5) ABOVE, NO SINGLE BREAK IN THE INDIVIDUAL'S RELATIONSHIP WITH DOD EXISTS GREATER THAN 24 MONTHS, AND/OR THE NEED FOR REGULAR ACCESS TO CLASSIFIED INFORMATION AT OR BELOW THE PREVIOUS LEVEL RECURS, THE APPROPRIATE CLEARANCE SHALL BE REISSUED WITHOUT FURTHER INVESTIGATION OR ADJUDICATION PROVIDED THERE HAS BEEN NO ADDITIONAL INVESTIGATION OR DEVELOPMENT OF DEROGATORY INFORMATION. If an employee who has a security clearance separates from DCAA under (2) of this paragraph, security specialists will ensure compliance with section 10-105.a(i), DCAA Manual 5205.1 (reference 1-100.g) and Chapter 53, DCAA Manual 1400.1 (reference 1-100.r). If a cleared employee no longer has need for regular access under (5) of this paragraph, security specialists will ensure compliance with section 10-105.a(ii)-(iv), DCAA Manual 5205.1.

C. PERSONNEL SECURITY CLEARANCES OF DOD MILITARY PERSONNEL SHALL BE GRANTED, DENIED, OR REVOKED ONLY BY THE DESIGNATED AUTHORITY OF THE PARENT MILITARY DEPARTMENT. ISSUANCE, REISSUANCE, DENIAL, OR REVOCATION OF A PERSONNEL SECURITY CLEARANCE BY ANY DOD COMPONENT CONCERNING PERSONNEL WHO HAVE BEEN DETERMINED TO BE ELIGIBLE FOR CLEARANCE BY ANOTHER COMPONENT IS EXPRESSLY PROHIBITED. INVESTIGATIONS CONDUCTED ON ARMY, NAVY, AND AIR FORCE PERSONNEL BY DIS WILL BE RETURNED ONLY TO THE PARENT SERVICE OF THE SUBJECT FOR ADJUDICATION REGARDLESS OF THE SOURCE OF THE ORIGINAL REQUEST. THE ADJUDICATIVE AUTHORITY WILL BE RESPONSIBLE FOR EXPEDITIOUSLY TRANSMITTING THE RESULTS OF THE CLEARANCE DETERMINATION. AS AN EXCEPTION, THE EMPLOYING DOD COMPONENT MAY ISSUE AN INTERIM CLEARANCE TO PERSONNEL UNDER THEIR ADMINISTRATIVE JURISDICTION PENDING A FINAL ELIGIBILITY DETERMINATION BY THE INDIVIDUAL'S PARENT COMPONENT. WHENEVER AN EMPLOYING DOD COMPONENT ISSUES AN INTERIM CLEARANCE TO AN INDIVIDUAL FROM ANOTHER COMPONENT, WRITTEN NOTICE OF THE ACTION SHALL BE PROVIDED TO THE PARENT COMPONENT.

D. WHEN AN SSBI (OR PR) FOR ACCESS TO SCI IS INITIATED ON A MILITARY MEMBER, WHO IS ASSIGNED TO A DEFENSE AGENCY (EXCEPT DIA), OSD STAFF, OR THE JOINT STAFF, DIS WILL RETURN THE COMPLETED INVESTIGATION TO THE APPROPRIATE MILITARY DEPARTMENT CAF, IN ACCORDANCE WITH SUBSECTION 7-101.C., ABOVE, FOR ISSUANCE (OR REISSUANCE) OF THE SCI ELIGIBILITY. THE CAF SHALL BE RESPONSIBLE FOR EXPEDITIOUSLY TRANSMITTING THE RESULTS OF THE SCI ELIGIBILITY DETERMINATION TO THE REQUESTING DEFENSE AGENCY. FOR MILITARY PERSONNEL ASSIGNED TO THE DIA, THE COMPLETED INVESTIGATION WILL BE FORWARDED TO THE DIA FOR THE SCI ELIGIBILITY DETERMINATION. THE DIA WILL EXPEDITIOUSLY TRANSMIT THE RESULTS OF THE SCI ELIGIBILITY DETERMINATION TO THE APPROPRIATE MILITARY DEPARTMENT CAF.

E. WHEN THE DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE (DISCO) INITIATES AN SSBI (OR PR) FOR ACCESS TO SCI ON A CONTRACTOR EMPLOYEE, DIS WILL RETURN THE COMPLETED INVESTIGATION TO THE APPROPRIATE CAF WITH SCI COGNIZANCE. FOLLOWING A FAVORABLE SCI ELIGIBILITY DETERMINATION, THE CAF WILL NOTIFY DISCO OF THE OUTCOME. IF THE SCI ELIGIBILITY IS DENIED OR REVOKED, THE CAF WILL COMPLETE ALL APPROPRIATE DUE PROCESS AND APPEAL PROCEDURES BEFORE FORWARDING THE CASE AND ALL RELEVANT ADDITIONAL DOCUMENTATION TO DISCO FOR APPROPRIATE ACTION, TO INCLUDE REFERRAL TO THE DEFENSE OFFICE OF HEARINGS AND APPEALS (DOHA) FOR POSSIBLE ACTION UNDER DOD DIRECTIVE 5220.6 (REFERENCE (C)).

F. THE INTERIM CLEARANCE SHALL BE RECORDED IN THE DCII (PARAGRAPH 6-103, ABOVE) BY THE PARENT DOD COMPONENT IN THE SAME MANNER AS A FINAL CLEARANCE.

7-102 GRANTING ACCESS

A. ACCESS TO CLASSIFIED INFORMATION SHALL BE GRANTED TO PERSONS WHOSE OFFICIAL DUTIES REQUIRE SUCH ACCESS AND WHO HAVE THE APPROPRIATE PERSONNEL SECURITY CLEARANCE. ACCESS DETERMINATIONS (OTHER THAN FOR SPECIAL ACCESS PROGRAMS) ARE NOT AN ADJUDICATIVE FUNCTION RELATING TO AN INDIVIDUAL'S SUITABILITY FOR SUCH ACCESS. RATHER THEY ARE DECISIONS MADE BY THE COMMANDER THAT ACCESS IS OFFICIALLY REQUIRED.

B. IN THE ABSENCE OF DEROGATORY INFORMATION ON THE INDIVIDUAL CONCERNED, DOD COMMANDERS AND ORGANIZATIONAL MANAGERS SHALL ACCEPT A PERSONNEL SECURITY CLEARANCE DETERMINATION, ISSUED BY ANY DOD AUTHORITY AUTHORIZED BY THIS REGULATION TO ISSUE PERSONNEL SECURITY CLEARANCE, AS THE BASIS FOR GRANTING ACCESS, WHEN ACCESS IS REQUIRED, WITHOUT REQUESTING ADDITIONAL INVESTIGATION OR INVESTIGATIVE FILES.

C. THE ACCESS LEVEL OF CLEARED INDIVIDUALS WILL, WHEREVER POSSIBLE, BE ENTERED INTO THE DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII), ALONG WITH CLEARANCE ELIGIBILITY. HOWEVER, COMPLETION OF THE DCII ACCESS FIELD IS REQUIRED EFFECTIVE 1 OCTOBER 1993 IN ALL INSTANCES WHERE THE ADJUDICATOR IS REASONABLY AWARE OF THE LEVEL OF CLASSIFIED ACCESS ASSOCIATED WITH A PERSONNEL SECURITY INVESTIGATION. AGENCIES ARE ENCOURAGED TO START COMPLETING THIS FIELD AS SOON AS POSSIBLE.

7-103 ADMINISTRATIVE WITHDRAWAL

AS SET FORTH IN PARAGRAPH 7-101.B., ABOVE, THE PERSONNEL SECURITY CLEARANCE AND ACCESS ELIGIBILITY MUST BE WITHDRAWN WHEN THE EVENTS DESCRIBED THEREIN OCCUR. WHEN REGULAR ACCESS TO A PRESCRIBED LEVEL OF CLASSIFIED INFORMATION IS NO LONGER REQUIRED IN THE NORMAL COURSE OF AN INDIVIDUAL'S DUTIES, THE PREVIOUSLY AUTHORIZED ACCESS ELIGIBILITY LEVEL MUST BE ADMINISTRATIVELY DOWNGRADED OR WITHDRAWN, AS APPROPRIATE. When an employee no longer requires access, CPS will be notified to administratively withdraw the clearance in accordance with this paragraph, and section 10-105.a(iv), DCAA Manual 5205.1 (reference 1-100.g). Section 7, Enclosure 3, provides disposition instructions for access and eligibility certificates on employees transferring within DCAA offices.

CHAPTER VIII

UNFAVORABLE ADMINISTRATIVE ACTIONS

Section 1

REQUIREMENTS

8-100 GENERAL

FOR PURPOSES OF THIS REGULATION, AN UNFAVORABLE ADMINISTRATIVE ACTION INCLUDES ANY ADVERSE ACTION WHICH IS TAKEN AS A RESULT OF A PERSONNEL SECURITY DETERMINATION, AS DEFINED AT PARAGRAPH 1-301, AND ANY UNFAVORABLE PERSONNEL SECURITY DETERMINATION, AS DEFINED AT PARAGRAPH 1-328. THIS CHAPTER IS INTENDED ONLY TO PROVIDE GUIDANCE FOR THE INTERNAL OPERATION OF THE DEPARTMENT OF DEFENSE AND IS NOT INTENDED TO, DOES NOT, AND MAY NOT BE RELIED UPON, TO CREATE OR ENLARGE THE JURISDICTION OR REVIEW AUTHORITY OF ANY COURT OR ADMINISTRATIVE TRIBUNAL, INCLUDING THE MERIT SYSTEMS PROTECTION BOARD.

8-101 REFERRAL FOR ACTION

A. WHENEVER DEROGATORY INFORMATION RELATED TO THE CRITERIA AND POLICY SET FORTH IN PARAGRAPH 2-200 AND APPENDIX I OF THIS REGULATION IS DEVELOPED OR OTHERWISE BECOMES AVAILABLE TO ANY DOD ELEMENT, IT SHALL BE REFERRED BY THE MOST EXPEDITIOUS MEANS TO THE COMMANDER OR THE SECURITY OFFICER OF THE ORGANIZATION TO WHICH THE INDIVIDUAL IS ASSIGNED FOR DUTY. THE COMMANDER OR SECURITY OFFICER OF THE ORGANIZATION TO WHICH THE SUBJECT OF THE INFORMATION IS ASSIGNED SHALL REVIEW THE INFORMATION IN TERMS OF ITS SECURITY SIGNIFICANCE AND COMPLETENESS. IF FURTHER INFORMATION IS NEEDED TO CONFIRM OR DISPROVE THE ALLEGATIONS, ADDITIONAL INVESTIGATION SHOULD BE REQUESTED. THE COMMANDER OF THE DUTY ORGANIZATION SHALL INSURE THAT THE APPROPRIATE CENTRAL ADJUDICATIVE FACILITY (CAF) OF THE INDIVIDUAL CONCERNED IS INFORMED PROMPTLY CONCERNING (1) THE DEROGATORY INFORMATION DEVELOPED AND (2) ANY ACTIONS TAKEN OR ANTICIPATED WITH RESPECT THERETO. HOWEVER, REFERRAL OF DEROGATORY INFORMATION TO THE COMMANDER OR SECURITY OFFICER SHALL IN NO WAY AFFECT OR LIMIT THE RESPONSIBILITY OF THE CAF TO CONTINUE TO PROCESS THE INDIVIDUAL FOR DENIAL OR REVOCATION OF CLEARANCE OR ACCESS TO CLASSIFIED INFORMATION, IN ACCORDANCE WITH PARAGRAPH 8-201, BELOW, IF SUCH ACTION IS WARRANTED AND SUPPORTABLE BY THE CRITERIA AND POLICY CONTAINED IN PARAGRAPH 2-200 AND APPENDIX I. NO UNFAVORABLE ADMINISTRATIVE ACTION AS DEFINED IN PARAGRAPH 1-327 AND 328 MAY BE TAKEN BY THE ORGANIZATION TO WHICH THE INDIVIDUAL IS ASSIGNED FOR DUTY WITHOUT AFFORDING THE PERSON THE FULL RANGE OF PROTECTIONS CONTAINED IN PARAGRAPH 8-201, BELOW, OR, IN THE CASE OF SCI, ANNEX B, DCID 1/14 (REFERENCE (L)).

DCAA managers are responsible for reporting derogatory information received on employees. Any information relating to the criteria in paragraph 2-200 and Appendix I, (which includes arrests, drug abuse, alcohol abuse, financial difficulties, etc.) should be reported without delay to the RSO, FDSO, or the ASO. The RSO and FDSO should notify the ASO immediately upon receipt of the information, evaluate the information to determine if additional inquiries or security investigation is required, and if so, initiate action as required. The security specialist responsible for Headquarters employees will initiate action as needed for Headquarters (including TSC and DCAI) employees.

B. THE DIRECTOR DIS SHALL ESTABLISH APPROPRIATE ALTERNATIVE MEANS WHEREBY INFORMATION WITH POTENTIALLY SERIOUS SECURITY SIGNIFICANCE CAN BE REPORTED OTHER THAN THROUGH DOD COMMAND OR INDUSTRIAL ORGANIZATION CHANNELS. SUCH ACCESS SHALL INCLUDE UTILIZATION OF THE DOD INSPECTOR GENERAL "HOTLINE" TO RECEIVE SUCH REPORTS FOR APPROPRIATE FOLLOW-UP BY DIS. DOD COMPONENTS AND INDUSTRY WILL ASSIST DIS IN PUBLICIZING THE AVAILABILITY OF APPROPRIATE REPORTING CHANNELS. ADDITIONALLY, DOD COMPONENTS WILL AUGMENT THE SYSTEM WHEN AND WHERE NECESSARY. HEADS OF DOD COMPONENTS WILL BE NOTIFIED IMMEDIATELY TO TAKE ACTION IF APPROPRIATE.

8-102 SUSPENSION

A. THE COMMANDER OR HEAD OF THE ORGANIZATION SHALL DETERMINE WHETHER, ON THE BASIS OF ALL FACTS AVAILABLE UPON RECEIPT OF THE INITIAL DEROGATORY INFORMATION, IT IS IN THE INTERESTS OF NATIONAL SECURITY TO CONTINUE SUBJECT'S SECURITY STATUS UNCHANGED OR TO TAKE INTERIM ACTION TO SUSPEND SUBJECT'S ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES (OR OTHER DUTIES REQUIRING A TRUSTWORTHINESS DETERMINATION), IF INFORMATION EXISTS WHICH RAISES SERIOUS QUESTIONS AS TO THE INDIVIDUAL'S ABILITY OR INTENT TO PROTECT CLASSIFIED INFORMATION OR EXECUTE SENSITIVE DUTIES (OR OTHER DUTIES REQUIRING A TRUSTWORTHINESS DETERMINATION) UNTIL A FINAL DETERMINATION IS MADE BY THE APPROPRIATE AUTHORITY DESIGNATED IN APPENDIX F.

B. WHENEVER A DETERMINATION IS MADE TO SUSPEND A SECURITY CLEARANCE FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES (OR OTHER DUTIES REQUIRING A TRUSTWORTHINESS DETERMINATION), THE INDIVIDUAL CONCERNED MUST BE NOTIFIED OF THE DETERMINATION IN WRITING BY THE COMMANDER, OR COMPONENT CAF, TO INCLUDE A BRIEF STATEMENT OF THE REASON(S) FOR THE SUSPENSION ACTION CONSISTENT WITH THE INTERESTS OF NATIONAL SECURITY.

C. COMPONENT FIELD ELEMENTS MUST PROMPTLY REPORT ALL SUSPENSION ACTIONS TO THE APPROPRIATE CAF, BUT NOT LATER THAN 10 WORKING DAYS FROM THE DATE OF THE SUSPENSION ACTION. THE ADJUDICATIVE AUTHORITY WILL IMMEDIATELY UPDATE THE DCII ELIGIBILITY AND ACCESS FIELDS TO ALERT ALL USERS TO THE INDIVIDUAL'S CHANGED STATUS.

D. EVERY EFFORT SHALL BE MADE TO RESOLVE SUSPENSION CASES AS EXPEDITIOUSLY AS CIRCUMSTANCES PERMIT. SUSPENSION CASES EXCEEDING 180 DAYS SHALL BE CLOSELY MONITORED AND MANAGED BY THE DOD COMPONENT CONCERNED UNTIL FINALLY RESOLVED. SUSPENSION CASES PENDING IN EXCESS OF 12 MONTHS WILL BE REPORTED TO THE DASD(I&S) FOR REVIEW AND APPROPRIATE ACTION.

E. A FINAL SECURITY CLEARANCE ELIGIBILITY DETERMINATION SHALL BE MADE FOR ALL SUSPENSION ACTIONS AND THE DETERMINATION ENTERED IN THE DCII. IF, HOWEVER, THE INDIVIDUAL UNDER SUSPENSION LEAVES THE JURISDICTION OF THE DEPARTMENT OF DEFENSE AND NO LONGER REQUIRES A CLEARANCE (OR TRUSTWORTHINESS DETERMINATION), ENTRY OF THE "2" CODE (ADJUDICATION ACTION INCOMPLETE DUE TO LOSS OF JURISDICTION) IN THE CLEARANCE ELIGIBILITY FIELD IS APPROPRIATE. IN NO CASE SHALL A "SUSPENSION" CODE (CODE Y) REMAIN AS A PERMANENT RECORD IN THE DCII.

F. A CLEARANCE OR ACCESS ENTRY IN THE DCII SHALL NOT BE SUSPENDED OR DOWNGRADED BASED SOLELY ON THE FACT THAT A PERIODIC REINVESTIGATION WAS NOT CONDUCTED PRECISELY WITHIN THE 5-YEAR TIME PERIOD FOR TOP SECRET/SCI OR WITHIN THE PERIOD PREVAILING FOR SECRET CLEARANCES UNDER DEPARTMENTAL POLICY. WHILE

EVERY EFFORT SHOULD BE MADE TO ENSURE THAT PRs ARE CONDUCTED WITHIN THE PRESCRIBED TIMEFRAME, AGENCIES MUST BE FLEXIBLE IN THEIR ADMINISTRATION OF THIS ASPECT OF THE PERSONNEL SECURITY PROGRAM SO AS NOT TO UNDERMINE THE ABILITY OF THE DEPARTMENT OF DEFENSE TO ACCOMPLISH ITS MISSION. [CH2 to DoD 5200.2-R, 7/14/93]

8-103 FINAL UNFAVORABLE ADMINISTRATIVE ACTIONS

THE AUTHORITY TO MAKE PERSONNEL SECURITY DETERMINATIONS THAT WILL RESULT IN AN UNFAVORABLE ADMINISTRATIVE ACTION IS LIMITED TO THOSE AUTHORITIES DESIGNATED IN APPENDIX F, EXCEPT THAT THE AUTHORITY TO TERMINATE THE EMPLOYMENT OF A CIVILIAN EMPLOYEE OF A MILITARY DEPARTMENT OR DEFENSE AGENCY IS VESTED SOLELY IN THE HEAD OF THE DOD COMPONENT CONCERNED AND IN SUCH OTHER STATUTORY OFFICIAL AS MAY BE DESIGNATED. ACTION TO TERMINATE CIVILIAN EMPLOYEES OF THE OFFICE OF THE SECRETARY OF DEFENSE AND DOD COMPONENTS, ON THE BASIS OF CRITERIA LISTED IN PARAGRAPH 2-200, A THROUGH F, SHALL BE COORDINATED WITH THE OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE OASD(C3I) PRIOR TO FINAL ACTION BY THE HEAD OF THE DOD COMPONENT. DOD CIVILIAN EMPLOYEES OR MEMBERS OF THE ARMED FORCES SHALL NOT BE REMOVED FROM EMPLOYMENT OR SEPARATED FROM THE SERVICE UNDER PROVISIONS OF THIS REGULATION IF REMOVAL OR SEPARATION CAN BE EFFECTED UNDER OPM REGULATIONS OR ADMINISTRATIVE (NONSECURITY) REGULATIONS OF THE MILITARY DEPARTMENTS. HOWEVER, ACTIONS CONTEMPLATED IN THIS REGARD SHALL NOT AFFECT OR LIMIT THE RESPONSIBILITY OF THE CAF TO CONTINUE TO PROCESS THE INDIVIDUAL FOR DENIAL OR REVOCATION OF A SECURITY CLEARANCE, ACCESS TO CLASSIFIED INFORMATION, OR ASSIGNMENT TO A SENSITIVE POSITION IF WARRANTED AND SUPPORTABLE BY THE CRITERIA AND STANDARDS CONTAINED IN THIS REGULATION. The WHS CAF and the DIA CCF are the authorities to make personnel security determinations for DCAA personnel.

Section 2

PROCEDURES

8-200 GENERAL

NO FINAL UNFAVORABLE PERSONNEL SECURITY CLEARANCE OR ACCESS DETERMINATION SHALL BE MADE ON A MEMBER OF THE ARMED FORCES, AN EMPLOYEE OF THE DEPARTMENT OF DEFENSE, A CONSULTANT TO THE DEPARTMENT OF DEFENSE, OR ANY OTHER PERSON AFFILIATED WITH THE DEPARTMENT OF DEFENSE WITHOUT GRANTING THE INDIVIDUAL CONCERNED THE PROCEDURAL BENEFITS SET FORTH IN 8-201 BELOW, WHEN SUCH DETERMINATION RESULTS IN AN UNFAVORABLE ADMINISTRATIVE ACTION (SEE PARAGRAPH 8-100). AS AN EXCEPTION, DOD CONTRACTOR PERSONNEL SHALL BE AFFORDED THE PROCEDURES CONTAINED IN DOD DIRECTIVE 5220.6 (REFERENCE (C)) AND RED CROSS/UNITED SERVICE ORGANIZATIONS EMPLOYEES SHALL BE AFFORDED THE PROCEDURES PRESCRIBED BY DOD DIRECTIVE 5210.25 (REFERENCE (W)). PROCEDURES FOR UNFAVORABLE DECISIONS REGARDING ACCESS TO SAPs MAY DIFFER FROM THE PROCEDURES IN THIS REGULATION AS AUTHORIZED IN E.O. 12968 AND AS APPROVED BY THE SECRETARY OF DEFENSE OR DEPUTY SECRETARY OF DEFENSE.

8-201 UNFAVORABLE ADMINISTRATIVE ACTION PROCEDURES

EXCEPT AS PROVIDED FOR BELOW, NO UNFAVORABLE ADMINISTRATIVE ACTION SHALL BE TAKEN UNDER THE AUTHORITY OF THIS REGULATION UNLESS THE INDIVIDUAL CONCERNED HAS BEEN:

A. PROVIDED A WRITTEN STATEMENT OF THE REASONS (SOR) AS TO WHY THE UNFAVORABLE ADMINISTRATIVE ACTION IS BEING TAKEN IN ACCORDANCE WITH THE EXAMPLE AT APPENDIX L, WHICH INCLUDES SAMPLE LETTERS AND ENCLOSURES. THE SOR SHALL BE AS COMPREHENSIVE AND DETAILED AS THE PROTECTION OF SOURCES AFFORDED CONFIDENTIALITY UNDER PROVISIONS OF THE PRIVACY ACT OF 1974 (REFERENCE (M)) AND NATIONAL SECURITY PERMIT. THE STATEMENT WILL CONTAIN, 1) A SUMMARY OF THE SECURITY CONCERNS AND SUPPORTING ADVERSE INFORMATION, 2) INSTRUCTIONS FOR RESPONDING TO THE SOR AND 3) COPIES OF THE RELEVANT SECURITY GUIDELINES FROM APPENDIX I. IN ADDITION, THE CAF WILL PROVIDE WITHIN 30 CALENDAR DAYS, UPON REQUEST OF THE INDIVIDUAL, COPIES OF RELEASABLE RECORDS OF THE PERSONNEL SECURITY INVESTIGATION (THE CAF MUST RETAIN COPIES OF THE FILE FOR AT LEAST 90 DAYS TO ENSURE THE READY AVAILABILITY OF THE MATERIAL FOR THE SUBJECT). IF THE CAF IS UNABLE TO PROVIDE REQUESTED DOCUMENTS FOR REASONS BEYOND THEIR CONTROL, THEN THE NAME AND ADDRESS OF THE AGENCY (AGENCIES) TO WHICH THE INDIVIDUAL MAY WRITE TO OBTAIN A COPY OF THE RECORDS WILL BE PROVIDED.

(1) THE HEAD OF THE LOCAL ORGANIZATION OF THE INDIVIDUAL RECEIVING AN SOR SHALL DESIGNATE A POINT OF CONTACT (POC) TO SERVE AS A LIAISON BETWEEN THE CAF AND THE INDIVIDUAL. THE DUTIES OF THE POC WILL INCLUDE, BUT NOT NECESSARILY BE LIMITED TO, DELIVERING THE SOR; HAVING THE INDIVIDUAL ACKNOWLEDGE RECEIPT OF THE SOR; DETERMINING WHETHER THE INDIVIDUAL INTENDS TO RESPOND WITHIN THE TIME SPECIFIED; ENSURING THAT THE INDIVIDUAL UNDERSTANDS THE CONSEQUENCES OF THE PROPOSED ACTION AS WELL AS THE CONSEQUENCES FOR FAILING TO RESPOND IN A TIMELY FASHION; EXPLAINING HOW TO OBTAIN TIME EXTENSIONS, PROCURE COPIES OF INVESTIGATIVE RECORDS, AND THE PROCEDURES FOR RESPONDING TO THE SOR; AND ENSURING THAT THE INDIVIDUAL UNDERSTANDS THAT HE OR SHE CAN OBTAIN LEGAL COUNSEL OR OTHER ASSISTANCE AT HIS OR HER OWN EXPENSE.

(2) Within DCAA, the POC for purposes of implementing this section is the ASO. The DCAA ASO will perform the duties above in coordination with WHS CAF for collateral clearances, and with DIA CCF for SCI accesses.

B. AFFORDED AN OPPORTUNITY TO REPLY IN WRITING TO THE CAF WITHIN 30 CALENDAR DAYS FROM THE DATE OF RECEIPT OF THE SOR. FAILURE TO SUBMIT A TIMELY RESPONSE WILL RESULT IN FORFEITURE OF ALL FUTURE APPEAL RIGHTS WITH REGARD TO THE UNFAVORABLE ADMINISTRATIVE ACTION. EXCEPTIONS TO THIS POLICY MAY ONLY BE GRANTED BY THE CAF IN EXTRAORDINARY CIRCUMSTANCES WHERE THE INDIVIDUAL'S FAILURE TO RESPOND TO THE SOR WAS DUE TO FACTORS BEYOND HIS OR HER CONTROL. THE CAF MUST BE NOTIFIED OF THE INDIVIDUAL'S INTENT TO RESPOND, VIA THE POC, WITHIN 10 CALENDAR DAYS OF RECEIPT OF THE SOR. AN EXTENSION OF UP TO 30 CALENDAR DAYS MAY BE GRANTED BY THE EMPLOYING ORGANIZATION FOLLOWING SUBMISSION OF A WRITTEN REQUEST FROM THE INDIVIDUAL. ADDITIONAL EXTENSIONS MAY ONLY BE GRANTED BY THE CAF. RESPONSES TO THE CAF MUST BE FORWARDED THROUGH THE HEAD OF THE EMPLOYING ORGANIZATION.

C. PROVIDED A WRITTEN RESPONSE BY THE CAF TO ANY SUBMISSION UNDER SUBPARAGRAPH B. STATING THE FINAL REASON(S) FOR THE UNFAVORABLE ADMINISTRATIVE ACTION, WHICH SHALL BE AS SPECIFIC AS PRIVACY AND NATIONAL SECURITY CONSIDERATIONS PERMIT AND IN ACCORDANCE WITH THE EXAMPLE OF A LETTER OF DENIAL (LOD) AND ITS ENCLOSURES AT APPENDIX L. SUCH RESPONSE SHALL BE AS PROMPT AS INDIVIDUAL CIRCUMSTANCES PERMIT, NOT TO EXCEED 60 CALENDAR DAYS FROM THE DATE OF RECEIPT OF THE RESPONSE SUBMITTED UNDER SUBPARAGRAPH B., ABOVE, PROVIDED NO ADDITIONAL INVESTIGATIVE ACTION IS NECESSARY. IF A FINAL RESPONSE CANNOT BE COMPLETED WITHIN THE TIME FRAME ALLOWED, THE INDIVIDUAL MUST BE NOTIFIED IN WRITING OF THIS FACT, THE REASONS THEREFOR, AND THE DATE A FINAL RESPONSE IS

EXPECTED, WHICH SHALL NOT NORMALLY EXCEED A TOTAL OF 90 DAYS FROM THE DATE OF RECEIPT OF THE RESPONSE UNDER SUBPARAGRAPH B.

D. AFFORDED AN OPPORTUNITY TO APPEAL AN LOD, ISSUED PURSUANT TO PARAGRAPH C. ABOVE, TO THE COMPONENT PERSONNEL SECURITY APPEALS BOARD (PSAB). THE PSAB SHALL CONSIST OF A MINIMUM OF THREE MEMBERS AND FUNCTION IN ACCORDANCE WITH APPENDIX M. IF A DECISION IS MADE TO APPEAL THE LOD, THE INDIVIDUAL MAY DO SO BY ONE OF THE FOLLOWING METHODS:

(1) APPEAL WITHOUT A PERSONAL APPEARANCE: ADVISE THE PSAB WITHIN 10 CALENDAR DAYS OF RECEIPT OF THE LOD, OF THE INTENT TO APPEAL. WITHIN 40 CALENDAR DAYS OF RECEIPT OF THE LOD, WRITE TO THE APPROPRIATE PSAB STATING REASONS WHY THE LOD SHOULD BE OVERTURNED AND PROVIDING ANY ADDITIONAL, RELEVANT INFORMATION THAT MAY HAVE A BEARING ON THE FINAL DECISION BY THE PSAB;

(2) APPEAL WITH A PERSONAL APPEARANCE: ADVISE THE DEFENSE OFFICE OF HEARINGS AND APPEALS (DOHA) WITHIN 10 CALENDAR DAYS OF RECEIPT OF THE LOD THAT A PERSONAL APPEARANCE BEFORE A DOHA ADMINISTRATIVE JUDGE (AJ) IS DESIRED IN ORDER TO PROVIDE ADDITIONAL, RELEVANT INFORMATION WHICH MAY HAVE A BEARING ON THE FINAL DECISION BY THE PSAB. DOHA WILL PROMPTLY SCHEDULE A PERSONAL APPEARANCE AND WILL PROVIDE A RECOMMENDATION TO THE PSAB GENERALLY WITHIN 60 DAYS OF RECEIPT OF THE NOTICE REQUESTING THE PERSONAL APPEARANCE. PROCEDURES GOVERNING THE CONDUCT OF THE PERSONAL APPEARANCE BEFORE A DOHA AJ ARE CONTAINED AT APPENDIX N.

E. PROVIDED A FINAL WRITTEN DECISION BY THE PSAB, INCLUDING A RATIONALE, TO ANY SUBMISSION UNDER SUBPARAGRAPH D., ABOVE, STATING THE FINAL DISPOSITION OF THE APPEAL. THIS WILL NORMALLY BE ACCOMPLISHED WITHIN 60 CALENDAR DAYS OF RECEIPT OF THE WRITTEN APPEAL FROM THE INDIVIDUAL IF NO PERSONAL APPEARANCE WAS REQUESTED, OR WITHIN 30 CALENDAR DAYS FROM RECEIPT OF THE AJ'S RECOMMENDATION IF A PERSONAL APPEARANCE WAS REQUESTED.

8-202 DUE PROCESS REVIEW

THE DUE PROCESS AND APPEAL PROCEDURES WILL BE REVIEWED ONE YEAR AFTER IMPLEMENTATION. THE ABOVE PROCEDURES WILL BECOME EFFECTIVE NO LATER THAN 120 DAYS AFTER THE DATE OF THIS CHANGE [CH3 issued 1 Nov 1995].

8-203 EXCEPTIONS TO POLICY

NOTWITHSTANDING PARAGRAPH 8-201 ABOVE OR ANY OTHER PROVISION OF THIS REGULATION, NOTHING IN THIS REGULATION SHALL BE DEEMED TO LIMIT OR AFFECT THE RESPONSIBILITY AND POWERS OF THE SECRETARY OF DEFENSE TO FIND THAT A PERSON IS UNSUITABLE FOR ENTRANCE OR RETENTION IN THE ARMED FORCES, OR IS INELIGIBLE FOR A SECURITY CLEARANCE OR ASSIGNMENT TO SENSITIVE DUTIES, IF THE NATIONAL SECURITY SO REQUIRES, PURSUANT TO SECTION 7532, TITLE 5, UNITED STATES CODE (REFERENCE (PP)). SUCH AUTHORITY MAY NOT BE DELEGATED AND MAY BE EXERCISED ONLY WHEN IT IS DETERMINED THAT THE PROCEDURES PRESCRIBED IN PARAGRAPH 8-201 ABOVE ARE NOT APPROPRIATE. SUCH DETERMINATION SHALL BE CONCLUSIVE.

Section 3

REINSTATEMENT OF CIVILIAN EMPLOYEES

8-300 GENERAL

ANY PERSON WHOSE CIVILIAN EMPLOYMENT IN THE DEPARTMENT OF DEFENSE IS TERMINATED UNDER THE PROVISIONS OF THIS REGULATION SHALL NOT BE REINSTATED OR RESTORED TO DUTY OR REEMPLOYED IN THE DEPARTMENT OF DEFENSE UNLESS THE SECRETARY OF DEFENSE, OR THE HEAD OF A DOD COMPONENT, FINDS THAT SUCH REINSTATEMENT, RESTORATION, OR REEMPLOYMENT IS CLEARLY CONSISTENT WITH THE INTERESTS OF NATIONAL SECURITY. SUCH A FINDING SHALL BE MADE PART OF THE PERSONNEL SECURITY RECORD.

8-301 REINSTATEMENT BENEFITS

A DOD CIVILIAN EMPLOYEE WHOSE EMPLOYMENT HAS BEEN SUSPENDED OR TERMINATED UNDER THE PROVISIONS OF THIS REGULATION AND WHO IS REINSTATED OR RESTORED TO DUTY UNDER THE PROVISIONS OF SECTION 3571 OF TITLE 5, U.S. CODE (REFERENCE (DD)) IS ENTITLED TO BENEFITS AS PROVIDED FOR BY SECTION 3 OF PUBLIC LAW 89-380 (REFERENCE (EE)).

CHAPTER IX

CONTINUING SECURITY RESPONSIBILITIES

Section 1

EVALUATING CONTINUED SECURITY ELIGIBILITY

9-100 GENERAL

A PERSONNEL SECURITY DETERMINATION IS AN EFFORT TO ASSESS THE FUTURE TRUSTWORTHINESS OF AN INDIVIDUAL IN TERMS OF THE LIKELIHOOD OF THE INDIVIDUAL PRESERVING THE NATIONAL SECURITY. OBVIOUSLY IT IS NOT POSSIBLE AT A GIVEN POINT TO ESTABLISH WITH CERTAINTY THAT ANY HUMAN BEING WILL REMAIN TRUSTWORTHY. ACCORDINGLY, THE ISSUANCE OF A PERSONNEL SECURITY CLEARANCE OR THE DETERMINATION THAT A PERSON IS SUITABLE FOR ASSIGNMENT TO SENSITIVE DUTIES CANNOT BE CONSIDERED AS A FINAL PERSONNEL SECURITY ACTION. RATHER, THERE IS THE CLEAR NEED TO ASSURE THAT, AFTER THE PERSONNEL SECURITY DETERMINATION IS REACHED, THE INDIVIDUAL'S TRUSTWORTHINESS IS A MATTER OF CONTINUING ASSESSMENT. THE RESPONSIBILITY FOR SUCH ASSESSMENT MUST BE SHARED BY THE ORGANIZATIONAL COMMANDER OR MANAGER, THE INDIVIDUAL'S SUPERVISOR AND, TO A LARGE DEGREE, THE INDIVIDUAL HIMSELF. THEREFORE, THE HEADS OF DOD COMPONENTS SHALL ESTABLISH AND MAINTAIN A PROGRAM DESIGNED TO EVALUATE ON A CONTINUING BASIS THE STATUS OF PERSONNEL UNDER THEIR JURISDICTION WITH RESPECT TO SECURITY ELIGIBILITY. THIS PROGRAM SHOULD INSURE CLOSE COORDINATION BETWEEN SECURITY AUTHORITIES AND PERSONNEL, MEDICAL, LEGAL AND SUPERVISORY PERSONNEL TO ASSURE THAT ALL PERTINENT INFORMATION AVAILABLE WITHIN A COMMAND IS CONSIDERED IN THE PERSONNEL SECURITY PROCESS. Any evidence of behavior by an employee which is questionable from a security standpoint should be reported immediately by either the employee's supervisor or a knowledgeable individual to the RSO (for regions), the ASO (for Headquarters), or the FDSO (for FD), as appropriate. The RSO or FDSO is responsible for inquiring into the matter, initiating appropriate investigation, and immediately reporting the circumstances in writing to the ASO. The report will include recommendations concerning the employee's suitability and assignment to sensitive duties and/or being entrusted with classified information. In cases, where appropriate, the RSO/FDSO may recommend to the personnel officer that the employee be provided assistance in resolving his/her problem. If the employee has a clearance, the report will also include indication that access has or has not been suspended in accordance with paragraph 8-102 of this manual. In cases involving Headquarters personnel, reports will be made directly to the ASO who will inquire into the matter, initiate appropriate investigation, and/or recommend to the personnel officer that the employee be provided assistance in resolving his/her problem. The information will be forwarded to the WHS CAF or the DIA CCF, as appropriate, by the ASO.

9-101 MANAGEMENT RESPONSIBILITY

A. COMMANDERS AND HEADS OF ORGANIZATIONS SHALL INSURE THAT PERSONNEL ASSIGNED TO SENSITIVE DUTIES (OR OTHER DUTIES REQUIRING A TRUSTWORTHINESS DETERMINATION UNDER THE PROVISIONS OF THIS REGULATION) ARE INITIALLY INDOCTRINATED AND PERIODICALLY INSTRUCTED THEREAFTER ON THE NATIONAL SECURITY IMPLICATION OF THEIR DUTIES AND ON THEIR INDIVIDUAL RESPONSIBILITIES. Heads of principal staff elements, the Director, Field Detachment, and regional directors

are responsible for ensuring that their employees are appropriately briefed in accordance with the requirements of this Chapter.

B. THE HEADS OF ALL DOD COMPONENTS ARE ENCOURAGED TO DEVELOP PROGRAMS DESIGNED TO COUNSEL AND ASSIST EMPLOYEES IN SENSITIVE POSITIONS WHO ARE EXPERIENCING PROBLEMS IN THEIR PERSONAL LIVES WITH RESPECT TO SUCH AREAS AS FINANCIAL, MEDICAL OR EMOTIONAL DIFFICULTIES. SUCH INITIATIVES SHOULD BE DESIGNED TO IDENTIFY POTENTIAL PROBLEM AREAS AT AN EARLY STAGE SO THAT ANY ASSISTANCE RENDERED BY THE EMPLOYING ACTIVITY WILL HAVE A REASONABLE CHANCE OF PRECLUDING LONG TERM, JOB-RELATED SECURITY PROBLEMS. DCAA supervisors should consult Chapter 67, DCAA Manual 1400.1 (reference 1-100.r), for information on the Agency's employee assistance programs. However, employees in sensitive positions who experience personal financial, medical, or emotional problems, or who may become involved in other issues of a type listed in Appendix E must be brought to the attention of the appropriate security official.

9-102 SUPERVISORY RESPONSIBILITY

SECURITY PROGRAMS SHALL BE ESTABLISHED TO INSURE THAT SUPERVISORY PERSONNEL ARE FAMILIARIZED WITH THEIR SPECIAL RESPONSIBILITIES IN MATTERS PERTAINING TO PERSONNEL SECURITY WITH RESPECT TO PERSONNEL UNDER THEIR SUPERVISION. SUCH PROGRAMS SHALL PROVIDE PRACTICAL GUIDANCE AS TO INDICATORS THAT MAY SIGNAL MATTERS OF PERSONNEL SECURITY CONCERN. SPECIFIC INSTRUCTIONS SHOULD BE DISSEMINATED CONCERNING REPORTING PROCEDURES TO ENABLE THE APPROPRIATE AUTHORITY TO TAKE TIMELY CORRECTIVE ACTION TO PROTECT THE INTERESTS OF NATIONAL SECURITY AS WELL AS TO PROVIDE ANY NECESSARY HELP TO THE INDIVIDUAL CONCERNED TO CORRECT ANY PERSONAL PROBLEM WHICH MAY HAVE A BEARING UPON THE INDIVIDUAL'S CONTINUED ELIGIBILITY FOR ACCESS.

A. IN CONJUNCTION WITH THE SUBMISSION OF PRs STATED IN SECTION 7, CHAPTER III, AND PARAGRAPH 5, APPENDIX B, SUPERVISORS WILL BE REQUIRED TO REVIEW AN INDIVIDUAL'S DD FORM 398 TO ENSURE THAT NO SIGNIFICANT ADVERSE INFORMATION OF WHICH THEY ARE AWARE AND THAT MAY HAVE A BEARING ON SUBJECT'S CONTINUED ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION IS OMITTED. The requirement in paragraph 9-102.A, for supervisors to review an individual's DD Form 398 in conjunction with the conduct of periodic reinvestigations was superseded by OASD(C3I) memorandum dated 9 June 1992. The required supervisory statement was incorporated as Item 20, DD Form 398 because concerns had been expressed over sharing personal information. The intent of the change was to preserve the privacy of the subject of investigation. Security specialists will forward the certificate (Item 20, DD Form 1879) to the supervisor for completion and return.

B. IF THE SUPERVISOR IS NOT AWARE OF ANY SIGNIFICANT ADVERSE INFORMATION THAT MAY HAVE A BEARING ON THE SUBJECT'S CONTINUED ELIGIBILITY FOR ACCESS, THEN THE FOLLOWING STATEMENT MUST BE DOCUMENTED, SIGNED AND DATED, AND FORWARDED TO DIS WITH THE INVESTIGATIVE PACKAGE.

"I AM AWARE OF NO INFORMATION OF THE TYPE CONTAINED IN APPENDIX E, DOD 5200.2-R, RELATING TO SUBJECT'S TRUSTWORTHINESS, RELIABILITY, OR LOYALTY THAT MAY REFLECT ADVERSELY ON HIS/HER ABILITY TO SAFEGUARD CLASSIFIED INFORMATION."

C. IF THE SUPERVISOR IS AWARE OF SUCH SIGNIFICANT ADVERSE INFORMATION, THE FOLLOWING STATEMENT SHALL BE DOCUMENTED, SIGNED AND DATED AND FORWARDED TO

DIS WITH THE INVESTIGATIVE PACKAGE, AND A WRITTEN SUMMARY OF THE DEROGATORY INFORMATION FORWARDED TO DIS WITH THE INVESTIGATIVE PACKAGE:

"I AM AWARE OF INFORMATION OF THE TYPE CONTAINED IN APPENDIX E, DOD 5200.2-R, RELATING TO SUBJECT'S TRUSTWORTHINESS, RELIABILITY, OR LOYALTY THAT MAY REFLECT ADVERSELY ON HIS/HER ABILITY TO SAFEGUARD CLASSIFIED INFORMATION AND HAVE REPORTED ALL RELEVANT DETAILS TO THE APPROPRIATE SECURITY OFFICIAL(S)."

Supervisors must ensure that if they indicate that they are aware of adverse information that they include all relevant information when the certification is forwarded to the requesting security official. The security specialist will forward the supervisory certificate, security forms, and a summary of the derogatory information to DIS for a PR. RSOs and FDSO will determine if the employee's access should be suspended and if necessary, prepare the memorandum to the employee for signature by the regional director or Director, Field Detachment, as appropriate. A copy of the memorandum suspending access will be forwarded to CPS for further transmission to the WHS or the DIA, as appropriate. If a determination cannot be made whether or not access should be suspended, forward copies of the forms to the ASO for review and forwarding to the WHS CAF or the DIA CCP for a determination.

D. IN CONJUNCTION WITH REGULARLY SCHEDULED FITNESS AND PERFORMANCE REPORTS OF MILITARY AND CIVILIAN PERSONNEL WHOSE DUTIES ENTAIL ACCESS TO CLASSIFIED INFORMATION, SUPERVISORS WILL INCLUDE A COMMENT IN ACCORDANCE WITH PARAGRAPHS 9-102.B AND C, ABOVE, AS WELL AS A COMMENT REGARDING AN EMPLOYEE'S DISCHARGE OF SECURITY RESPONSIBILITIES, PURSUANT TO THEIR COMPONENT GUIDANCE. Supervisors are also required to comply with the provisions Chapter 17 (Section 4-1.g, DCAAM Manual 1400.1 (reference 1-100.r), regarding supervisory statements prepared in conjunction with annual performance appraisals. The following guidance will be used for this requirement.

1. If the supervisor is not aware of reportable information as reflected in Appendix E, the following statement will be made on a separate page and forwarded in a sealed envelope to the appropriate security officer.

"I am aware of no information of the type contained in Appendix E, DoD 5200.2-R relating to subject which may reflect adversely on his/her ability to safeguard classified information or occupy a sensitive position.

Signature: _____

Date: _____"

2. If the supervisor is aware of reportable information, the following statement, including pertinent details, will be immediately forwarded in a sealed envelope to the appropriate security officer.

"I am aware of information of the type contained in Appendix E, DoD 5200.2-R, relating to subject which may reflect adversely on his/her ability to safeguard classified information or occupy a sensitive position.

Signature: _____

Date: _____"

9-103 INDIVIDUAL RESPONSIBILITY

A. INDIVIDUALS MUST FAMILIARIZE THEMSELVES WITH PERTINENT SECURITY REGULATIONS THAT PERTAIN TO THEIR ASSIGNED DUTIES. FURTHER, INDIVIDUALS MUST BE AWARE OF THE STANDARDS OF CONDUCT REQUIRED OF PERSONS HOLDING POSITIONS OF TRUST. IN THIS CONNECTION, INDIVIDUALS MUST RECOGNIZE AND AVOID THE KIND OF PERSONAL BEHAVIOR THAT WOULD RESULT IN RENDERING ONE INELIGIBLE FOR CONTINUED ASSIGNMENT IN A POSITION OF TRUST. IN THE FINAL ANALYSIS, THE ULTIMATE RESPONSIBILITY FOR MAINTAINING CONTINUED ELIGIBILITY FOR A POSITION OF TRUST RESTS WITH THE INDIVIDUAL. In accordance with the policy of DoD Directive 5240.6 (Enclosure 5), all DCAA employees must promptly report to their security officer or supervisor the following:

1. Information concerning any international or domestic terrorist organization, sabotage, or subversive activity that is reasonably believed to pose or have a potential to pose a direct threat to DoD or other U.S. facilities, activities, personnel, or resources.
2. A request by anyone (regardless of nationality) for illegal or unauthorized access to classified or controlled defense information.
3. Any contact with an individual (regardless of nationality) under circumstances which suggest the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.
4. Information indicating the deliberate compromise of classified defense information, attempted or contemplated by DoD personnel, with the intention of conveying classified documents, information, or material to any unauthorized persons.

B. MOREOVER, INDIVIDUALS HAVING ACCESS TO CLASSIFIED INFORMATION MUST REPORT PROMPTLY TO THEIR SECURITY OFFICE:

(1) ANY FORM OF CONTACT, INTENTIONAL OR OTHERWISE, WITH INDIVIDUALS OF ANY NATIONALITY, WHETHER WITHIN OR OUTSIDE THE SCOPE OF THE EMPLOYEE'S OFFICIAL ACTIVITIES, IN WHICH:

(A) ILLEGAL OR UNAUTHORIZED ACCESS IS SOUGHT TO CLASSIFIED OR OTHERWISE SENSITIVE INFORMATION.

(B) THE EMPLOYEE IS CONCERNED THAT HE OR SHE MAY BE THE TARGET OF EXPLOITATION BY A FOREIGN ENTITY.

(2) ANY INFORMATION OF THE TYPE REFERRED TO IN PARAGRAPH 2-200 OR APPENDIX I. [CH2 to DoD 5200.2-R, 7/14/93]

DCAA employees occupying sensitive positions must also report to their security officer all information of the type listed in paragraph 2-200 and Appendix I. Failure to make such reports will result in appropriate judicial and/or administrative action.

9-104 CO-WORKER RESPONSIBILITY

CO-WORKERS HAVE AN EQUAL OBLIGATION TO ADVISE THEIR SUPERVISOR OR APPROPRIATE SECURITY OFFICIAL WHEN THEY BECOME AWARE OF INFORMATION WITH

POTENTIALLY SERIOUS SECURITY SIGNIFICANCE REGARDING SOMEONE WITH ACCESS TO CLASSIFIED INFORMATION OR EMPLOYED IN A SENSITIVE POSITION.

Section 2

SECURITY EDUCATION

9-200 GENERAL

THE EFFECTIVENESS OF AN INDIVIDUAL IN MEETING SECURITY RESPONSIBILITIES IS PROPORTIONAL TO THE DEGREE TO WHICH THE INDIVIDUAL UNDERSTANDS THEM. THUS, AN INTEGRAL PART OF THE DOD SECURITY PROGRAM IS THE INDOCTRINATION OF INDIVIDUALS ON THEIR SECURITY RESPONSIBILITIES. MOREOVER, SUCH INDOCTRINATION IS ESSENTIAL TO THE EFFICIENT FUNCTIONING OF THE DOD PERSONNEL SECURITY PROGRAM.

ACCORDINGLY, HEADS OF DOD COMPONENTS SHALL ESTABLISH PROCEDURES IN ACCORDANCE WITH THIS CHAPTER WHEREBY PERSONS REQUIRING ACCESS TO CLASSIFIED INFORMATION, OR BEING ASSIGNED TO POSITIONS THAT REQUIRE THE OCCUPANTS TO BE DETERMINED TRUSTWORTHY ARE PERIODICALLY BRIEFED AS TO THEIR SECURITY RESPONSIBILITIES.

Security education of all Agency employees is required in varying degrees by DoD Directive 5240.6 (reference 1-100.c), DCAAM 5205.1 (reference 1-100.g), and this section. In compliance with these provisions, the Agency has developed a briefings outline which is Enclosure 4. Enclosure 4 will be used as a guide by security specialists to ensure that employees receive appropriate briefings and debriefings required by this section.

9-201 INITIAL BRIEFING

A. ALL PERSONS CLEARED FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNED TO DUTIES REQUIRING A TRUSTWORTHINESS DETERMINATION UNDER THIS REGULATION SHALL BE GIVEN AN INITIAL SECURITY BRIEFING. THE BRIEFING SHALL BE IN ACCORDANCE WITH THE REQUIREMENTS OF PARAGRAPH 10-102, DOD 5200.1-R (REFERENCE (Q)) AND CONSIST OF THE FOLLOWING ELEMENTS:

- (1) THE SPECIFIC SECURITY REQUIREMENTS OF THEIR PARTICULAR JOB.
- (2) THE TECHNIQUES EMPLOYED BY FOREIGN INTELLIGENCE ACTIVITIES IN ATTEMPTING TO OBTAIN CLASSIFIED INFORMATION AND THEIR RESPONSIBILITY FOR REPORTING SUCH ATTEMPTS.
- (3) THE PROHIBITION AGAINST DISCLOSING CLASSIFIED INFORMATION, BY ANY MEANS, TO UNAUTHORIZED PERSONS OR DISCUSSING OR HANDLING CLASSIFIED INFORMATION IN A MANNER THAT WOULD MAKE IT ACCESSIBLE TO UNAUTHORIZED PERSONS.
- (4) THE PENALTIES THAT MAY BE IMPOSED FOR SECURITY VIOLATIONS.

DCAA Form 5210-4, Security Briefing Acknowledgment, will be used to document briefings administered in accordance with provisions of this paragraph, and section 10-102, DCAA Manual 5205.1 (reference 1-100.g). DCAA Form 5210-4, for employees retaining security clearances after transfer to another DCAA office, will be forwarded for filing in the gaining office security files.

B. IF AN INDIVIDUAL DECLINES TO EXECUTE STANDARD FORM 312, "CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT" (REPLACED THE STANDARD FORM 189), THE DOD COMPONENT SHALL INITIATE ACTION TO DENY OR REVOKE THE SECURITY CLEARANCE OF SUCH PERSON IN ACCORDANCE WITH PARAGRAPH 8-201, ABOVE. [CH2 to DoD 5200.2-R, 7/14/93] The policy outlined in this paragraph will be implemented if an individual refuses to sign Standard Form 312, Classified Information Nondisclosure Agreement.

9-202 REFRESHER BRIEFING

PROGRAMS SHALL BE ESTABLISHED TO PROVIDE, AT A MINIMUM, ANNUAL SECURITY TRAINING FOR PERSONNEL HAVING CONTINUED ACCESS TO CLASSIFIED INFORMATION. THE ELEMENTS OUTLINED IN PARAGRAPH 10-101, DOD 5200.1-R (REFERENCE (Q)) SHALL BE TAILORED TO FIT THE NEEDS OF EXPERIENCED PERSONNEL.

9-203 FOREIGN TRAVEL BRIEFING

WHILE WORLD EVENTS DURING THE PAST SEVERAL YEARS HAVE DIMINISHED THE THREAT TO OUR NATIONAL SECURITY FROM TRADITIONAL COLD-WAR ERA FOREIGN INTELLIGENCE SERVICES, FOREIGN INTELLIGENCE SERVICES CONTINUE TO PURSUE THE UNAUTHORIZED ACQUISITION OF CLASSIFIED OR OTHERWISE SENSITIVE U.S. GOVERNMENT INFORMATION, THROUGH THE RECRUITMENT OF U.S. GOVERNMENT EMPLOYEES WITH ACCESS TO SUCH INFORMATION. THROUGH SECURITY BRIEFINGS AND EDUCATION, THE DEPARTMENT OF DEFENSE CONTINUES TO PROVIDE FOR THE PROTECTION OF INFORMATION AND TECHNOLOGY CONSIDERED VITAL TO THE NATIONAL SECURITY INTERESTS FROM ILLEGAL OR UNAUTHORIZED ACQUISITION BY FOREIGN INTELLIGENCE SERVICES.

A. DOD COMPONENTS WILL ESTABLISH APPROPRIATE INTERNAL PROCEDURES REQUIRING ALL PERSONNEL POSSESSING A DOD SECURITY CLEARANCE TO REPORT TO THEIR SECURITY OFFICE ALL CONTACTS WITH INDIVIDUALS OF ANY NATIONALITY, WHETHER WITHIN OR OUTSIDE THE SCOPE OF THE EMPLOYEE'S OFFICIAL ACTIVITIES, IN WHICH:

(1) ILLEGAL OR UNAUTHORIZED ACCESS IS SOUGHT TO CLASSIFIED OR OTHERWISE SENSITIVE INFORMATION.

(2) THE EMPLOYEE IS CONCERNED THAT HE OR SHE MAY BE THE TARGET OF EXPLOITATION BY A FOREIGN ENTITY.

All DCAA employees are required to immediately report to their security officer contacts with individuals of any nationality, whether within or outside the scope of their official activities, if either of the above criteria apply.

B. THE DOD SECURITY MANAGER, SECURITY SPECIALIST, OR OTHER QUALIFIED INDIVIDUAL WILL REVIEW AND EVALUATE THE REPORTED INFORMATION. ANY FACTS OR CIRCUMSTANCES OF A REPORTED CONTACT WITH A FOREIGN NATIONAL THAT APPEAR TO:

(1) INDICATE AN ATTEMPT OR INTENTION TO OBTAIN UNAUTHORIZED ACCESS TO PROPRIETARY, SENSITIVE, OR CLASSIFIED INFORMATION OR TECHNOLOGY,

(2) OFFER A REASONABLE POTENTIAL FOR SUCH, OR

(3) INDICATE THE POSSIBILITY OF CONTINUED CONTACT WITH THE FOREIGN NATIONAL FOR SUCH PURPOSES,

SHALL BE PROMPTLY REPORTED TO THE APPROPRIATE COUNTERINTELLIGENCE AGENCY. [CH2 to DoD 5200.2-R, 7/14/93]

The ASO will be notified immediately if an employee reports any facts or circumstances of a contact with a foreign national that meets the criteria in 9-203.E. RSOs, SCOs, FDSO, and CPS security specialists will summarize the information in a memorandum to the ASO, addressing the who, what, when, where, and how the contact happened. The ASO will report to the appropriate counterintelligence agency, if appropriate.

9-204 TERMINATION BRIEFING

A. UPON TERMINATION OF EMPLOYMENT, ADMINISTRATIVE WITHDRAWAL OF SECURITY CLEARANCE, OR CONTEMPLATED ABSENCE FROM DUTY OR EMPLOYMENT FOR 60 DAYS OR MORE, DOD MILITARY PERSONNEL AND CIVILIAN EMPLOYEES SHALL BE GIVEN A TERMINATION BRIEFING, RETURN ALL CLASSIFIED MATERIAL, AND EXECUTE A SECURITY TERMINATION STATEMENT. THIS STATEMENT SHALL INCLUDE:

(1) AN ACKNOWLEDGMENT THAT THE INDIVIDUAL HAS READ THE APPROPRIATE PROVISIONS OF THE ESPIONAGE ACT, OTHER CRIMINAL STATUTES, DOD REGULATIONS APPLICABLE TO THE SAFEGUARDING OF CLASSIFIED INFORMATION TO WHICH THE INDIVIDUAL HAS HAD ACCESS, AND UNDERSTANDS THE IMPLICATIONS THEREOF;

(2) A DECLARATION THAT THE INDIVIDUAL NO LONGER HAS ANY DOCUMENTS OR MATERIAL CONTAINING CLASSIFIED INFORMATION IN HIS OR HER POSSESSION;

(3) AN ACKNOWLEDGMENT THAT THE INDIVIDUAL WILL NOT COMMUNICATE OR TRANSMIT CLASSIFIED INFORMATION TO ANY UNAUTHORIZED PERSON OR AGENCY; AND

(4) AN ACKNOWLEDGMENT THAT THE INDIVIDUAL WILL REPORT WITHOUT DELAY TO THE FBI OR THE DOD COMPONENT CONCERNED ANY ATTEMPT BY ANY UNAUTHORIZED PERSON TO SOLICIT CLASSIFIED INFORMATION.

Termination briefings will be administered in accordance with provisions of this section, and section 10-105, DCAA Manual 5205.1 (reference 1-100.g). DCAA Form 5210-3, Security Termination Statement, will be used to document the required debriefing within DCAA. Debriefings may be administered by managers, their designated SCOs, and security specialists who will sign as the witness to an employee's signature on the DCAA Form 5210-3. Completed DCAA Forms 5210-3 will be forwarded to CPS through RSOs or FDSO, as appropriate.

B. WHEN AN INDIVIDUAL REFUSES TO EXECUTE A SECURITY TERMINATION STATEMENT, THAT FACT SHALL BE REPORTED IMMEDIATELY TO THE SECURITY MANAGER OF THE COGNIZANT ORGANIZATION CONCERNED. IN ANY SUCH CASE, THE INDIVIDUAL INVOLVED SHALL BE DEBRIEFED ORALLY. THE FACT OF A REFUSAL TO SIGN A SECURITY TERMINATION STATEMENT SHALL BE REPORTED TO THE DIRECTOR, DEFENSE INVESTIGATIVE SERVICE, WHO SHALL ENSURE THAT IT IS RECORDED IN THE DEFENSE CLEARANCE AND INVESTIGATIONS INDEX.
[CH2 to DoD 5200.2-R, 7/14/93]

C. THE SECURITY TERMINATION STATEMENT SHALL BE RETAINED BY THE DOD COMPONENT THAT AUTHORIZED THE INDIVIDUAL ACCESS TO CLASSIFIED INFORMATION FOR

THE PERIOD SPECIFIED IN THE COMPONENT'S RECORDS RETENTION SCHEDULES, BUT FOR A MINIMUM OF 2 YEARS AFTER THE INDIVIDUAL IS GIVEN A TERMINATION BRIEFING.

D. IN ADDITION TO THE PROVISIONS OF SUBPARAGRAPHS A., B., AND C. ABOVE, DOD COMPONENTS SHALL ESTABLISH A CENTRAL AUTHORITY TO BE RESPONSIBLE FOR ENSURING THAT SECURITY TERMINATION STATEMENTS ARE EXECUTED BY SENIOR PERSONNEL

(GENERAL OFFICERS, FLAG OFFICERS AND GS-16s AND ABOVE). FAILURE ON THE PART OF SUCH PERSONNEL TO EXECUTE A SECURITY TERMINATION STATEMENT SHALL BE REPORTED IMMEDIATELY TO THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY.

CHAPTER X

SAFEGUARDING PERSONNEL SECURITY INVESTIGATIVE RECORDS

10-100 GENERAL

IN RECOGNITION OF THE SENSITIVITY OF PERSONNEL SECURITY REPORTS AND RECORDS, PARTICULARLY WITH REGARD TO INDIVIDUAL PRIVACY, IT IS DEPARTMENT OF DEFENSE POLICY THAT SUCH PERSONAL INFORMATION SHALL BE HANDLED WITH THE HIGHEST DEGREE OF DISCRETION. ACCESS TO SUCH INFORMATION SHALL BE AFFORDED ONLY FOR THE PURPOSE CITED HEREIN AND TO PERSONS WHOSE OFFICIAL DUTIES REQUIRE SUCH INFORMATION. PERSONNEL SECURITY INVESTIGATIVE REPORTS MAY BE USED ONLY FOR THE PURPOSES OF DETERMINING ELIGIBILITY OF DOD MILITARY AND CIVILIAN PERSONNEL, CONTRACTOR EMPLOYEES, AND OTHER PERSONS AFFILIATED WITH THE DEPARTMENT OF DEFENSE, FOR ACCESS TO CLASSIFIED INFORMATION, ASSIGNMENT OR RETENTION IN SENSITIVE DUTIES OR OTHER SPECIFICALLY DESIGNATED DUTIES REQUIRING SUCH INVESTIGATION, OR FOR LAW ENFORCEMENT AND COUNTERINTELLIGENCE INVESTIGATIONS. OTHER USES ARE SUBJECT TO THE SPECIFIC WRITTEN AUTHORIZATION OF THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY. It is the policy of DCAA that personnel security investigations and personnel security determinations be handled with the highest degree of protection. The Privacy Act of 1974, as well as implementing DoD and OPM regulations, require that appropriate safeguards be established to ensure the security and confidentiality of records, and to protect them from unauthorized or unintentional access, disclosure, modification, or destruction. These records will be safeguarded in the manner prescribed by paragraph 10-103.c.

10-101 RESPONSIBILITIES

DOD AUTHORITIES RESPONSIBLE FOR ADMINISTERING THE DOD PERSONNEL SECURITY PROGRAM AND ALL DOD PERSONNEL AUTHORIZED ACCESS TO PERSONNEL SECURITY REPORTS AND RECORDS SHALL ENSURE THAT THE USE OF SUCH INFORMATION IS LIMITED TO THAT AUTHORIZED BY THIS REGULATION AND THAT SUCH REPORTS AND RECORDS ARE SAFEGUARDED AS PRESCRIBED HEREIN. THE HEADS OF DOD COMPONENTS AND THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY FOR THE OFFICE OF THE SECRETARY OF DEFENSE SHALL ESTABLISH INTERNAL CONTROLS TO ENSURE ADEQUATE SAFEGUARDING AND LIMIT ACCESS TO AND USE OF PERSONNEL SECURITY REPORTS AND RECORDS AS REQUIRED BY PARAGRAPH 10-102 AND 10-103 BELOW. The ASO for Headquarters, the RSOs in regional offices, and the FDSO in the Field Detachment, are responsible for ensuring that personnel security investigations and records are safeguarded properly and released only to personnel having action in the case.

10-102 ACCESS RESTRICTIONS

ACCESS TO PERSONNEL SECURITY INVESTIGATIVE REPORTS AND PERSONNEL SECURITY CLEARANCE DETERMINATION INFORMATION SHALL BE AUTHORIZED ONLY IN ACCORDANCE WITH DOD DIRECTIVES 5400.7 AND 5400.11 (REFERENCES (AA) AND (BB)) AND WITH THE FOLLOWING:

A. DOD PERSONNEL SECURITY INVESTIGATIVE REPORTS SHALL BE RELEASED OUTSIDE OF THE DOD ONLY WITH THE SPECIFIC APPROVAL OF THE INVESTIGATIVE AGENCY HAVING AUTHORITY OVER THE CONTROL AND DISPOSITION OF THE REPORTS. Personnel security investigative reports in DCAA possession will not be released outside the Agency without specific approval of the investigative agency having authority over the control and disposition of the reports.

B. WITHIN DOD, ACCESS TO PERSONNEL SECURITY INVESTIGATIVE REPORTS SHALL BE LIMITED TO THOSE DESIGNATED DOD OFFICIALS WHO REQUIRE ACCESS IN CONNECTION WITH SPECIFICALLY ASSIGNED PERSONNEL SECURITY DUTIES, OR OTHER ACTIVITIES SPECIFICALLY IDENTIFIED UNDER THE PROVISIONS OF PARAGRAPH 10-100. Access to personnel security investigative reports and personnel security determination data will be limited to those designated DCAA officials who require access in connection with specifically assigned personnel security duties, and to managers who have an official need for the information.

C. ACCESS BY SUBJECTS OF PERSONNEL SECURITY INVESTIGATIVE REPORTS SHALL BE AFFORDED IN ACCORDANCE WITH DOD DIRECTIVE 5400.11 (REFERENCE (BB)). Requests from employees for access to their personnel security investigations will be referred to the appropriate investigative agency with notification of the referral to the employee. (Also see DCAA Instruction 5410.8, DCAA Freedom of Information Act Program, and DCAA Instruction 5410.10, DCAA Privacy Act Program (references 1-100.n and c)).

D. ACCESS TO PERSONNEL SECURITY CLEARANCE DETERMINATION INFORMATION SHALL BE MADE AVAILABLE, OTHER THAN PROVIDED FOR IN C. ABOVE, THROUGH SECURITY CHANNELS, ONLY TO DOD OR OTHER OFFICIALS OF THE FEDERAL GOVERNMENT WHO HAVE AN OFFICIAL NEED FOR SUCH INFORMATION.

10-103 SAFEGUARDING PROCEDURES

PERSONNEL SECURITY INVESTIGATIVE REPORTS AND PERSONNEL SECURITY DETERMINATION INFORMATION SHALL BE SAFEGUARDED AS FOLLOWS:

A. AUTHORIZED REQUESTERS SHALL CONTROL AND MAINTAIN ACCOUNTABILITY OF ALL REPORTS OF INVESTIGATION RECEIVED.

B. REPRODUCTION, IN WHOLE OR IN PART, OF PERSONNEL SECURITY INVESTIGATIVE REPORTS BY REQUESTERS SHALL BE RESTRICTED TO THE MINIMUM NUMBER OF COPIES REQUIRED FOR THE PERFORMANCE OF ASSIGNED DUTIES. Reproduction of personnel security investigative reports will be restricted to the number of copies required for the performance of assigned duties.

C. PERSONNEL SECURITY INVESTIGATIVE REPORTS SHALL BE STORED IN A VAULT, SAFE, OR STEEL FILE CABINET HAVING AT LEAST A LOCKBAR AND AN APPROVED THREE-POSITION DIAL-TYPE COMBINATION PADLOCK OR IN A SIMILARLY PROTECTED AREA/CONTAINER. Personnel security investigations, determinations, and records will be safeguarded in accordance with procedures for individual personnel security files as prescribed in DCAA Manual 5015.1 (reference 1-100.r).

D. REPORTS OF DOD PERSONNEL SECURITY INVESTIGATIONS SHALL BE SEALED IN DOUBLE ENVELOPES OR COVERS WHEN TRANSMITTED BY MAIL OR WHEN CARRIED BY PERSONS NOT AUTHORIZED ACCESS TO SUCH INFORMATION. THE INNER COVER SHALL BEAR A NOTATION SUBSTANTIALLY AS FOLLOWS:

TO BE OPENED ONLY BY OFFICIALS DESIGNATED TO
RECEIVE REPORTS OF PERSONNEL SECURITY INVESTIGATION

Personnel security investigations and evaluations will be sealed in double envelopes or covers when transmitted by mail or hand carried by persons

not authorized access to such information. The inner cover will bear a notation substantially as follows:

TO BE OPENED ONLY BY (NAME AND TITLE OF SECURITY OFFICIAL)

E. AN INDIVIDUAL'S STATUS WITH RESPECT TO A PERSONNEL SECURITY CLEARANCE OR A SPECIAL ACCESS AUTHORIZATION IS TO BE PROTECTED AS PROVIDED FOR IN PARAGRAPH VI.C.6, DOD DIRECTIVE 5400.7 (REFERENCE (AA)).

10-104 RECORDS DISPOSITION

A. PERSONNEL SECURITY INVESTIGATIVE REPORTS, TO INCLUDE OPM NACIS MAY BE RETAINED BY DOD RECIPIENT ORGANIZATIONS, ONLY FOR THE PERIOD NECESSARY TO COMPLETE THE PURPOSE FOR WHICH IT WAS ORIGINALLY REQUESTED. SUCH REPORTS ARE CONSIDERED TO BE THE PROPERTY OF THE INVESTIGATING ORGANIZATION AND ARE ON LOAN TO THE RECIPIENT ORGANIZATION. ALL COPIES OF SUCH REPORTS SHALL BE DESTROYED WITHIN 90 DAYS AFTER COMPLETION OF THE REQUIRED PERSONNEL SECURITY DETERMINATION. DESTRUCTION SHALL BE ACCOMPLISHED IN THE SAME MANNER AS FOR CLASSIFIED INFORMATION IN ACCORDANCE WITH PARAGRAPH 9-101, DOD 5200.1-R (REFERENCE (Q)).

B. DOD RECORD REPOSITORIES AUTHORIZED TO FILE PERSONNEL SECURITY INVESTIGATIVE REPORTS SHALL DESTROY PSI REPORTS OF A FAVORABLE OR OF A MINOR DEROGATORY NATURE 15 YEARS AFTER THE DATE OF THE LAST ACTION. THAT IS, AFTER THE COMPLETION DATE OF THE INVESTIGATION OR THE DATE ON WHICH THE RECORD WAS LAST RELEASED TO AN AUTHORIZED USER--WHICHEVER IS LATER. PERSONNEL SECURITY INVESTIGATIVE REPORTS RESULTING IN AN UNFAVORABLE ADMINISTRATIVE PERSONNEL ACTION OR COURT-MARTIAL OR OTHER INVESTIGATIONS OF A SIGNIFICANT NATURE DUE TO INFORMATION CONTAINED IN THE INVESTIGATION SHALL BE DESTROYED 25 YEARS AFTER THE DATE OF THE LAST ACTION. FILES IN THIS LATTER CATEGORY THAT ARE DETERMINED TO BE OF POSSIBLE HISTORICAL VALUE AND THOSE OF WIDESPREAD PUBLIC OR CONGRESSIONAL INTEREST MAY BE OFFERED TO THE NATIONAL ARCHIVES AFTER 15 YEARS.

C. PERSONNEL SECURITY INVESTIGATIVE REPORTS ON PERSONS WHO ARE CONSIDERED FOR AFFILIATION WITH DOD WILL BE DESTROYED AFTER 1 YEAR IF THE AFFILIATION IS NOT COMPLETED.

DCAA Manual 5015.1 (reference 1-100.q), section 152, furnishes guidance for the disposition of personnel security files.

10-105 FOREIGN SOURCE INFORMATION

INFORMATION THAT IS CLASSIFIED BY A FOREIGN GOVERNMENT IS EXEMPT FROM PUBLIC DISCLOSURE UNDER THE FREEDOM OF INFORMATION AND PRIVACY ACTS. FURTHER, INFORMATION PROVIDED BY FOREIGN GOVERNMENTS REQUESTING AN EXPRESS PROMISE OF CONFIDENTIALITY SHALL BE RELEASED ONLY IN A MANNER THAT WILL NOT IDENTIFY OR ALLOW UNAUTHORIZED PERSONS TO IDENTIFY THE FOREIGN AGENCY CONCERNED.

CHAPTER XI

PROGRAM MANAGEMENT

11-100 GENERAL

TO ENSURE UNIFORM IMPLEMENTATION OF THE DOD PERSONNEL SECURITY PROGRAM THROUGHOUT THE DEPARTMENT, PROGRAM RESPONSIBILITY SHALL BE CENTRALIZED AT DOD COMPONENT LEVEL.

11-101 RESPONSIBILITIES

A. THE ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE (ASD(C3I)) SHALL HAVE PRIMARY RESPONSIBILITY FOR PROVIDING GUIDANCE, OVERSIGHT, DEVELOPMENT AND APPROVAL FOR POLICY AND PROCEDURES GOVERNING PERSONNEL SECURITY PROGRAM MATTERS WITHIN THE DEPARTMENT:

(1) PROVIDE PROGRAM MANAGEMENT THROUGH ISSUANCE OF POLICY AND OPERATING GUIDANCE.

(2) PROVIDE STAFF ASSISTANCE TO THE DOD COMPONENTS AND DEFENSE AGENCIES IN RESOLVING DAY-TO-DAY SECURITY POLICY AND OPERATING PROBLEMS.

(3) CONDUCT INSPECTIONS OF THE DOD COMPONENTS FOR IMPLEMENTATION AND COMPLIANCE WITH DOD SECURITY POLICY AND OPERATING PROCEDURES.

(4) PROVIDE POLICY, OVERSIGHT, AND GUIDANCE TO THE COMPONENT ADJUDICATION FUNCTIONS.

(5) APPROVE, COORDINATE AND OVERSEE ALL DOD PERSONNEL SECURITY RESEARCH INITIATIVES AND ACTIVITIES.

B. THE GENERAL COUNSEL SHALL ENSURE THAT THE PROGRAM IS ADMINISTERED IN A MANNER CONSISTENT WITH THE LAWS; ALL PROCEEDINGS ARE PROMPTLY INITIATED AND EXPEDITIOUSLY COMPLETED; AND THAT THE RIGHTS OF INDIVIDUALS INVOLVED ARE PROTECTED, CONSISTENT WITH THE INTERESTS OF NATIONAL SECURITY. THE GENERAL COUNSEL SHALL ALSO ENSURE THAT ALL RELEVANT DECISIONS OF THE COURTS AND LEGISLATIVE INITIATIVES OF THE CONGRESS ARE OBTAINED ON A CONTINUING BASIS AND THAT ANALYSIS OF THE FOREGOING IS ACCOMPLISHED AND DISSEMINATED TO DOD PERSONNEL SECURITY PROGRAM MANAGEMENT AUTHORITIES.

C. THE HEADS OF THE COMPONENTS SHALL ENSURE THAT:

(1) THE DOD PERSONNEL SECURITY PROGRAM IS ADMINISTERED WITHIN THEIR AREA OF RESPONSIBILITY IN A MANNER CONSISTENT WITH THIS REGULATION.

(2) A SINGLE AUTHORITY WITHIN THE OFFICE OF THE HEAD OF THE DOD COMPONENT IS ASSIGNED RESPONSIBILITY FOR ADMINISTERING THE PROGRAM WITHIN THE COMPONENT.

(3) INFORMATION AND RECOMMENDATIONS ARE PROVIDED THE ASD(C3I) AND THE GENERAL COUNSEL AT THEIR REQUEST CONCERNING ANY ASPECT OF THE PROGRAM.

The Director, DCAA, has delegated responsibilities under this section as follows:

MARCH 1996

(1) The Assistant Director, Resources, will ensure that the personnel security program is administered within DCAA in a manner consistent with this manual.

(2) The ASO will exercise overall management and day-to-day administration of the DCAA personnel security program. This official may report directly to the Agency Director when, in the ASO's opinion, the potential impact, extreme sensitivity, or delicacy of special cases makes such a procedure desirable. The ASO will seek legal guidance on the administration of the DCAA personnel security program, and the rights of individuals thereunder, from the Agency Counsel.

(3) The ASO is designated as point of contact with OASD(C3I) and the General Counsel of the Agency on all aspects of this program.

(4) Heads of principal staff elements at the DCAA Headquarters; the Director of Field Detachment; regional directors; regional audit managers; personnel officers; regional security and security control officers; and the heads of field audit offices will ensure that the DCAA personnel security program policies, procedures, and requirements of this manual are implemented within their respective areas of management responsibility.

11-102

REPORTING REQUIREMENTS

A. THE OASD(C3I) SHALL BE PROVIDED PERSONNEL SECURITY PROGRAM MANAGEMENT DATA BY THE DEFENSE DATA MANPOWER CENTER (DMDC) BY 31 DECEMBER EACH YEAR FOR THE PRECEDING FISCAL YEAR. TO FACILITATE ACCURATE PREPARATION OF THIS REPORT, ALL ADJUDICATIVE DETERMINATIONS MUST BE ENTERED INTO THE DCII BY ALL DOD CENTRAL ADJUDICATION FACILITIES NO LATER THAN THE END OF THE FISCAL YEAR. THE INFORMATION REQUIRED BELOW IS ESSENTIAL FOR BASIC PERSONNEL SECURITY PROGRAM MANAGEMENT AND IN RESPONDING TO REQUESTS FOR THE SECRETARY OF DEFENSE AND CONGRESS. THE REPORT SHALL COVER THE PRECEDING FISCAL YEAR, BROKEN OUT BY CLEARANCE CATEGORY, ACCORDING TO MILITARY (OFFICER OR ENLISTED), CIVILIAN OR CONTRACTOR STATUS AND BY THE CENTRAL ADJUDICATION FACILITY THAT TOOK THE ACTION, USING THE ENCLOSED FORMAT:

ISSUED; (1) NUMBER OF TOP SECRET, SECRET AND CONFIDENTIAL CLEARANCES

DENIED; (2) NUMBER OF TOP SECRET, SECRET AND CONFIDENTIAL CLEARANCES

REVOKED; (3) NUMBER OF TOP SECRET, SECRET AND CONFIDENTIAL CLEARANCES

(4) NUMBER OF SCI ACCESS DETERMINATIONS ISSUED;

(5) NUMBER OF SCI ACCESS DETERMINATIONS DENIED;

(6) NUMBER OF SCI ACCESS DETERMINATIONS REVOKED; AND

(7) TOTAL NUMBER OF PERSONNEL HOLDING A CLEARANCE FOR TOP SECRET, SECRET, CONFIDENTIAL AND SENSITIVE COMPARTMENTED INFORMATION AS OF THE END OF THE FISCAL YEAR.

B. THE DEFENSE INVESTIGATIVE SERVICE (DIS) SHALL PROVIDE THE OASD(C3I) A QUARTERLY REPORT THAT REFLECTS INVESTIGATIVE CASES OPENED AND CLOSED DURING THE MOST RECENT QUARTER, BY CASE CATEGORY TYPE, AND BY MAJOR REQUESTER. THE INFORMATION PROVIDED BY DIS IS ESSENTIAL FOR EVALUATING STATISTICAL DATA REGARDING INVESTIGATIVE WORKLOAD AND THE MANPOWER REQUIRED TO PERFORM PERSONNEL SECURITY INVESTIGATIONS. CASE CATEGORY TYPES INCLUDE NATIONAL AGENCY CHECKS (NACs); EXPANDED NACs; SINGLE SCOPE BACKGROUND INVESTIGATIONS; PERIODIC REINVESTIGATIONS (PRs); SECRET PERIODIC REINVESTIGATIONS (SPRs); POST ADJUDICATIVE; SPECIAL INVESTIGATIVE INQUIRIES (SIIs); AND LIMITED INQUIRIES. THIS REPORT SHALL BE FORWARDED TO OASD(C3I) WITHIN 45 DAYS AFTER THE END OF EACH QUARTER.

C. THE REPORTING REQUIREMENT FOR DMDC AND DIS HAS BEEN ASSIGNED REPORT CONTROL SYMBOL DD-C3I(A) 1749. [CH2 to DoD 5200.2-R, 7/14/93.]

d. Under the provisions of DoD Directive 5240.6 (reference 1-100.c and Enclosure 5), and Chapter IX of this manual, RSOs and FDSO will submit the following report to the ASO by 15 October of each year. The report control symbol is RCS:CPS(A249). The ASO will consolidate regional reports with Headquarters statistics and forward to OASD(C3I) by 1 November of each year:

(a) Number of personnel briefed on the requirement to report information or circumstances that could pose a threat to the security of DoD personnel, resources, or classified or controlled defense information.

(b) Number of contacts or reports received by category. (See Enclosure 5 for defined categories I through III, V, and VI).

(c) Number of investigations initiated as a result of information reported.

(d) Number of investigations resulting in:

(1) Planned or actual offensive counterespionage operations.

(2) Confirmed instances of espionage.

(3) Confirmed deliberate compromise of defense information.

(4) Administrative or judicial action against individuals violating reporting requirements.

(5) Persons prosecuted or pending prosecution on charges of espionage or related offenses, based upon reports under DoD Directive 5240.6 (reference 1-100.c).

(e) Reports involving information on terrorist threats to the security of DoD or other U.S. personnel and resources.

11-103

INSPECTIONS

THE HEADS OF DOD COMPONENTS SHALL ASSURE THAT PERSONNEL SECURITY PROGRAM MATTERS ARE INCLUDED IN THEIR ADMINISTRATIVE INSPECTION PROGRAMS. The ASO, security specialists, and FAO SCOs will conduct periodic reviews of regional and selected field audit office personnel security programs in accordance with DCAA Regulation 5205.3 (reference 1-100.t).

CHAPTER XII

DEFENSE CLEARANCE AND INVESTIGATIONS INDEX

12-100 GENERAL

A. THE DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII) IS THE SINGLE, AUTOMATED CENTRAL REPOSITORY THAT IDENTIFIES INVESTIGATIONS CONDUCTED BY DOD INVESTIGATIVE AGENCIES, AND PERSONNEL SECURITY DETERMINATIONS MADE BY DOD ADJUDICATIVE AUTHORITIES.

B. THE DCII DATA BASE CONSISTS OF AN ALPHABETICAL INDEX OF PERSONAL NAMES AND IMPERSONAL TITLES THAT APPEAR AS SUBJECTS, CO-SUBJECTS, VICTIMS, OR CROSS-REFERENCED INCIDENTAL SUBJECTS, IN INVESTIGATIVE DOCUMENTS MAINTAINED BY DOD CRIMINAL, COUNTERINTELLIGENCE, FRAUD, AND PERSONNEL SECURITY INVESTIGATIVE ACTIVITIES. ADDITIONALLY, PERSONNEL SECURITY ADJUDICATIVE DETERMINATIONS ARE MAINTAINED, BY SUBJECT, IN THE DCII.

C. DOD INVESTIGATIVE AND ADJUDICATIVE AUTHORITIES REPORT INFORMATION WHICH IS USED FOR INVESTIGATIVE, ADJUDICATIVE, STATISTICAL, RESEARCH AND OTHER PURPOSES AS AUTHORIZED BY OASD(C3I) APPROVAL.

12-101 ACCESS

THE DCII IS OPERATED AND MAINTAINED BY THE DEFENSE INVESTIGATIVE SERVICE (DIS). ACCESS IS NORMALLY LIMITED TO THE DEPARTMENT OF DEFENSE AND OTHER FEDERAL AGENCIES WITH ADJUDICATIVE, INVESTIGATIVE AND/OR COUNTERINTELLIGENCE (CI) MISSIONS. AGENCIES WISHING TO GAIN ACCESS TO THE DCII MUST SUBMIT A WRITTEN REQUEST OUTLINING SPECIFIC REQUIREMENTS WITH CORRESPONDING JUSTIFICATION, AS STATED IN PARAGRAPH 12-101.A. THROUGH 12-101.D. BELOW. ON APPROVAL, A MEMORANDUM OF UNDERSTANDING (MOU) ADDRESSING EQUIPMENT, MAINTENANCE, SECURITY, PRIVACY, AND OTHER AGENCY RESPONSIBILITIES SHALL BE FORWARDED TO THE REQUESTER BY DIS FOR SIGNATURE.

A. MILITARY DEPARTMENTS. REQUESTS FROM MILITARY DEPARTMENTS OR ORGANIZATIONS MUST BE SUBMITTED FOR APPROVAL AND ENDORSEMENT THROUGH THE FOLLOWING OFFICES TO DIS, DIRECTOR, NATIONAL COMPUTER CENTER, P.O. BOX 1211, BALTIMORE, MD 21203-1211.

(1) AIR FORCE. ADMINISTRATIVE ASSISTANT TO THE SECRETARY OF THE AIR FORCE, PENTAGON, ROOM 4D881, WASHINGTON, DC 20330-4000.

(2) ARMY. DIRECTOR, COUNTERINTELLIGENCE AND SECURITY COUNTERMEASURES, OFFICE OF THE DEPUTY CHIEF OF STAFF FOR INTELLIGENCE, DEPARTMENT OF THE ARMY, PENTAGON, ROOM 2D481, WASHINGTON, DC 20301-1050.

(3) NAVY AND MARINE CORPS. DIRECTOR, INFORMATION AND PERSONNEL SECURITY POLICY DIRECTORATE, NAVAL CRIMINAL INVESTIGATIVE SERVICE, CHIEF OF NAVAL OPERATIONS (OP-09N), WASHINGTON, DC 20350-2000.

B. UNIFIED COMBATANT COMMANDS. REQUESTS FROM UNIFIED COMBATANT COMMANDS MUST BE SUBMITTED FOR APPROVAL TO DIS, DIRECTOR, NATIONAL COMPUTER CENTER THROUGH THE JOINT CHIEFS OF STAFF, CHIEF, SECURITY DIVISION, DIRECTORATE FOR

INFORMATION AND RESOURCE MANAGEMENT, THE JOINT STAFF, ROOM 1B738, THE PENTAGON, WASHINGTON DC 20318-9300.

C. DEFENSE AGENCIES. REQUESTS FROM DOD AGENCIES MUST BE SUBMITTED THROUGH, AND WITH THE APPROVAL OF, THE AGENCY'S SECURITY HEADQUARTERS OFFICE TO DIS, DIRECTOR, NATIONAL COMPUTER CENTER, PO BOX 1211, BALTIMORE, MD 21203-1211.

D. NON-DOD AGENCIES. REQUESTS FROM NON-DOD AGENCIES MUST BE SUBMITTED TO THE DEPUTY ASSISTANT SECRETARY OF DEFENSE (INTELLIGENCE AND SECURITY), ATTN: COUNTERINTELLIGENCE AND SECURITY PROGRAMS, ROOM 3C281, 6000 DEFENSE PENTAGON, WASHINGTON, DC 20301-6000. ON APPROVAL, THOSE REQUESTS SHALL BE FORWARDED TO THE DIS FOR ACTION.

12-102 INVESTIGATIVE DATA

CONTRIBUTORS TO THE DCII SHALL ENSURE THAT ALL INVESTIGATIVE DATA ON AN INDIVIDUAL IS ENTERED INTO THE DCII.

A. AN ENTRY SHALL BE MADE TO INDICATE A PENDING INVESTIGATION WHEN AN INVESTIGATION IS OPENED.

B. WHEN AN INVESTIGATION HAS BEEN COMPLETED, THE CONTRIBUTOR SHALL CHANGE THE DCII STATUS TO REFLECT A COMPLETED INVESTIGATION, INCLUDING THE DATE (YEAR) OF THE INVESTIGATION.

C. CHANGES OR ADDITIONS TO EXISTING FILES MUST, WHENEVER APPROPRIATE, ALL BE REFLECTED IN THE DCII.

D. INVESTIGATIVE FILE TRACINGS MAY BE DELETED FROM THE DCII WHEN THE RETENTION PERIOD IS OVER AND THE RECORD FILE HAS BEEN DESTROYED.

12-103 ADJUDICATIVE DATA

ALL ADJUDICATIVE DETERMINATIONS ON PERSONNEL WITH ACCESS TO CLASSIFIED INFORMATION OR PERFORMING SENSITIVE DUTIES SHALL BE INDEXED IN THE DCII.

A. SPECIFICALLY, A DCII CLEARANCE ENTRY SHALL BE CREATED OR UPDATED AS FOLLOWS:

- (1) IMMEDIATELY UPON SUSPENSION OF ACCESS.
- (2) WHEN INTERIM ACCESS HAS BEEN AUTHORIZED BY THE CAF OR EMPLOYING ACTIVITY.
- (3) IMMEDIATELY FOLLOWING THE GRANTING, DENIAL, OR REVOCATION OF A CLEARANCE OR ACCESS.
- (4) FOLLOWING THE RECEIPT, REVIEW, AND ADJUDICATION OF INFORMATION RECEIVED SUBSEQUENT TO THE PRIOR CLEARANCE OR ACCESS DETERMINATION.

B. DCII ENTRIES SHALL INFORM THE DOD COMPONENTS OF THE CLEARANCE ELIGIBILITY AND/OR ACCESS STATUS OF AN INDIVIDUAL OR THE PRESENCE OF AN ADJUDICATIVE FILE.

C. AN ADJUDICATIVE DETERMINATION SHALL REMAIN IN THE DCII AS LONG AS THE SUBJECT IS AFFILIATED WITH THE DEPARTMENT OF DEFENSE. THE DETERMINATION MAY BE DELETED 2 YEARS AFTER THE EMPLOYMENT AND/OR CLEARANCE ELIGIBILITY ENDS. THE DELETED DCII DATA SHALL BE RETAINED BY THE DIS IN A HISTORICAL FILE FOR A MINIMUM OF 5 YEARS AFTER DELETION BY THE CONTRIBUTOR.

D. THE DATE OF THE DCII CLEARANCE AND/OR ACCESS ENTRY SHALL ALWAYS BE THE SAME AS OR SUBSEQUENT TO THE DATE OF THE MOST RECENT INVESTIGATION.

E. DOD COMPONENTS WILL NOTIFY THE CAP OF APPLICABLE PERSONNEL CHANGES TO ENSURE THE ACCURACY OF THE DCII DATA BASE.

12-104 NOTIFICATION TO OTHER CONTRIBUTORS

WHENEVER A DOD CONTRIBUTOR TO THE DCII BECOMES AWARE OF SIGNIFICANT UNFAVORABLE INFORMATION ABOUT AN INDIVIDUAL WITH A CLEARANCE AND/OR ACCESS ENTRY FROM ANOTHER DOD CONTRIBUTOR, IMMEDIATE NOTIFICATION MUST BE MADE TO THE LATTER ALONG WITH COPIES OF ALL RELEVANT INFORMATION.

12-105 SECURITY REQUIREMENTS FOR THE DCII

A. THE DCII IS AN UNCLASSIFIED SYSTEM THAT MEETS THE C-2 LEVEL OF PROTECTION UNDER THE COMPUTER SECURITY ACT OF 1987. CONTRIBUTORS MAY ENTER ONLY UNCLASSIFIED INFORMATION.

B. INFORMATION CONTAINED IN THE DCII RECEIVES THE PROTECTION REQUIRED BY THE PRIVACY ACT OF 1974. (REFERENCE M)

(1) DUE TO THE SENSITIVE NATURE OF THE INFORMATION, POSITIONS HAVING DIRECT (PASSWORD) ACCESS TO A DCII TERMINAL ARE CONSIDERED TO BE ADP-I CRITICAL SENSITIVE POSITIONS.

(2) INDIVIDUALS AUTHORIZED ACCESS TO THE DCII MUST HAVE A FAVORABLY COMPLETED SSBI (OR BI AND/OR SBI).

(3) DOD ACTIVITIES AND OTHER FEDERAL AGENCIES THAT HAVE BEEN AUTHORIZED "READ ONLY" ACCESS TO THE DCII MUST ALSO COMPLY WITH THOSE INVESTIGATIVE REQUIREMENTS.

C. EACH AUTHORIZED CONTRIBUTOR IS RESPONSIBLE FOR THE ACCURACY OF THE DATA IT ENTERS. CONTRIBUTORS MAY ENTER, MODIFY OR DELETE ONLY DATA ORIGINATED BY THEM. THE DCII SHALL NOT ALLOW ONE CONTRIBUTOR TO ALTER OR DELETE ANOTHER CONTRIBUTOR'S INFORMATION.

D. TO PREVENT UNAUTHORIZED ACCESS OR TAMPERING DURING NONWORKING HOURS, DCII TERMINALS MUST BE LOCATED IN AN AREA THAT IS SECURED BY GUARD PERSONNEL, AN ALARM SYSTEM, OR APPROPRIATE LOCKING DEVICE.

E. WHEN THE DCII TERMINAL IS OPERATIONAL, ACCESS TO DCII INFORMATION SHALL BE CONTROLLED AND LIMITED TO THOSE PERSONS AUTHORIZED ACCESS TO THAT INFORMATION.

12-106 DISCLOSURE OF INFORMATION

THE PRIVACY ACT OF 1974 REQUIRES AN ACCOUNTING OF THE DISCLOSURE OF PERSONAL INFORMATION WHEN IT IS PROVIDED TO ANOTHER AGENCY. FOR ACCESSING THE DCII, THE DEPARTMENT OF DEFENSE IS CONSIDERED A SINGLE AGENCY. DISCLOSURE OF PERSONAL INFORMATION IN THE DEPARTMENT OF DEFENSE DOES NOT REQUIRE SPECIFIC ACCOUNTING FOR EACH DISCLOSURE. ALL RELEASES OF INFORMATION OBTAINED FROM THE DCII TO ANY NON-DOD SOURCE MUST BE RECORDED IN THE DCII DISCLOSURE ACCOUNTING SYSTEM (DDAS) BY THE AGENCY THAT RELEASES THE INFORMATION. A CONTRIBUTOR MAY DISCLOSE ONLY THE DCII DATA ORIGINATED BY THAT CONTRIBUTOR TO THE SUBJECT OF THE DATA. REQUESTS FOR RELEASE OF INVESTIGATIVE REPORTS OR ADJUDICATIVE FILES ARE HANDLED AS PRIVACY ACT REQUESTS BY CONTRIBUTORS.

APPENDIX A

REFERENCES, CONTINUED

- (E) PUBLIC LAW 88-290, "NATIONAL SECURITY AGENCY - PERSONNEL SECURITY PROCEDURES," MARCH 26, 1964 (78 STAT. 168)
- (F) PUBLIC LAW 86-36, "NATIONAL SECURITY AGENCY-OFFICERS AND EMPLOYEES," MAY 29, 1959 (73 STAT. 63)
- (G) EXECUTIVE ORDER 10450, "SECURITY REQUIREMENTS FOR GOVERNMENT EMPLOYMENT," APRIL 27, 1953
- (H) EXECUTIVE ORDER 12333, "UNITED STATES INTELLIGENCE ACTIVITIES," DECEMBER 4, 1981
- (I) DOD DIRECTIVE 5210.45, "PERSONNEL SECURITY IN THE NATIONAL SECURITY AGENCY," MAY 9, 1964
- (J) EXECUTIVE ORDER 12958, "CLASSIFIED NATIONAL SECURITY INFORMATION," APRIL 17, 1995
- (K) EXECUTIVE ORDER 11935, "CITIZENSHIP REQUIREMENTS FOR FEDERAL EMPLOYMENT," SEPTEMBER 2, 1976
- (L) DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) NO. 1/14, "PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION (SCI)," JANUARY 22, 1992
- (M) SECTION 552A OF TITLE 5, UNITED STATES CODE
- (N) DOD DIRECTIVE 5100.23, "ADMINISTRATIVE ARRANGEMENTS FOR THE NATIONAL SECURITY AGENCY," MAY 17, 1967
- (O) AGREEMENT GOVERNING THE CONDUCT OF DEFENSE DEPARTMENT COUNTERINTELLIGENCE ACTIVITIES IN CONJUNCTION WITH THE FEDERAL BUREAU OF INVESTIGATION, APRIL 5, 1979
- (P) DOD DIRECTIVE 5210.48, "DOD POLYGRAPH PROGRAM," DECEMBER 24, 1984
- (Q) DOD 5200.1-R, "INFORMATION SECURITY PROGRAM REGULATION," JUNE 1986, AUTHORIZED BY DOD DIRECTIVE 5200.1, "DOD INFORMATION SECURITY PROGRAM," JUNE 7, 1982
- (R) DOD DIRECTIVE 5210.55, "SELECTION OF DOD MILITARY AND CIVILIAN PERSONNEL AND CONTRACTOR EMPLOYEES FOR ASSIGNMENT TO PRESIDENTIAL SUPPORT ACTIVITIES," JULY 6, 1977
- (S) DOD DIRECTIVE 5210.42, "NUCLEAR WEAPON PERSONNEL RELIABILITY PROGRAM," MAY 25, 1993
- (T) DOD DIRECTIVE 5200.8, "SECURITY OF MILITARY INSTALLATIONS AND RESOURCES," APRIL 25, 1991
- (U) DOD 1401.1-M, "PERSONNEL POLICY MANUAL FOR NONAPPROPRIATED FUND INSTRUMENTALITIES," JANUARY 1981, AUTHORIZED BY DOD INSTRUCTION 1401.1, NOVEMBER 15, 1985
- (V) DOD 5030.49-R, "CUSTOMS INSPECTION," MAY 1977, AUTHORIZED BY DOD DIRECTIVE 5030.49, JANUARY 6, 1984
- (W) DOD INSTRUCTION 5210.25, "ASSIGNMENT OF AMERICAN NATIONAL RED CROSS AND UNITED SERVICE ORGANIZATIONS, INC., EMPLOYEES TO DUTY WITH THE MILITARY SERVICES," MAY 12, 1983
- (X) DOD DIRECTIVE 5210.46, "DOD BUILDING SECURITY FOR THE NATIONAL CAPITAL REGION," JANUARY 28, 1982
- (Y) DOD DIRECTIVE 5210.65, "CHEMICAL AGENT SECURITY PROGRAM," OCTOBER 15, 1986
- (Z) DOD DIRECTIVE 5210.2, "ACCESS TO AND DISSEMINATION OF RESTRICTED DATA," JANUARY 12, 1978
- (AA) DOD DIRECTIVE 5400.7, "DOD FREEDOM OF INFORMATION ACT PROGRAM," MAY 13, 1988

- (BB) DOD DIRECTIVE 5400.11, "DEPARTMENT OF DEFENSE PRIVACY PROGRAM," JUNE 9, 1982
- (CC) 5 CFR, PART 732, "NATIONAL SECURITY POSITIONS," JANUARY 1, 1995
- (DD) SECTION 3571 OF TITLE 5, UNITED STATES CODE
- (EE) SECTION 3 OF PUBLIC LAW 89-380, "BACK PAY ACT OF 1966," MARCH 30, 1966 (80 STAT. 94)
- (FF) EXECUTIVE ORDER 9835, "PRESCRIBING PROCEDURES FOR THE ADMINISTRATION OF AN EMPLOYEE LOYALTY PROGRAM IN THE EXECUTIVE BRANCH OF THE GOVERNMENT," ISSUED 1947 (SUPERSEDED BY EXECUTIVE ORDER 10450)
- (GG) PUBLIC LAW 83-703, "ATOMIC ENERGY ACT OF 1954," AS AMENDED, AUGUST 30, 1954
- (HH) DOD DIRECTIVE 5105.42, "DEFENSE INVESTIGATIVE SERVICE," JUNE 14, 1985
- (II) DEFENSE INVESTIGATIVE SERVICE 20-1-M, "MANUAL FOR PERSONNEL SECURITY INVESTIGATIONS," JANUARY 1993
- (JJ) MEMORANDUM OF UNDERSTANDING BETWEEN THE DIRECTOR, WHITE HOUSE MILITARY OFFICE AND THE SPECIAL ASSISTANT TO THE SECRETARY AND DEPUTY SECRETARY OF DEFENSE, "WHITE HOUSE CLEARANCES," JULY 30, 1980
- (KK) USSAN INSTRUCTION 1-69, APRIL 21, 1982 (ENCLOSURE 2 TO DOD DIRECTIVE 5100.55, "UNITED STATES SECURITY AUTHORITY FOR NORTH ATLANTIC TREATY ORGANIZATION AFFAIRS," APRIL 21, 1982)
- (LL) DOD DIRECTIVE 5230.11, "DISCLOSURE OF CLASSIFIED MILITARY INFORMATION TO FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS," JUNE 16, 1982
- (MM) DOD DIRECTIVE 5100.3, "SUPPORT OF THE HEADQUARTERS OF UNIFIED, SPECIFIED, AND SUBORDINATE JOINT COMMANDS," NOVEMBER 1, 1988
- (NN) PUBLIC LAW 96-456, "CLASSIFIED INFORMATION PROCEDURES ACT," OCTOBER 15, 1980 (94 STAT. 2025)
- (OO) DOD DIRECTIVE 5142.1, "ASSISTANT SECRETARY OF DEFENSE (LEGISLATIVE AFFAIRS)," JULY 2, 1982
- (PP) SECTION 7532 OF TITLE 5, UNITED STATES CODE
- (QQ) DOD DIRECTIVE O-5205.7, "SPECIAL ACCESS PROGRAM (SAP) POLICY," JANUARY 4, 1989
- (RR) NATIONAL SECURITY DIRECTIVE 63, "SINGLE SCOPE BACKGROUND INVESTIGATIONS," OCTOBER 21, 1991

APPENDIX B

INVESTIGATIVE SCOPE

THIS APPENDIX PRESCRIBES THE SCOPE OF THE VARIOUS TYPES OF PERSONNEL SECURITY INVESTIGATIONS.

1. NATIONAL AGENCY CHECK (NAC). THE SCOPE FOR NAC IS FIVE YEARS OR TO AGE 18, WHICHEVER IS THE SHORTER PERIOD. AT A MINIMUM, THE FIRST THREE OF THE DESCRIBED AGENCIES (DCII, FBI/HQ, AND FBI/ID) BELOW SHALL BE INCLUDED IN EACH COMPLETE NAC; HOWEVER, A NAC MAY ALSO INCLUDE A CHECK OF ANY OR ALL OF THE OTHER DESCRIBED AGENCIES, IF APPROPRIATE.

A. THE DCII DATA BASE CONSISTS OF AN ALPHABETICAL INDEX OF PERSONAL NAMES AND IMPERSONAL TITLES THAT APPEAR AS SUBJECTS, CO-SUBJECTS, VICTIMS, OR CROSS-REFERENCED INCIDENTAL SUBJECTS, IN INVESTIGATIVE DOCUMENTS MAINTAINED BY DOD CRIMINAL, COUNTERINTELLIGENCE, FRAUD, AND PERSONNEL SECURITY INVESTIGATIVE ACTIVITIES. ADDITIONALLY, PERSONNEL SECURITY ADJUDICATIVE DETERMINATIONS ARE MAINTAINED, BY SUBJECT, IN THE DCII. DCII RECORDS WILL BE CHECKED ON ALL SUBJECTS OF DOD INVESTIGATIONS.

B. FBI/HQ HAS ON FILE COPIES OF INVESTIGATIONS CONDUCTED BY THE FBI. THE FBI/HQ CHECK, INCLUDED IN EVERY NAC, CONSISTS OF A REVIEW OF FILES FOR INFORMATION OF A SECURITY NATURE AND THAT DEVELOPED DURING APPLICANT-TYPE INVESTIGATIONS.

C. AN FBI/ID CHECK, INCLUDED IN EVERY NAC (BUT NOT ENTNAC), IS BASED UPON A TECHNICAL FINGERPRINT SEARCH THAT CONSISTS OF A CLASSIFICATION OF THE SUBJECT'S FINGERPRINTS AND COMPARISON WITH FINGERPRINT CARDS SUBMITTED BY LAW ENFORCEMENT ACTIVITIES. IF THE FINGERPRINT CARD IS NOT CLASSIFIABLE, A "NAME CHECK ONLY" OF THESE FILES IS AUTOMATICALLY CONDUCTED.

D. OPM. THE FILES OF OPM CONTAIN THE RESULTS OF INVESTIGATIONS CONDUCTED BY OPM UNDER E.O. 9835 AND 10450 (REFERENCES (FF) AND (G)), THOSE REQUESTED BY THE NUCLEAR REGULATORY COMMISSION (NRC), THE DEPARTMENT OF ENERGY (DOE), AND THOSE REQUESTED SINCE AUGUST 1952 TO SERVE AS A BASIS FOR "Q" CLEARANCES. OPM RECORDS ARE CHECKED ON ALL PERSONS WHO ARE, OR WHO HAVE BEEN, CIVILIAN EMPLOYEES OF THE U.S. GOVERNMENT; OR U.S. CITIZENS WHO ARE, OR WHO HAVE BEEN, EMPLOYED BY A UNITED NATIONS ORGANIZATION OR OTHER PUBLIC INTERNATIONAL ORGANIZATION; AND ON THOSE WHO HAVE BEEN GRANTED SECURITY CLEARANCES BY THE NRC OR THE DOE.

E. IMMIGRATION AND NATURALIZATION SERVICE (I&NS). THE FILES OF I&NS CONTAIN (OR SHOW WHERE FILED) NATURALIZATION CERTIFICATES, CERTIFICATES OF DERIVATIVE CITIZENSHIP, ALL MILITARY CERTIFICATES OF NATURALIZATION, REPATRIATION FILES, PETITIONS FOR NATURALIZATION AND DECLARATION OF INTENTION, VISITORS' VISAS, AND RECORDS OF ALIENS (INCLUDING GOVERNMENT OFFICIALS AND REPRESENTATIVES OF INTERNATIONAL ORGANIZATIONS) ADMITTED TEMPORARILY INTO THE U.S. I&NS RECORDS ARE CHECKED WHEN THE SUBJECT IS:

- (1) AN ALIEN IN THE U.S., OR
- (2) A NATURALIZED CITIZEN WHOSE NATURALIZATION HAS NOT BEEN VERIFIED, OR

(3) AN IMMIGRANT ALIEN, OR

(4) A U.S. CITIZEN WHO RECEIVES DERIVATIVE CITIZENSHIP THROUGH THE NATURALIZATION OF ONE OR BOTH PARENTS, PROVIDED THAT SUCH CITIZENSHIP HAS NOT BEEN VERIFIED IN A PRIOR INVESTIGATION.

F. STATE DEPARTMENT. THE STATE DEPARTMENT MAINTAINS THE FOLLOWING RECORDS:

(1) SECURITY DIVISION (S/D) FILES CONTAIN INFORMATION PERTINENT TO MATTERS OF SECURITY, VIOLATIONS OF SECURITY, PERSONNEL INVESTIGATIONS PERTINENT TO THAT AGENCY, AND CORRESPONDENCE FILES FROM 1950 TO DATE. THESE FILES ARE CHECKED ON ALL FORMER STATE DEPARTMENT EMPLOYEES.

(2) PASSPORT DIVISION (P/D) SHALL BE CHECKED IF SUBJECT INDICATES U.S. CITIZENSHIP DUE TO BIRTH IN A FOREIGN COUNTRY OF AMERICAN PARENTS. THIS IS A CHECK OF STATE DEPARTMENT EMBASSY FILES TO DETERMINE IF SUBJECT'S BIRTH WAS REGISTERED AT THE U.S. EMBASSY IN THE COUNTRY WHERE HE WAS BORN. VERIFICATION OF THIS REGISTRATION IS VERIFICATION OF CITIZENSHIP.

G. CENTRAL INTELLIGENCE AGENCY (CIA). THE CIA MAINTAINS THE FOLLOWING RECORDS:

(1) DIRECTORATE OF OPERATIONS (CIA-DO/IMS) MAINTAINS THE FOREIGN INTELLIGENCE/COUNTERINTELLIGENCE DATABASE. THIS DATABASE SHALL BE CHECKED FOR ALL ALIENS RESIDING OUTSIDE THE U.S. REQUIRING ACCESS TO CLASSIFIED INFORMATION (I.E., LAA). IF THE REQUESTER PROVIDES COMPLETE PERSONAL IDENTIFYING INFORMATION (COMPLETE NAME, DATE OF BIRTH, PLACE OF BIRTH, AND CITIZENSHIP), ALL ALIEN CO-SUBJECTS (ON SSBI's) RESIDING OUTSIDE THE U.S. ARE ALSO CHECKED. IN ADDITION, THIS DATABASE SHALL BE QUERIED ON THE SUBJECT ANY TIME THERE IS A COUNTERINTELLIGENCE CONCERN RAISED DURING THE CONDUCT OF THE PERSONNEL SECURITY INVESTIGATION.

(2) OFFICE OF SECURITY (CIA-SEC) MAINTAINS INFORMATION ON PRESENT AND FORMER EMPLOYEES, INCLUDING MEMBERS OF THE OFFICE OF STRATEGIC SERVICES (OSS), AND APPLICANTS FOR EMPLOYMENT. THESE FILES SHALL BE CHECKED IF SUBJECT HAS BEEN AN EMPLOYEE OF THE CIA OR WHEN OTHER SOURCES INDICATE THAT CIA MAY HAVE PERTINENT INFORMATION.

H. MILITARY PERSONNEL RECORD CENTER FILES ARE MAINTAINED BY SEPARATE DEPARTMENTS OF THE ARMED FORCES, GENERAL SERVICES ADMINISTRATION AND THE RESERVE RECORDS CENTERS. THEY CONSIST OF THE MASTER PERSONNEL RECORDS OF RETIRED, SEPARATED, RESERVE, AND ACTIVE DUTY MEMBERS OF THE ARMED FORCES. THESE RECORDS SHALL BE CHECKED WHEN THE REQUESTER PROVIDES REQUIRED IDENTIFYING DATA INDICATING SERVICE DURING THE LAST 5 YEARS.

I. TREASURY DEPARTMENT. THE FILES OF TREASURY DEPARTMENT AGENCIES (SECRET SERVICE, INTERNAL REVENUE SERVICE, AND BUREAU OF CUSTOMS) WILL BE CHECKED ONLY WHEN AVAILABLE INFORMATION INDICATES THAT AN AGENCY OF THE TREASURY DEPARTMENT MAY BE REASONABLY EXPECTED TO HAVE PERTINENT INFORMATION.

J. THE FILES OF OTHER AGENCIES SUCH AS THE NATIONAL GUARD BUREAU, THE DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE (DISCO), ETC., WILL BE CHECKED WHEN PERTINENT TO THE PURPOSE FOR WHICH THE INVESTIGATION IS BEING CONDUCTED.

2. SINGLE SCOPE BACKGROUND INVESTIGATION (SSBI):

THE FOLLOWING SSBI SCOPE REFLECTS THE REQUIREMENTS OF NATIONAL SECURITY DIRECTIVE 63 (REFERENCE (RR)).

A. SCOPE: THE PERIOD OF INVESTIGATION FOR AN SSBI IS THE LAST TEN (10) YEARS OR TO AGE 18, WHICHEVER IS THE SHORTER PERIOD, PROVIDED THAT THE INVESTIGATION COVERS AT LEAST THE LAST 2 FULL YEARS OF THE SUBJECT'S LIFE. NO INVESTIGATION WILL BE CONDUCTED FOR THE PERIOD PRIOR TO AN INDIVIDUAL'S 16TH BIRTHDAY. EMPHASIS SHALL BE PLACED ON PEER COVERAGE WHENEVER INTERVIEWS ARE HELD WITH PERSONAL SOURCES IN MAKING EDUCATION, EMPLOYMENT, AND REFERENCE (INCLUDING DEVELOPED) CONTACT.

B. EXPANSION OF INVESTIGATION. THE INVESTIGATION MAY BE EXPANDED AS NECESSARY, TO RESOLVE ISSUES AND/OR ADDRESS EMPLOYMENT STANDARDS UNIQUE TO INDIVIDUAL AGENCIES.

C. NAC. CHECKS ON SUBJECT AND SPOUSE/COHABITANT OF INVESTIGATIVE AND CRIMINAL HISTORY FILES OF THE FEDERAL BUREAU OF INVESTIGATION, INCLUDING SUBMISSION OF FINGERPRINT RECORDS ON THE SUBJECT, AND SUCH OTHER NATIONAL AGENCIES (DCII, INS, OPM, CIA, ETC.). IN ADDITION TO CONDUCTING A NAC ON THE SUBJECT OF THE INVESTIGATION, THE FOLLOWING ADDITIONAL REQUIREMENTS APPLY.

(1) A DCII, FBI/ID NAME CHECK ONLY AND FBI/HQ CHECK SHALL BE CONDUCTED ON SUBJECT'S SPOUSE OR COHABITANT. IN ADDITION, SUCH OTHER NATIONAL AGENCY CHECKS AS DEEMED APPROPRIATE BASED ON INFORMATION ON THE SUBJECT'S PSQ SHALL BE CONDUCTED.

(2) A CHECK OF FBI/HQ FILES ON MEMBERS OF SUBJECT'S IMMEDIATE FAMILY WHO ARE 18 YEARS OF AGE OR OLDER AND WHO ARE NON-U.S. CITIZENS SHALL BE CONDUCTED. AS USED THROUGHOUT THE REGULATION, MEMBERS OF SUBJECT'S IMMEDIATE FAMILY INCLUDE THE FOLLOWING:

(A) CURRENT SPOUSE.

(B) ADULT CHILDREN, 18 YEARS OF AGE OR OLDER, BY BIRTH, ADOPTION, OR MARRIAGE.

(C) NATURAL, ADOPTED, FOSTER, OR STEPPARENTS.

(D) GUARDIANS.

(E) BROTHERS AND SISTERS EITHER BY BIRTH, ADOPTION, OR REMARRIAGE OF EITHER PARENT.

(F) COHABITANT.

(3) THE FILES OF CIA SHALL BE REVIEWED ON NON-U.S. CITIZENS OF SUBJECT'S IMMEDIATE FAMILY WHO ARE 18 YEARS OF AGE OR OLDER.

(4) I&NS FILES ON MEMBERS OF SUBJECT'S IMMEDIATE FAMILY 18 YEARS OF AGE OR OLDER SHALL BE REVIEWED WHEN THEY ARE:

(A) NON-U.S. CITIZENS, OR

(B) NATURALIZED U.S. CITIZENS WHOSE NATURALIZATION HAS NOT BEEN VERIFIED IN A PRIOR INVESTIGATION, OR

(C) U.S. CITIZENS BORN IN A FOREIGN COUNTRY OF AMERICAN PARENT(S) OR U.S. CITIZENS WHO RECEIVED DERIVATIVE CITIZENSHIP THROUGH THE NATURALIZATION OF ONE OR BOTH PARENTS, PROVIDED THAT SUCH CITIZENSHIP HAS NOT BEEN VERIFIED IN A PRIOR INVESTIGATION.

D. SUBJECT INTERVIEW. REQUIRED IN ALL CASES AND SHALL BE CONDUCTED BY TRAINED SECURITY, INVESTIGATIVE, OR COUNTERINTELLIGENCE PERSONNEL TO ENSURE FULL INVESTIGATIVE COVERAGE. AN ADDITIONAL PERSONAL INTERVIEW SHALL BE CONDUCTED WHEN NECESSARY TO RESOLVE ANY SIGNIFICANT INFORMATION AND/OR INCONSISTENCIES DEVELOPED DURING THE INVESTIGATION. IN DEPARTMENTS OR AGENCIES WITH POLICIES SANCTIONING THE USE OF POLYGRAPH FOR PERSONNEL SECURITY PURPOSES, THE PERSONAL INTERVIEW MAY INCLUDE A POLYGRAPH EXAMINATION, CONDUCTED BY A QUALIFIED POLYGRAPH EXAMINER;

E. BIRTH. INDEPENDENT CERTIFICATION OF DATE AND PLACE OF BIRTH RECEIVED DIRECTLY FROM APPROPRIATE REGISTRATION AUTHORITY IF NOT OTHERWISE VERIFIED UNDER F., BELOW, OR IF A VARIANCE IS DEVELOPED.

F. CITIZENSHIP. SUBJECT MUST BE A U.S. CITIZEN. INDEPENDENT VERIFICATION OF CITIZENSHIP RECEIVED DIRECTLY FROM APPROPRIATE REGISTRATION AUTHORITY. FOR FOREIGN-BORN IMMEDIATE FAMILY MEMBERS 18 YEARS OF AGE OR OLDER, VERIFICATION OF CITIZENSHIP OR LEGAL STATUS IS ALSO REQUIRED. SUBJECT'S CITIZENSHIP STATUS MUST BE VERIFIED IN ALL CASES. U.S. CITIZENS WHO ARE SUBJECTS OF INVESTIGATION WILL BE REQUIRED TO PRODUCE DOCUMENTATION THAT WILL CONFIRM THEIR CITIZENSHIP. NORMALLY SUCH DOCUMENTATION SHOULD BE PRESENTED TO THE DOD COMPONENT CONCERNED PRIOR TO THE INITIATION OF THE REQUEST FOR INVESTIGATION. WHEN SUCH DOCUMENTATION IS NOT READILY AVAILABLE, INVESTIGATIVE ACTION MAY BE INITIATED WITH THE UNDERSTANDING THAT THE DESIGNATED AUTHORITY IN THE DOD COMPONENT WILL BE PROVIDED WITH THE DOCUMENTATION PRIOR TO THE ISSUANCE OF A CLEARANCE. DIS WILL NOT CHECK THE BVS FOR NATIVE-BORN U.S. CITIZENS EXCEPT AS INDICATED IN 4.E. ABOVE. IN THE CASE OF FOREIGN-BORN U.S. CITIZENS, DIS WILL CHECK I&NS RECORDS. THE CITIZENSHIP STATUS OF ALL FOREIGN-BORN MEMBERS OF SUBJECT'S IMMEDIATE FAMILY SHALL BE VERIFIED. ADDITIONALLY, WHEN THE INVESTIGATION INDICATES THAT A MEMBER OF SUBJECT'S IMMEDIATE FAMILY HAS NOT OBTAINED U.S. CITIZENSHIP AFTER HAVING BEEN ELIGIBLE FOR A CONSIDERABLE PERIOD OF TIME, AN ATTEMPT SHOULD BE MADE TO DETERMINE THE REASON. THE DOCUMENTS LISTED BELOW ARE ACCEPTABLE FOR PROOF OF U.S. CITIZENSHIP FOR PERSONNEL SECURITY DETERMINATION PURPOSES:

(1) A BIRTH CERTIFICATE MUST BE PRESENTED IF THE INDIVIDUAL WAS BORN IN THE UNITED STATES. TO BE ACCEPTABLE, THE CERTIFICATE MUST SHOW THAT THE BIRTH RECORD WAS FILED SHORTLY AFTER BIRTH AND MUST BE CERTIFIED WITH THE REGISTRAR'S SIGNATURE AND THE RAISED, IMPRESSED, OR MULTICOLORED SEAL OF HIS OFFICE EXCEPT FOR STATES OR JURISDICTIONS WHICH, AS A MATTER OF POLICY, DO NOT ISSUE CERTIFICATES WITH A RAISED OR IMPRESSED SEAL. UNCERTIFIED COPIES OF BIRTH CERTIFICATES ARE NOT ACCEPTABLE.

(A) A DELAYED BIRTH CERTIFICATE (A RECORD FILED MORE THAN ONE YEAR AFTER THE DATE OF BIRTH) IS ACCEPTABLE PROVIDED THAT IT SHOWS THAT THE REPORT OF BIRTH WAS SUPPORTED BY ACCEPTABLE SECONDARY EVIDENCE OF BIRTH AS DESCRIBED IN SUBPARAGRAPH (B), BELOW.

(B) IF SUCH PRIMARY EVIDENCE IS NOT OBTAINABLE, A NOTICE FROM THE REGISTRAR STATING THAT NO BIRTH RECORD EXISTS SHOULD BE SUBMITTED. THE NOTICE SHALL BE ACCOMPANIED BY THE BEST COMBINATION OF SECONDARY EVIDENCE OBTAINABLE. SUCH EVIDENCE MAY INCLUDE A BAPTISMAL CERTIFICATE, A CERTIFICATE OF CIRCUMCISION, A HOSPITAL BIRTH RECORD, AFFIDAVITS OF PERSONS HAVING PERSONAL KNOWLEDGE OF THE FACTS OF THE BIRTH, OR OTHER DOCUMENTARY EVIDENCE SUCH AS EARLY CENSUS, SCHOOL, OR FAMILY BIBLE RECORDS, NEWSPAPER FILES AND INSURANCE PAPERS. SECONDARY EVIDENCE SHOULD HAVE BEEN CREATED AS CLOSE TO THE TIME OF BIRTH AS POSSIBLE.

(C) ALL DOCUMENTS SUBMITTED AS EVIDENCE OF BIRTH IN THE UNITED STATES SHALL BE ORIGINAL OR CERTIFIED DOCUMENTS. UNCERTIFIED COPIES ARE NOT ACCEPTABLE.

(2) A CERTIFICATE OF NATURALIZATION SHALL BE SUBMITTED IF THE INDIVIDUAL CLAIMS CITIZENSHIP BY NATURALIZATION.

(3) A CERTIFICATE OF CITIZENSHIP ISSUED BY THE I&NS SHALL BE SUBMITTED IF CITIZENSHIP WAS ACQUIRED BY BIRTH ABROAD TO A U.S. CITIZEN PARENT OR PARENTS.

(4) A REPORT OF BIRTH ABROAD OF A CITIZEN OF THE UNITED STATES OF AMERICAN (FORM FS-240), A CERTIFICATION OF BIRTH (FORM FS-545 OR DS-L350), OR A CERTIFICATE OF CITIZENSHIP IS ACCEPTABLE IF CITIZENSHIP WAS ACQUIRED BY BIRTH ABROAD TO A U.S. CITIZEN PARENT OR PARENTS.

(5) A PASSPORT OR ONE IN WHICH THE INDIVIDUAL WAS INCLUDED WILL BE ACCEPTED AS PROOF OF CITIZENSHIP.

G. EDUCATION: INDEPENDENT VERIFICATION OF MOST RECENT OR MOST SIGNIFICANT CLAIMED ATTENDANCE AND/OR DEGREE/DIPLOMA WITHIN THE SCOPE OF INVESTIGATION VIA SEALED TRANSCRIPT RECEIVED DIRECTLY FROM THE INSTITUTION. IF ALL EDUCATION IS OUTSIDE OF THE INVESTIGATIVE SCOPE, THE LAST EDUCATION ABOVE HIGH SCHOOL LEVEL WILL BE VERIFIED.

H. EMPLOYMENT: DIRECT VERIFICATION THROUGH RECORDS OF ALL PERIODS OF EMPLOYMENT WITHIN SCOPE BUT IN ANY EVENT THE MOST RECENT TWO (2) YEARS. PERSONAL INTERVIEWS OF TWO SOURCES (SUPERVISOR/COWORKERS) FOR EACH EMPLOYMENT OF SIX MONTHS OR MORE SHALL BE ATTEMPTED. IN THE EVENT THAT NO EMPLOYMENT EXCEEDS SIX MONTHS, INTERVIEWS OF SUPERVISOR/COWORKERS SHALL BE ATTEMPTED. ALL PERIODS OF UNEMPLOYMENT IN EXCESS OF SIXTY (60) DAYS SHALL BE VERIFIED THROUGH RECORDS AND/OR SOURCES. ALL PRIOR FEDERAL/MILITARY SERVICE AND TYPE OF DISCHARGE(S) SHALL BE VERIFIED.

(1) NON-FEDERAL EMPLOYMENT. VERIFY ALL EMPLOYMENT WITHIN THE PERIOD OF INVESTIGATION TO INCLUDE SEASONAL, HOLIDAY, CHRISTMAS, PART-TIME, AND TEMPORARY EMPLOYMENT. INTERVIEW ONE SUPERVISOR AND ONE CO-WORKER AT SUBJECT'S CURRENT PLACE OF EMPLOYMENT AS WELL AS AT EACH PRIOR PLACE OF EMPLOYMENT DURING THE PAST 10 YEARS OF SIX MONTHS DURATION OR LONGER. THE INTERVIEW REQUIREMENT FOR SUPERVISORS AND CO-WORKERS DOES NOT APPLY TO SEASONAL, HOLIDAY, CHRISTMAS, PART-TIME, AND TEMPORARY EMPLOYMENT (4 MONTHS OR LESS) UNLESS THERE ARE UNFAVORABLE ISSUES TO RESOLVE OR THE LETTER OF INQUIRY PROVIDES INSUFFICIENT INFORMATION.

(2) FEDERAL EMPLOYMENT. ALL FEDERAL EMPLOYMENT WILL BE VERIFIED WITHIN THE PERIOD OF INVESTIGATION TO INCLUDE CHRISTMAS, SEASONAL TEMPORARY, SUMMER HIRE, PART-TIME, AND HOLIDAY EMPLOYMENT. DO NOT VERIFY FEDERAL EMPLOYMENT THROUGH REVIEW OF RECORDS IF ALREADY VERIFIED BY THE REQUESTER. IF FEDERAL EMPLOYMENT HAS NOT BEEN VERIFIED BY THE REQUESTER, THEN SUBJECT'S PERSONNEL FILE AT HIS/HER CURRENT PLACE OF EMPLOYMENT WILL BE REVIEWED. ALL PREVIOUS FEDERAL EMPLOYMENT WILL BE VERIFIED DURING THIS REVIEW. IN THE CASE OF FORMER FEDERAL EMPLOYEES, RECORDS SHALL BE EXAMINED AT THE FEDERAL RECORDS CENTER IN ST. LOUIS, MISSOURI. INTERVIEW ONE SUPERVISOR AND ONE CO-WORKER AT ALL PLACES OF EMPLOYMENT DURING THE PAST 10 YEARS IF SO EMPLOYED FOR 6 MONTHS OR MORE.

(3) MILITARY EMPLOYMENT. MILITARY SERVICE FOR THE LAST 10 YEARS SHALL BE VERIFIED. THE SUBJECT'S DUTY STATION, FOR THE PURPOSE OF INTERVIEW COVERAGE, IS CONSIDERED AS A PLACE OF EMPLOYMENT. ONE SUPERVISOR AND ONE CO-WORKER SHALL BE INTERVIEWED AT SUBJECT'S CURRENT DUTY STATION IF SUBJECT HAS BEEN STATIONED THERE FOR 6 MONTHS OR MORE; ADDITIONALLY, A SUPERVISOR AND A CO-WORKER AT SUBJECT'S PRIOR DUTY STATIONS WHERE ASSIGNED FOR 6 MONTHS OR MORE DURING THE PAST 5 YEARS SHALL BE INTERVIEWED. DO NOT VERIFY MILITARY EMPLOYMENT THROUGH REVIEW OF LOCAL RECORDS IF ALREADY VERIFIED BY THE REQUESTER.

(4) UNEMPLOYMENT. SUBJECT'S ACTIVITIES DURING ALL PERIODS OF UNEMPLOYMENT IN EXCESS OF 60 CONSECUTIVE DAYS, WITHIN THE PERIOD OF INVESTIGATION, THAT ARE NOT OTHERWISE ACCOUNTED FOR SHALL BE DETERMINED.

(5) WHEN AN INDIVIDUAL HAS RESIDED OUTSIDE THE U.S. CONTINUOUSLY FOR OVER ONE YEAR, ATTEMPTS WILL BE MADE TO CONFIRM OVERSEAS EMPLOYMENTS AS WELL AS CONDUCT REQUIRED INTERVIEWS OF A SUPERVISOR AND CO-WORKER.

I. REFERENCES: FOUR REQUIRED (AT LEAST THREE OF WHICH ARE DEVELOPED). TO THE EXTENT PRACTICAL, ALL SHOULD HAVE SOCIAL KNOWLEDGE OF SUBJECT AND COLLECTIVELY SPAN THE ENTIRE SCOPE OF THE INVESTIGATION. AS APPROPRIATE, ADDITIONAL INTERVIEWS MAY INCLUDE COHABITANTS(S), EX-SPOUSES, AND RELATIVE(S). INTERVIEWS WITH PSYCHOLOGICAL/MEDICAL PERSONNEL ARE TO BE ACCOMPLISHED AS REQUIRED TO RESOLVE ISSUES. THREE DEVELOPED CHARACTER REFERENCES WHO HAVE SUFFICIENT KNOWLEDGE OF SUBJECT TO COMMENT ON HIS BACKGROUND, SUITABILITY, AND LOYALTY SHALL BE INTERVIEWED. EFFORTS SHALL BE MADE TO INTERVIEW DEVELOPED REFERENCES WHOSE COMBINED ASSOCIATION WITH SUBJECT COVERS THE FULL PERIOD OF THE INVESTIGATION WITH PARTICULAR EMPHASIS ON THE LAST 5 YEARS. EMPLOYMENT, EDUCATION, AND NEIGHBORHOOD REFERENCES, IN ADDITION TO THE REQUIRED ONES, MAY BE USED AS DEVELOPED REFERENCES PROVIDED THAT THEY HAVE PERSONAL KNOWLEDGE CONCERNING THE INDIVIDUAL'S CHARACTER, DISCRETION, AND LOYALTY. A LISTED CHARACTER REFERENCE WILL BE INTERVIEWED ONLY WHEN DEVELOPED REFERENCES ARE NOT AVAILABLE OR WHEN IT IS NECESSARY TO IDENTIFY AND LOCATE ADDITIONAL DEVELOPED CHARACTER REFERENCES OR WHEN IT IS NECESSARY TO VERIFY SUBJECT'S ACTIVITIES (E.G., UNEMPLOYMENT).

J. NEIGHBORHOOD: INTERVIEWS WITH NEIGHBORS FOR THE LAST FIVE YEARS IF RESIDENCE EXCEEDS SIX MONTHS. CONFIRMATION OF CURRENT RESIDENCE SHALL BE ACCOMPLISHED REGARDLESS OF LENGTH TO INCLUDE REVIEW OF RENTAL RECORDS IF NECESSARY. IN THE EVENT NO RESIDENCE EXCEEDS SIX MONTHS, INTERVIEW OF NEIGHBORS SHOULD BE UNDERTAKEN AT CURRENT RESIDENCE. DURING EACH NEIGHBORHOOD INVESTIGATION, INTERVIEW TWO NEIGHBORS WHO CAN VERIFY SUBJECT'S PERIOD OF RESIDENCE IN THAT AREA AND WHO WERE SUFFICIENTLY ACQUAINTED TO COMMENT ON

SUBJECT'S SUITABILITY FOR A POSITION OF TRUST. NEIGHBORHOOD INVESTIGATIONS WILL BE EXPANDED BEYOND THIS 5-YEAR PERIOD ONLY WHEN THERE IS UNFAVORABLE INFORMATION TO RESOLVE IN THE INVESTIGATION. NEIGHBORHOOD INVESTIGATIONS ARE NOT REQUIRED OUTSIDE THE UNITED STATES AND PUERTO RICO.

K. CREDIT: VERIFICATION OF THE SUBJECT'S FINANCIAL STATUS AND CREDIT HABITS AT ALL LOCATIONS WHERE SUBJECT HAS RESIDED, BEEN EMPLOYED, OR ATTENDED SCHOOL FOR SIX MONTHS OR MORE FOR THE LAST SEVEN (7) YEARS. CONDUCT CREDIT BUREAU CHECK IN THE 50 STATES, THE DISTRICT OF COLUMBIA, PUERTO RICO AND OVERSEAS (WHERE APO/FPO ADDRESSES ARE PROVIDED) AT ALL PLACES WHERE SUBJECT HAS RESIDED (INCLUDING DUTY STATIONS AND HOME PORTS), BEEN EMPLOYED, OR ATTENDED SCHOOL FOR 6 MONTHS OR MORE, ON A CUMULATIVE BASIS, DURING THE LAST 7 YEARS OR DURING THE PERIOD OF THE INVESTIGATION, WHICHEVER IS SHORTER. FINANCIAL RESPONSIBILITY, INCLUDING UNEXPLAINED AFFLUENCE, WILL BE STRESSED IN ALL REFERENCE INTERVIEWS.

L. LOCAL AGENCY CHECKS: A CHECK OF APPROPRIATE POLICE RECORDS, INCLUDING STATE CENTRAL CRIMINAL HISTORY RECORD REPOSITORIES, COVERING ALL LOCATIONS WHERE SUBJECT HAS RESIDED, BEEN EMPLOYED, OR ATTENDED SCHOOL FOR SIX MONTHS OR MORE DURING THE SCOPE OF INVESTIGATION, TO INCLUDE CURRENT RESIDENCE REGARDLESS OF DURATION. IN THE EVENT THAT NO RESIDENCE, EMPLOYMENT, OR EDUCATION EXCEEDS SIX MONTHS, LOCAL AGENCY CHECKS SHOULD BE CONDUCTED AT THE CURRENT RESIDENCE, CURRENT EMPLOYMENT, AND LAST EDUCATIONAL INSTITUTION ATTENDED.

M. FOREIGN TRAVEL. IF SUBJECT HAS BEEN EMPLOYED, EDUCATED, TRAVELED OR RESIDED OUTSIDE OF THE U.S. FOR MORE THAN 90 DAYS DURING THE PERIOD OF INVESTIGATION, EXCEPT UNDER THE AUSPICES OF THE U.S. GOVERNMENT, ADDITIONAL RECORD CHECKS DURING THE NAC SHALL BE MADE IN ACCORDANCE WITH PARAGRAPH 1.F. OF THIS APPENDIX. IN ADDITION, THE FOLLOWING REQUIREMENTS APPLY:

(1) FOREIGN TRAVEL NOT UNDER THE AUSPICES OF THE U.S. GOVERNMENT. WHEN EMPLOYMENT, EDUCATION, OR RESIDENCE HAS OCCURRED OVERSEAS FOR MORE THAN 90 DAYS DURING THE PAST 10 YEARS OR SINCE AGE 18, WHICH WAS NOT UNDER THE AUSPICES OF THE U.S. GOVERNMENT, A CHECK OF RECORDS WILL BE MADE AT THE PASSPORT OFFICE OF THE DEPARTMENT OF STATE AND OTHER APPROPRIATE AGENCIES. EFFORTS SHALL BE MADE TO DEVELOP SOURCES, GENERALLY IN THE U.S., WHO KNEW THE INDIVIDUAL OVERSEAS TO COVER SIGNIFICANT EMPLOYMENT, EDUCATION, OR RESIDENCE AND TO DETERMINE WHETHER THE INDIVIDUAL HAS WORKED OR LIVED OUTSIDE OF THE U.S. CONTINUOUSLY FOR OVER ONE YEAR, THE INVESTIGATION WILL BE EXPANDED TO COVER FULLY THIS PERIOD THROUGH THE USE OF SUCH INVESTIGATIVE ASSETS AND CHECKS OF RECORD SOURCES AS MAY BE AVAILABLE TO THE U.S. GOVERNMENT IN THE FOREIGN COUNTRY IN WHICH THE INDIVIDUAL RESIDED.

(2) FOREIGN TRAVEL UNDER THE AUSPICES OF THE U.S. GOVERNMENT. WHEN EMPLOYMENT, EDUCATION, OR RESIDENCE HAS OCCURRED OVERSEAS FOR A PERIOD OF MORE THAN ONE YEAR, UNDER THE AUSPICES OF THE U.S. GOVERNMENT, A RECORD CHECK WILL BE MADE AT THE PASSPORT OFFICE OF THE DEPARTMENT OF STATE AND OTHER APPROPRIATE AGENCIES. EFFORTS SHALL BE MADE TO DEVELOP SOURCES (GENERALLY IN THE U.S.) WHO KNEW THE INDIVIDUAL OVERSEAS TO COVER SIGNIFICANT EMPLOYMENT, EDUCATION, OR RESIDENCE AND TO DETERMINE WHETHER ANY LASTING FOREIGN CONTACTS OR CONNECTIONS WERE ESTABLISHED DURING THIS PERIOD. ADDITIONALLY, THE INVESTIGATION WILL BE EXPANDED TO COVER FULLY THIS PERIOD THROUGH THE USE OF SUCH INVESTIGATIVE ASSETS AND CHECKS OF RECORD SOURCES AS MAY BE AVAILABLE TO THE U.S. GOVERNMENT IN THE FOREIGN COUNTRY IN WHICH THE INDIVIDUAL RESIDED.

N. FOREIGN CONNECTIONS. ALL FOREIGN CONNECTIONS (FRIENDS, RELATIVES, AND/OR BUSINESS CONNECTIONS) OF SUBJECT AND IMMEDIATE FAMILY IN THE U.S. OR ABROAD, EXCEPT WHERE SUCH ASSOCIATION WAS THE DIRECT RESULT OF SUBJECT'S OFFICIAL DUTIES WITH THE U.S. GOVERNMENT, SHALL BE ASCERTAINED. INVESTIGATION SHALL BE DIRECTED TOWARD DETERMINING THE SIGNIFICANCE OF FOREIGN CONNECTIONS OF THE PART OF SUBJECT AND THE IMMEDIATE FAMILY, PARTICULARLY WHERE THE ASSOCIATION IS OR HAS BEEN WITH PERSONS WHOSE ORIGIN WAS WITHIN A COUNTRY WHOSE NATIONAL INTERESTS ARE INIMICAL TO THOSE OF THE U.S.

O. ORGANIZATIONS. EFFORTS WILL BE MADE DURING REFERENCE INTERVIEWS AND RECORD REVIEWS TO DETERMINE IF SUBJECT AND/OR THE IMMEDIATE FAMILY HAS, OR FORMERLY HAD, MEMBERSHIP IN, AFFILIATION WITH, SYMPATHETIC ASSOCIATION TOWARDS, OR PARTICIPATED IN ANY FOREIGN OR DOMESTIC ORGANIZATION, ASSOCIATION, MOVEMENT, GROUP, OR COMBINATION OF PERSONS OF THE TYPE DESCRIBED IN PARAGRAPHS 2-200 A. THROUGH D. OF THIS REGULATION.

P. MILITARY SERVICE. ALL MILITARY SERVICE AND TYPES OF DISCHARGE DURING THE LAST 10 YEARS SHALL BE VERIFIED.

Q. MEDICAL RECORDS. MEDICAL RECORDS SHALL NOT BE REVIEWED UNLESS:

(1) THE REQUESTER INDICATES THAT SUBJECT'S MEDICAL RECORDS WERE UNAVAILABLE FOR REVIEW PRIOR TO SUBMITTING THE REQUEST FOR INVESTIGATION, OR

(2) THE REQUESTER INDICATES THAT UNFAVORABLE INFORMATION IS CONTAINED IN SUBJECT'S MEDICAL RECORDS, OR

(3) THE SUBJECT LISTS ONE OR MORE OF THE FOLLOWING ON THE PSQ:

(A) A HISTORY OF MENTAL OR NERVOUS DISORDERS.

(B) THAT SUBJECT IS NOW OR HAS BEEN ADDICTED TO THE USE OF HABIT-FORMING DRUGS SUCH AS NARCOTICS OR BARBITURATES OR IS NOW OR HAS BEEN A CHRONIC USER TO EXCESS OF ALCOHOLIC BEVERAGES.

R. PUBLIC RECORDS: VERIFICATION OF DIVORCE(S), BANKRUPTCY, ETC., AND ANY OTHER COURT (CIVIL OR CRIMINAL) ACTIONS TO WHICH SUBJECT HAS BEEN OR IS A PARTY WITHIN THE SCOPE OF INVESTIGATION, WHEN KNOWN OR DEVELOPED. DIVORCES, ANNULMENTS, AND LEGAL SEPARATIONS OF SUBJECT SHALL BE VERIFIED ONLY WHEN THERE IS REASON TO BELIEVE THAT THE GROUNDS FOR THE ACTION COULD REFLECT ON SUBJECT'S SUITABILITY FOR A POSITION OF TRUST.

S. EX-SPOUSE INTERVIEW. IF THE SUBJECT OF INVESTIGATION IS DIVORCED, THE EX-SPOUSE WILL BE INTERVIEWED WHEN THE DATE OF FINAL DIVORCE ACTION IS WITHIN THE SCOPE OF INVESTIGATION.

T. POLYGRAPH: AGENCIES WITH POLICIES SANCTIONING THE USE OF THE POLYGRAPH FOR PERSONNEL SECURITY PURPOSES MAY REQUIRE POLYGRAPH EXAMINATIONS WHEN DEEMED NECESSARY.

U. SELECT SCOPING. WHEN THE FACTS OF THE CASE WARRANT, ADDITIONAL SELECT SCOPING WILL BE ACCOMPLISHED, AS NECESSARY, TO FULLY DEVELOP OR RESOLVE AN ISSUE.

V. TRANSFERABILITY: INVESTIGATIONS SATISFYING THE SCOPE AND STANDARDS SPECIFIED ABOVE ARE TRANSFERABLE BETWEEN AGENCIES AND SHALL BE DEEMED TO MEET THE INVESTIGATIVE STANDARDS FOR ACCESS TO COLLATERAL TOP SECRET/NATIONAL SECURITY INFORMATION AND SENSITIVE COMPARTMENTED INFORMATION. NO FURTHER INVESTIGATION OR REINVESTIGATION PRIOR TO REVALIDATION EVERY FIVE YEARS WILL BE UNDERTAKEN UNLESS THE AGENCY HAS SUBSTANTIAL INFORMATION INDICATING THAT THE TRANSFERRING INDIVIDUAL MAY NOT SATISFY ELIGIBILITY STANDARDS FOR CLEARANCE OR THE AGENCY HEAD DETERMINES IN WRITING THAT TO ACCEPT THE INVESTIGATION WOULD NOT BE IN THE NATIONAL SECURITY INTEREST OF THE UNITED STATES.

W. UPDATING A PREVIOUS INVESTIGATION TO SSBI STANDARDS. IF A PREVIOUS INVESTIGATION DOES NOT SUBSTANTIALLY MEET THE MINIMUM STANDARDS OF AN SSBI OR IF IT IS MORE THAN 5 YEARS OLD, A CURRENT INVESTIGATION IS REQUIRED BUT MAY BE LIMITED TO THAT NECESSARY TO BRING THE INDIVIDUAL'S FILE UP TO DATE IN ACCORDANCE WITH THE INVESTIGATIVE REQUIREMENTS OF AN SSBI. SHOULD NEW INFORMATION BE DEVELOPED DURING THE CURRENT INVESTIGATION THAT BEARS UNFAVORABLY UPON THE INDIVIDUAL'S ACTIVITIES COVERED BY THE PREVIOUS INVESTIGATION, THE CURRENT INQUIRIES SHALL BE EXPANDED AS NECESSARY TO DEVELOP FULL DETAILS OF THIS NEW INFORMATION.

3. PERIODIC REINVESTIGATION (PR)

A. EACH DOD MILITARY, CIVILIAN, CONSULTANT, AND CONTRACTOR EMPLOYEE OCCUPYING A CRITICAL SENSITIVE POSITION OR POSSESSING A TOP SECRET CLEARANCE, OR OCCUPYING A SPECIAL ACCESS PROGRAM POSITION AND NON-U.S. CITIZENS (FOREIGN NATIONALS AND/OR IMMIGRANT ALIENS) HOLDING A LIMITED ACCESS AUTHORIZATION SHALL BE THE SUBJECT OF A PR INITIATED 5 YEARS FROM THE DATE OF COMPLETION OF THE LAST INVESTIGATION. THE PR SHALL COVER THE PERIOD OF THE LAST 5 YEARS.

B. MINIMUM INVESTIGATIVE REQUIREMENTS. A PR SHALL INCLUDE THE FOLLOWING MINIMUM SCOPE.

(1) NAC. A VALID NAC ON THE SUBJECT WILL BE CONDUCTED IN ALL CASES (NOTE: ONLY A NAME CHECK OF THE FBI/ID WILL BE CONDUCTED UNLESS RECORDS INDICATE THAT A TECHNICAL FINGERPRINT CHECK WAS NOT DONE PREVIOUSLY). CHECKS OF DCII, FBI/HQ, FBI/ID NAME CHECK ONLY, AND OTHER AGENCIES DEEMED APPROPRIATE, WILL BE CONDUCTED ON THE SUBJECT'S CURRENT SPOUSE OR COHABITANT, IF NOT PREVIOUSLY CONDUCTED. ADDITIONALLY, NACs WILL BE CONDUCTED ON IMMEDIATE FAMILY MEMBERS, 18 YEARS OF AGE OR OLDER, WHO ARE NON-U.S. CITIZENS, IF NOT PREVIOUSLY ACCOMPLISHED.

(2) CREDIT. CREDIT BUREAU CHECKS COVERING ALL PLACES WHERE THE SUBJECT RESIDED FOR 6 MONTHS OR MORE, ON A CUMULATIVE BASIS, DURING THE PERIOD OF INVESTIGATION, IN THE 50 STATES, DISTRICT OF COLUMBIA, PUERTO RICO AND OVERSEAS (WHERE APO/FPO ADDRESSES ARE PROVIDED), WILL BE CONDUCTED.

(3) SUBJECT INTERVIEW. THE INTERVIEW SHOULD COVER THE ENTIRE PERIOD OF TIME SINCE THE LAST INVESTIGATION, NOT JUST THE LAST 5-YEAR PERIOD. SIGNIFICANT INFORMATION DISCLOSED DURING THE INTERVIEW, WHICH HAS BEEN SATISFACTORILY COVERED DURING A PREVIOUS INVESTIGATION, SHOULD NOT BE EXPLORED AGAIN UNLESS ADDITIONAL RELEVANT INFORMATION WARRANTS FURTHER COVERAGE.

(4) EMPLOYMENT. CURRENT EMPLOYMENT WILL BE VERIFIED. MILITARY AND FEDERAL SERVICE RECORDS WILL NOT ROUTINELY BE CHECKED, IF PREVIOUSLY CHECKED BY THE REQUESTER WHEN THE PR WAS ORIGINALLY SUBMITTED. ALSO, EMPLOYMENT RECORDS

WILL BE CHECKED WHEREVER EMPLOYMENT INTERVIEWS ARE CONDUCTED. RECORDS NEED BE CHECKED ONLY WHEN THEY ARE LOCALLY AVAILABLE, UNLESS UNFAVORABLE INFORMATION HAD BEEN DETECTED.

(5) EMPLOYMENT REFERENCES. TWO SUPERVISORS OR CO-WORKERS AT THE MOST RECENT PLACE OF EMPLOYMENT OR DUTY STATION OF 6 MONTHS; IF THE CURRENT EMPLOYMENT IS LESS THAN 6 MONTHS EMPLOYMENT REFERENCE INTERVIEWS WILL BE CONDUCTED AT THE NEXT PRIOR PLACE OF EMPLOYMENT, WHICH WAS AT LEAST A 6-MONTH DURATION.

(6) DEVELOPED CHARACTER REFERENCES (DCRS). TWO DEVELOPED CHARACTER REFERENCES WHO ARE KNOWLEDGEABLE OF THE SUBJECT WILL BE INTERVIEWED. DEVELOPED CHARACTER REFERENCES WHO WERE PREVIOUSLY INTERVIEWED WILL ONLY BE REINTERVIEWED WHEN OTHER DEVELOPED REFERENCES ARE NOT AVAILABLE.

(7) LOCAL AGENCY CHECKS (LACs). DIS WILL CONDUCT LOCAL AGENCY CHECKS ON THE SUBJECT AT ALL PLACES OF RESIDENCE, EMPLOYMENT, AND EDUCATION DURING THE PERIOD OF INVESTIGATION, REGARDLESS OF DURATION, INCLUDING OVERSEAS LOCATIONS (EXCEPT OVERSEAS LOCATIONS FROM WHICH MILITARY MEMBERS HAVE TRANSFERRED).

(8) NEIGHBORHOOD INVESTIGATION. CONDUCT A NEIGHBORHOOD INVESTIGATION TO VERIFY SUBJECT'S CURRENT RESIDENCE IN THE UNITED STATES. TWO NEIGHBORS WHO CAN VERIFY SUBJECT'S PERIOD OF RESIDENCE IN THAT AREA AND WHO ARE SUFFICIENTLY ACQUAINTED TO COMMENT ON THE SUBJECT'S SUITABILITY FOR A POSITION OF TRUST WILL BE INTERVIEWED. NEIGHBORHOOD INVESTIGATIONS WILL BE EXPANDED BEYOND THE CURRENT RESIDENCE WHEN UNFAVORABLE INFORMATION ARISES.

(9) EX-SPOUSE INTERVIEW. IF THE SUBJECT OF INVESTIGATION IS DIVORCED, THE EX-SPOUSE WILL BE INTERVIEWED WHEN THE DATE OF FINAL DIVORCE ACTION IS WITHIN THE PERIOD OF INVESTIGATION.

(10) POLYGRAPH: AGENCIES WITH POLICIES SANCTIONING THE USE OF THE POLYGRAPH FOR PERSONNEL SECURITY PURPOSES MAY REQUIRE POLYGRAPH EXAMINATIONS WHEN DEEMED NECESSARY.

(11) SELECT SCOPING. WHEN THE FACTS OF THE CASE WARRANT, ADDITIONAL SELECT SCOPING WILL BE ACCOMPLISHED, AS NECESSARY, TO FULLY DEVELOP OR RESOLVE AN ISSUE.

4. SECRET PERIODIC REINVESTIGATION (S-PR)

A. EACH DOD MILITARY, CIVILIAN, CONSULTANT, AND CONTRACTOR EMPLOYEE WITH CURRENT ACCESS TO SECRET INFORMATION SHALL BE THE SUBJECT OF A S-PR INITIATED 10 YEARS FROM THE DATE OF COMPLETION OF THE LAST INVESTIGATION. THE PR SHALL COVER THE PERIOD OF THE LAST 5 YEARS.

B. MINIMUM INVESTIGATIVE REQUIREMENTS. THE S-PR SHALL INCLUDE THE FOLLOWING MINIMUM SCOPE.

(1) NAC. A NAC WITH A NAME CHECK OF THE FBI IDENTIFICATION DIVISION, A CHECK OF THE FBI INVESTIGATIVE FILES, AS WELL AS OTHER AGENCIES' INDICES, E.G. DOD, OPM, CIA, STATE, INS, ETC., AS APPROPRIATE. (NOTE: A TECHNICAL FINGERPRINT CHECK OF THE FBI IDENTIFICATION DIVISION WILL BE CONDUCTED VICE A NAME CHECK IF ONE WAS NOT DONE PREVIOUSLY);

(2) CREDIT. CONDUCT CREDIT BUREAU CHECKS AT ALL LOCATIONS WHERE SUBJECT HAS RESIDED, BEEN EMPLOYED, OR ATTENDED AN INSTITUTION OF HIGHER LEARNING FOR A PERIOD OF SIX MONTHS OR MORE DURING THE PERIOD OF COVERAGE;

(3) THE INVESTIGATION MAY BE EXPANDED AS NECESSARY TO FULLY DEVELOP OR RESOLVE AN ISSUE.

APPENDIX C
REQUEST PROCEDURES

A. GENERAL

TO CONSERVE INVESTIGATIVE RESOURCES AND TO INSURE THAT PERSONNEL SECURITY INVESTIGATIONS ARE LIMITED TO THOSE ESSENTIAL TO CURRENT OPERATIONS AND ARE CLEARLY AUTHORIZED BY DOD POLICIES, ORGANIZATIONS REQUESTING INVESTIGATIONS MUST ASSURE THAT CONTINUING COMMAND ATTENTION IS GIVEN TO THE INVESTIGATIVE REQUEST PROCESS.

IN THIS CONNECTION, IT IS PARTICULARLY IMPORTANT THAT THE PROVISION OF EXECUTIVE ORDER 12356 (REFERENCE (J)) REQUIRING STRICT LIMITATIONS ON THE DISSEMINATION OF OFFICIAL INFORMATION AND MATERIAL BE CLOSELY ADHERED TO AND THAT INVESTIGATIONS REQUESTED FOR ISSUING CLEARANCES ARE LIMITED TO THOSE INSTANCES IN WHICH AN INDIVIDUAL HAS A CLEAR NEED FOR ACCESS TO CLASSIFIED INFORMATION. SIMILARLY, INVESTIGATIONS REQUIRED TO DETERMINE ELIGIBILITY FOR APPOINTMENT OR RETENTION IN DOD, IN EITHER A CIVILIAN OR MILITARY CAPACITY, MUST NOT BE REQUESTED IN FREQUENCY OR SCOPE EXCEEDING THAT PROVIDED FOR IN THIS REGULATION.

IN VIEW OF THE FOREGOING, THE FOLLOWING GUIDELINES HAVE BEEN DEVELOPED TO SIMPLIFY AND FACILITATE THE INVESTIGATIVE REQUEST PROCESS:

1. LIMIT REQUESTS FOR INVESTIGATION TO THOSE THAT ARE ESSENTIAL TO CURRENT OPERATIONS AND CLEARLY AUTHORIZED BY DOD POLICIES AND ATTEMPT TO UTILIZE INDIVIDUALS WHO, UNDER THE PROVISIONS OF THIS REGULATION, HAVE ALREADY MET THE SECURITY STANDARD;
2. ASSURE THAT MILITARY PERSONNEL ON WHOM INVESTIGATIVE REQUESTS ARE INITIATED WILL HAVE SUFFICIENT TIME REMAINING IN SERVICE AFTER COMPLETION OF THE INVESTIGATION TO WARRANT CONDUCTING IT;
3. INSURE THAT REQUEST FORMS AND PRESCRIBED DOCUMENTATION ARE PROPERLY EXECUTED IN ACCORDANCE WITH INSTRUCTIONS;
4. DISPATCH THE REQUEST DIRECTLY TO THE DIS PERSONNEL INVESTIGATIONS CENTER;
5. PROMPTLY NOTIFY THE DIS PERSONNEL INVESTIGATIONS CENTER IF THE INVESTIGATION IS NO LONGER NEEDED (NOTIFY OPM IF A NACI IS NO LONGER NEEDED); AND
6. LIMIT ACCESS THROUGH STRICT NEED-TO-KNOW, THEREBY REQUIRING FEWER INVESTIGATIONS.

IN SUMMARY, CLOSE OBSERVANCE OF THE ABOVE-CITED GUIDELINES WILL ALLOW THE DIS TO OPERATE MORE EFFICIENTLY AND PERMIT MORE EFFECTIVE, TIMELY, AND RESPONSIVE SERVICE IN ACCOMPLISHING INVESTIGATIONS.

In addition to the guidelines in this section, requesters must ensure before requesting a security investigation (1) that a current (conducted

with the past five years), complete investigative file is not available from any other department or agency of the Federal government with respect to the individual and (2) that no other department or agency of the Federal government is conducting an investigation with respect to that individual that could be used as a basis for determining whether to grant a security clearance. A confirmation that another agency/department is not processing the subject for security clearance must be shown on the DD Form 1879 used to request the investigation from DIS.

B. NATIONAL AGENCY CHECK (NAC)

WHEN A NAC IS REQUESTED AN ORIGINAL ONLY OF THE DD FORM 398-2 (NATIONAL AGENCY CHECK REQUEST) AND A COMPLETED FD 258 (APPLICANT FINGERPRINT CARD) ARE REQUIRED. IF THE REQUEST IS FOR AN ENTNAC, AN ORIGINAL ONLY OF THE DD FORM 398-2 AND A COMPLETED DD FORM 2280 (ARMED FORCES FINGERPRINT CARD) ARE REQUIRED. THOSE FORMS SHOULD BE SENT DIRECTLY TO:

PERSONNEL INVESTIGATION CENTER

DEFENSE INVESTIGATIVE SERVICE

P.O. BOX 1083

BALTIMORE, MARYLAND 21203

C. NATIONAL AGENCY CHECK PLUS WRITTEN INQUIRIES (NACI)

WHEN A NACI IS REQUESTED, AN ORIGINAL AND ONE COPY OF THE SF 85 (DATA FOR NONSENSITIVE OR NONCRITICAL-SENSITIVE POSITION), AN SF 171 (PERSONAL QUALIFICATIONS STATEMENT), AND AN SF 87 (U.S. CIVIL SERVICE COMMISSION FINGERPRINT CHART) SHALL BE SENT DIRECTLY TO:

OFFICE OF PERSONNEL MANAGEMENT

BUREAU OF PERSONNEL INVESTIGATIONS

NACI CENTER

BOYERS, PENNSYLVANIA 16018

THE NOTATION "ALL REFERENCES" SHALL BE STAMPED IMMEDIATELY ABOVE THE TITLE AT THE TOP OF THE STANDARD FORM 85.

D. DOD NATIONAL AGENCY CHECK WITH INQUIRIES (DNACI)

1. WHEN A DNACI IS REQUESTED, ONE COPY OF THE DD FORM 1879, AN ORIGINAL AND TWO COPIES OF THE DD FORM 398-2 (NATIONAL AGENCY CHECK REQUEST), TWO COPIES OF FD 258 (FINGERPRINT CARD), AND AN ORIGINAL OF DD FORM 2221 (AUTHORITY FOR RELEASE OF INFORMATION AND RECORDS) SHALL BE SENT DIRECTLY TO:

PERSONNEL INVESTIGATIONS CENTER

DEFENSE INVESTIGATIVE SERVICE

P.O. BOX 1083

BALTIMORE, MARYLAND 21203

2. THE DD FORM 398-2 MUST BE COMPLETED TO COVER THE MOST RECENT FIVE YEAR PERIOD. ALL INFORMATION, TO INCLUDE ITEMS RELATIVE TO RESIDENCES AND EMPLOYMENT, MUST BE COMPLETE AND ACCURATE TO AVOID DELAYS IN PROCESSING.

MARCH 1996

E. SPECIAL BACKGROUND INVESTIGATION (SBI)/BACKGROUND INVESTIGATION (BI)

1. WHEN REQUESTING A BI OR SBI, ONE COPY OF DD FORM 1879 (REQUEST FOR PERSONNEL SECURITY INVESTIGATION), AN ORIGINAL AND FOUR COPIES OF DD FORM 398 (STATEMENT OF PERSONNEL HISTORY), TWO COPIES OF FD-258, AND AN ORIGINAL OF DD FORM 2221 (AUTHORITY FOR RELEASE OF INFORMATION AND RECORDS) SHALL BE SENT DIRECTLY TO THE:

PERSONNEL INVESTIGATIONS CENTER

DEFENSE INVESTIGATIVE SERVICE

P.O. BOX 454

BALTIMORE, MARYLAND 21203

2. FOR THE BI AND SBI, THE DD FORM 398 MUST BE COMPLETED TO COVER THE MOST RECENT FIVE AND 15 YEAR PERIOD, RESPECTIVELY, OR SINCE THE 18TH BIRTHDAY, WHICHEVER IS SHORTER.

National Security Decision Directive No. 63 established the Single Scope Background Investigation (SSBI) which replaced the BI and SBI. See Appendix B for scoping of the SSBI. The SSBI is the standard investigative prerequisite for access to Top Secret, sensitive compartmented information, and employment in critical sensitive positions. When requesting a SSBI, the DD Form 1879 must be accompanied by the following:

Original and four copies of SF-85P (for positions of trust when the incumbent will not require access to classified information) or 86 (when the incumbent will require access to classified information).

FD 258 (2 copies)

F. PERIODIC REINVESTIGATION (PR)

1. PRs SHALL BE REQUESTED ONLY IN SUCH CASES AS ARE AUTHORIZED BY PARAGRAPHS 3-700 THROUGH 3-710 OF THIS REGULATION.

A. FOR A PR REQUESTED IN ACCORDANCE WITH PARAGRAPH 3-700 AND 3-710, THE DD FORM 1879 MUST BE ACCOMPANIED BY THE FOLLOWING DOCUMENTS:

(1) ORIGINAL AND FOUR COPIES OF DD FORM 398.

(2) TWO COPIES OF FD-258. (This requirement was cancelled by OASD(C3I) memorandum dated 9 April 1993, unless it is known that a technical check was not previously completed. See reference 1-100.x.2.)

(3) ORIGINAL COPY OF DD FORM 2221.

B. IN PROCESSING PRs, PREVIOUS INVESTIGATIVE REPORTS WILL NOT BE REQUESTED BY THE REQUESTING ORGANIZATION, UNLESS SIGNIFICANT DEROGATORY OR ADVERSE INFORMATION, POSTDATING THE MOST RECENT FAVORABLE ADJUDICATION, IS DEVELOPED DURING THE COURSE OF REVIEWING OTHER LOCALLY AVAILABLE RECORDS. IN THE LATTER INSTANCE, REQUESTS FOR PREVIOUS INVESTIGATIVE REPORTS MAY ONLY BE MADE IF IT IS DETERMINED BY THE REQUESTING ORGANIZATION THAT THE DEROGATORY INFORMATION IS SO SIGNIFICANT THAT A REVIEW OF PREVIOUS INVESTIGATIVE REPORTS IS NECESSARY FOR CURRENT ADJUDICATIVE DETERMINATIONS.

MARCH 1996

2. NO ABBREVIATED VERSION OF DD FORM 398 MAY BE SUBMITTED IN CONNECTION WITH A PR.

3. THE PR REQUEST SHALL BE SENT TO THE ADDRESS IN PARAGRAPH E.1., ABOVE.

G. ADDITIONAL INVESTIGATION TO RESOLVE DEROGATORY OR ADVERSE INFORMATION

1. REQUESTS FOR ADDITIONAL INVESTIGATION REQUIRED TO RESOLVE DEROGATORY OR ADVERSE INFORMATION SHALL BE SUBMITTED BY DD FORM 1879 (REQUEST FOR PERSONNEL SECURITY INVESTIGATION) TO THE:

DEFENSE INVESTIGATIVE SERVICE

P.O. BOX 454

BALTIMORE, MARYLAND 21203

SUCH REQUESTS SHALL SET FORTH THE BASIS FOR THE ADDITIONAL INVESTIGATION AND DESCRIBE THE SPECIFIC MATTER TO BE SUBSTANTIATED OR DISPROVED.

2. THE REQUEST SHOULD BE ACCOMPANIED BY AN ORIGINAL AND FOUR COPIES OF THE DD FORM 398, WHERE APPROPRIATE, TWO COPIES OF FD-258 AND AN ORIGINAL COPY OF DD FORM 2221, UNLESS SUCH DOCUMENTATION WAS SUBMITTED WITHIN THE LAST 12 MONTHS TO DIS AS PART OF A NAC OR OTHER PERSONNEL SECURITY INVESTIGATION. IF PERTINENT, THE RESULTS OF A RECENTLY COMPLETED NAC, NACI, OR OTHER RELATED INVESTIGATIVE REPORTS AVAILABLE SHOULD ALSO ACCOMPANY THE REQUEST.

H. OBTAINING RESULTS OF PRIOR INVESTIGATIONS

REQUESTERS REQUIRING VERIFICATION OF A SPECIFIED TYPE OF PERSONNEL SECURITY INVESTIGATION, AND/OR REQUIRING COPIES OF PRIOR INVESTIGATIONS CONDUCTED BY THE DIS SHALL SUBMIT REQUESTS BY LETTER OR MESSAGE TO:

DEFENSE INVESTIGATIVE SERVICE INVESTIGATIVE FILES DIVISION

P.O. BOX 1211

BALTIMORE, MARYLAND 21203

MESSAGE ADDRESS: DIS PIC BALTIMORE MD/ /D0640

THE REQUEST WILL INCLUDE SUBJECT'S NAME, GRADE, SOCIAL SECURITY NUMBER, DATE AND PLACE OF BIRTH, AND DIS CASE CONTROL NUMBER IF KNOWN.

I. REQUESTING POSTADJUDICATION CASES

1. REQUESTS PERTAINING TO ISSUES ARISING AFTER ADJUDICATION OF AN INVESTIGATION (POSTADJUDICATION CASES) SHALL BE ADDRESSED TO DIS ON A DD FORM 1879 ACCOMPANIED BY A DD FORM 398, WHERE APPROPRIATE.

2. ALL REQUESTS FOR INITIAL INVESTIGATIONS WILL BE SUBMITTED TO PIC REGARDLESS OF THEIR URGENCY. IF, HOWEVER, THERE IS AN URGENT NEED FOR A POST-ADJUDICATION INVESTIGATION, OR THE MAILING OF A REQUEST TO PIC FOR INITIATION OF A POSTADJUDICATION CASE WOULD PREJUDICE TIMELY PURSUIT OF INVESTIGATIVE ACTION, THE DD FORM 1879 MAY BE DIRECTED FOR INITIATION, IN CONUS, TO THE NEAREST DIS FIELD OFFICE, AND IN OVERSEAS LOCATIONS, TO THE MILITARY INVESTIGATIVE SERVICE

ELEMENT SUPPORTING THE REQUESTER (APPENDIX J). THE FIELD ELEMENT (EITHER DIS OR THE MILITARY INVESTIGATIVE AGENCY) WILL SUBSEQUENTLY FORWARD EITHER THE DD FORM 1879 OR COMPLETED INVESTIGATION TO PIC.

3. A FULLY EXECUTED DD FORM 1879 AND APPROPRIATE SUPPORTING DOCUMENTS MAY NOT BE IMMEDIATELY AVAILABLE. FURTHER, A CASE THAT IS BASED ON SENSITIVE SECURITY ISSUES MAY BE COMPROMISED BY A REQUEST THAT THE SUBJECT SUBMIT A DD FORM 398. A BRIEF EXPLANATION SHOULD APPEAR ON DD FORM 1879 WHICH DOES NOT INCLUDE COMPLETE SUPPORTING DOCUMENTATION.

J. REQUESTS INVOLVING CONTRACTOR EMPLOYEES

TO PRECLUDE DUPLICATIVE INVESTIGATIVE REQUESTS AND DOUBLE HANDLING OF CONTRACTOR EMPLOYEE CASES INVOLVING ACCESS TO CLASSIFIED INFORMATION, ALL REQUESTS FOR INVESTIGATION OF CONTRACTOR PERSONNEL MUST BE SUBMITTED, USING AUTHORIZED INDUSTRIAL SECURITY CLEARANCE FORMS, FOR PROCESSING THROUGH THE DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE, EXCEPT FOR PROGRAMS IN WHICH SPECIFIC APPROVAL HAS BEEN OBTAINED FROM THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY TO UTILIZE OTHER PROCEDURES.

K. RESPONSIBILITY FOR PROPER DOCUMENTATION OF REQUESTS

THE OFFICIAL SIGNING THE REQUEST FOR INVESTIGATION SHALL BE RESPONSIBLE FOR INSURING THAT ALL DOCUMENTATION IS COMPLETED IN ACCORDANCE WITH THESE INSTRUCTIONS.

TABLES FOR REQUESTING INVESTIGATIONS

TABLE 1

GUIDE FOR REQUESTING BACKGROUND INVESTIGATIONS (BI)

A	B	C
If the individual is a:	and duties require:	then a BI is required before:
U.S. national military member, civilian, consultant, or contractor employee	Top Secret clearance	granting final clearance
U.S. national civilian employee	assignment to a "Critical" sensitive position	assignment to the position
U.S. national military member, DoD civilian or contractor employee	occupying a "critical" position in the Nuclear Weapon Personnel Reliability Program (PRP) (reference (a))	occupying a "critical" position
U.S. national military member or civilian employee	granting, denying clearances	performing clearance functions
U.S. national military member or civilian employee	membership on security screening, hearing, or review board	appointment to the board
immigrant alien	limited access to Secret or Confidential information	issuing limited access authorization (Note 1)
non-U.S. national employee excluding immigrant alien	limited access to Secret or Confidential information	issuing limited access authorization
non-U.S. national nominee for military education and orientation program (from a country listed at Appendix H)	education and orientation of military personnel	before performing duties

NOTE 1 - BI will cover a 10 year scope.

TABLE 1 (continued)

A	B	C
<u>If the individual is a:</u>	<u>and duties require:</u>	<u>then a BI is required before:</u>
U.S. national military member, DoD civilian or contractor employee	assignment to a category two Presidential Support position	assignment
U.S. national military member, DoD civilian or contractor employee assigned to NATO	access to NATO COSMIC information	access may be granted

TABLE 2

GUIDE FOR REQUESTING SPECIAL BACKGROUND INVESTIGATIONS (SBI)

A	B	C
<u>If the individual is a:</u>	<u>and duties require:</u>	<u>then a SBI is required before:</u>
U.S. national military member, DoD civilian, consultant, or contractor employee	access to SCI assignment to a category one Presidential Support position access to SIOP-ESI assignment to the National Security Agency access to other Special Access programs approved under paragraph 3-506 assignment to personnel security, counterintelligence, or criminal investigative or direct investigative support duties	granting access assignment granting access assignment granting access assignment

TABLE 3

GUIDE FOR REQUESTING PERIODIC REINVESTIGATIONS (PR)

A	B	C
<u>If the individual is a:</u>	<u>and duties require:</u>	<u>then a PR is required:</u>
U.S. national military member, DoD civilian, consultant, or contractor employee	access to SCI	5 years from date of last SBI/BI or PR
U.S. national civilian employee	Top Secret Clearance	5 years from date of last SBI/BI or PR
Non-U.S. national employee	access to NATO COSMIC	5 years from date of last SBI/BI or PR
	assignment to Presidential Support activities	5 years from date of last SBI/BI or PR
	assignment to a "Critical" sensitive position	5 years from last SBI/BI or PR
	current limited access authorization to Secret or Confidential information	5 years from last SBI/BI or PR

TABLE 4

GUIDE FOR REQUESTING DOD NATIONAL AGENCY CHECK
WITH INQUIRIES (DNACI) OR NACI

A	B	C
<u>If the individual is a:</u>	<u>and duties require:</u>	<u>Then DNACI/NACI is required</u>
U.S. national military member or contractor employee	Secret clearance	before granting clearance (note 1)
U.S. national civilian employee or consultant	Interim Secret clearance	may be automatically issued (note 2)
	Secret clearance	before granting clearance
	Interim Secret Clearance	may be automatically issued (note 3)
U.S. national military member, DoD civilian or contractor employee	Appointment to "Non Critical" sensitive position	before appointment
	occupying a "controlled" positions in the Nuclear Weapon PRR (reference (s))	before assignment
applicant for appointment as a commissioned officer	Commission in the Armed Forces	before appointment (after appointment for health professionals, chaplains, and attorneys, under conditions authorized by paragraph 3-303 of this Regulation)

TABLE 4 (continued)

GUIDE FOR REQUESTING DOD NATIONAL AGENCY CHECK
WITH INQUIRIES (DNACI) OR NACI

A	B	C
<u>If the individual is a:</u>	<u>and duties require:</u>	<u>then a DNACI/NACI is required:</u>
Naval Academy Midshipman, Military Academy Cadet, or Air Force Academy Cadet	enrollment	to be initiated 90 days after entry
Reserve Officer Training Corps Cadet of Midshipman	entry to advanced course or College Scholarship Program	then a DNACI is required to be initiated 90 days after entry

NOTE 1 - First term enlistees shall require an ENTNAC

NOTE 2 - Provided DD Form 398-2 is favorably reviewed, local records check favorably accomplished, and DNACI initiated.

NOTE 3 - Provided an authority designated in Appendix F finds delay in such appointment would be harmful to national security; favorable review of DD Form 398-2; NACI initiated; favorable local records check accomplished.

TABLE 5

GUIDE FOR REQUESTING NATIONAL AGENCY CHECKS (NAC)

A	B	C
<u>If the individual is a:</u>	<u>and duties require:</u>	<u>then a NAC is required:</u>
a first-term enlistee	retention in the Armed Forces (including National Guard and Reserve)	to be initiated NLT three work 3 days after entry (note 1)
prior service member reentering military service after break in Federal employment exceeding 1 year	Retention in the Armed Forces (including National Guard and Reserve)	to be initiated NLT three work days after reentry
nominee for military education and orientation program	education and orientation of military personnel	before performing duties (note 2)
U.S. national military, DoD civilian, or contractor employee	access to restricted areas, sensitive information, or equipment as defined in paragraph 3-601	before authorizing entry
nonappropriated fund instrumentality (NAFI) civilian employee (reference (u))	appointment as NAFI custodian accountability for non appropriated funds	before appointment
Persons requiring access to chemical agents	fiscal responsibility as determined by NAFI custodian other "positions of trust" access to or security of chemical agents	before completion of probationary period before completion of probationary period before appointment before assignment

NOTE: 1 - Request ENTNAC only.

NOTE: 2 - Except where personnel whose country of origin is a country listed at Appendix H, a BI will be required (See Para 3-611)

TABLE 5 (continued)

A	B	C
If the individual is a:	and duties require:	then a NAC is required:
U.S. national, civilian employee nominee for customs inspection duties	waiver under provisions of para 3-603	before appointment (note 3)
Red Cross/United States Organization personnel	assignment with the Armed Forces overseas	before assignment (See note 4 for foreign national personnel)
U.S. national	DoD building pass	prior to issuance
Foreign national employed overseas	no access to classified information	prior to employment (note 4)

NOTE: 3 - A NAC not over 5 years old suffices unless there has been a break in employment over 12 months. Then a current NAC is required.

NOTE: 4 - In such cases, the NAC shall consist of: (a) Host government law enforcement and security agency record checks at the city, state (province), and national level, and (b) DCII.

APPENDIX E

REPORTING OF NONDEROGATORY CASES

BACKGROUND INVESTIGATION (BI) AND SPECIAL BACKGROUND INVESTIGATION (SBI) SHALL BE CONSIDERED AS DEVOID OF SIGNIFICANT ADVERSE INFORMATION UNLESS THEY CONTAIN INFORMATION LISTED BELOW:

1. INCIDENTS, INFRACTIONS, OFFENSES, CHARGES, CITATIONS, ARRESTS, SUSPICION OR ALLEGATIONS OF ILLEGAL USE OR ABUSE OF DRUGS OR ALCOHOL, THEFT OR DISHONESTY, UNRELIABILITY, IRRESPONSIBILITY, IMMATURITY, INSTABILITY OR RECKLESSNESS, THE USE OF FORCE, VIOLENCE OR WEAPONS OR ACTIONS THAT INDICATE DISREGARD FOR THE LAW DUE TO MULTIPLICITY OF MINOR INFRACTIONS.
2. ALL INDICATIONS OF MORAL TURPITUDE, HETEROSEXUAL PROMISCUITY, ABERRANT, DEVIANT, OR BIZARRE SEXUAL CONDUCT OR BEHAVIOR, TRANSVESTITISM, TRANSSEXUALISM, INDECENT EXPOSURE, RAPE, CONTRIBUTING TO THE DELINQUENCY OF A MINOR, CHILD MOLESTATION, WIFE-SWAPPING, WINDOW-PEEPING, AND SIMILAR SITUATIONS FROM WHATEVER SOURCE. UNLISTED FULL-TIME EMPLOYMENT OR EDUCATION; FULL-TIME EDUCATION OR EMPLOYMENT THAT CANNOT BE VERIFIED BY ANY REFERENCE OR RECORD SOURCE OR THAT CONTAINS INDICATIONS OF FALSIFIED EDUCATION OR EMPLOYMENT EXPERIENCE. RECORDS OR TESTIMONY OF EMPLOYMENT, EDUCATION, OR MILITARY SERVICE WHERE THE INDIVIDUAL WAS INVOLVED IN SERIOUS OFFENSES OR INCIDENTS THAT WOULD REFLECT ADVERSELY ON THE HONESTY, RELIABILITY, TRUSTWORTHINESS, OR STABILITY OF THE INDIVIDUAL.
3. FOREIGN TRAVEL, EDUCATION, VISITS, CORRESPONDENCE, RELATIVES, OR CONTACT WITH PERSONS FROM OR LIVING IN A FOREIGN COUNTRY OR FOREIGN INTELLIGENCE SERVICE. [CH2 to DoD 5200.2-R, 7/14/93]
4. MENTAL, NERVOUS, EMOTIONAL, PSYCHOLOGICAL, PSYCHIATRIC, OR CHARACTER DISORDERS/BEHAVIOR OR TREATMENT REPORTED OR ALLEGED FROM ANY SOURCE.
5. EXCESSIVE INDEBTEDNESS, BAD CHECKS, FINANCIAL DIFFICULTIES OR IRRESPONSIBILITY, UNEXPLAINED AFFLUENCE, BANKRUPTCY, OR EVIDENCE OF LIVING BEYOND THE INDIVIDUAL'S MEANS.
6. ANY OTHER SIGNIFICANT INFORMATION RELATING TO THE CRITERIA INCLUDED IN A. THROUGH Q. OF PARAGRAPH 2-200 OR APPENDIX I OF THIS REGULATION.

APPENDIX F

DOD SECURITY CLEARANCE AND/OR SCI ACCESS DETERMINATION AUTHORITIES

A. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE PERSONNEL SECURITY CLEARANCES (TOP SECRET, SECRET, AND CONFIDENTIAL).

1. SECRETARY OF DEFENSE AND/OR SINGLE DESIGNEE
2. SECRETARY OF THE ARMY AND/OR SINGLE DESIGNEE¹
3. SECRETARY OF THE NAVY AND/OR SINGLE DESIGNEE¹
4. SECRETARY OF THE AIR FORCE AND/OR SINGLE DESIGNEE¹
5. CHAIRMAN OF THE JOINT CHIEFS OF STAFF AND/OR SINGLE DESIGNEE
6. DIRECTOR, WASHINGTON HEADQUARTERS SERVICES, AND/OR SINGLE DESIGNEE
7. DIRECTOR, NATIONAL SECURITY AGENCY, AND/OR SINGLE DESIGNEE^{1,2}
8. DIRECTOR, DEFENSE INTELLIGENCE AGENCY, AND/OR SINGLE DESIGNEE¹
9. DEPUTY GENERAL COUNSEL, LEGAL COUNSEL, OGC, AND/OR SINGLE DESIGNEE (FOR CONTRACTORS UNDER THE DEFENSE INDUSTRIAL SECURITY PROGRAM (DISP))
10. DIRECTOR, DEFENSE INVESTIGATIVE SERVICE, AND/OR SINGLE DESIGNEE, (MAY GRANT SECURITY CLEARANCES ONLY FOR CONTRACTOR PERSONNEL UNDER THE DISP)

B. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE LAA.

OFFICIALS LISTED IN SUBSECTION A.1 THROUGH A.10., ABOVE, AND THE COMMANDERS OF THE UNIFIED COMBATANT COMMANDS, OR THEIR SINGLE DESIGNEE, (MUST BE AT GENERAL OFFICER, FLAG RANK OR CIVILIAN EQUIVALENT).

C. OFFICIALS AUTHORIZED TO CERTIFY PERSONNEL UNDER THEIR JURISDICTION FOR ACCESS TO CRITICAL NUCLEAR WEAPON DESIGN INFORMATION.

SEE ENCLOSURE TO DOD DIRECTIVE 5210.2 (REFERENCE (2)). See DCAA Regulation 5210.3, Access to and Dissemination of Restricted Data (reference 1-100 j).

¹ AUTHORITY TO GRANT, DENY OR REVOKE ACCESS TO SCI IS A FUNCTION OF THE SENIOR OFFICIALS OF THE INTELLIGENCE COMMUNITY (SOIC), OR THEIR DESIGNATED REPRESENTATIVE, AS IDENTIFIED IN E.O. 12333 AND DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 1/14. THE AUTHORITY FOR MAKING SCI ACCESS DETERMINATIONS MAY ALSO BE THE SAME OFFICIAL MAKING SECURITY CLEARANCE DETERMINATIONS.

² REFERENCE TO THE DIRECTOR, NSA OR SINGLE DESIGNEE IS NOT INTENDED TO INFRINGE UPON THE AUTHORITIES OR RESPONSIBILITIES CONTAINED IN DOD DIRECTIVE 5210.45, "PERSONNEL SECURITY IN THE NATIONAL SECURITY AGENCY."

D. OFFICIAL AUTHORIZED TO APPROVE PERSONNEL FOR ASSIGNMENT TO PRESIDENTIAL SUPPORT ACTIVITIES.

THE EXECUTIVE SECRETARY TO THE SECRETARY OF DEFENSE AND THE DEPUTY SECRETARY OF DEFENSE, OR DESIGNEE.

E. OFFICIALS AUTHORIZED TO GRANT ACCESS TO SIOP-ESI:

1. DIRECTOR OF STRATEGIC TARGET PLANNING
2. DIRECTOR, JOINT STAFF
3. CHIEF OF STAFF, U.S. ARMY
4. CHIEF OF NAVAL OPERATIONS
5. CHIEF OF STAFF, U.S. AIR FORCE
6. COMMANDANT OF THE MARINE CORPS
7. COMMANDERS OF THE UNIFIED COMBATANT COMMANDS

8. THE AUTHORITY MAY BE FURTHER DELEGATED IN WRITING BY THE OFFICIALS IN SUBSECTIONS E.1. THROUGH E.7. TO THE APPLICABLE SUBORDINATES.

F. THREE MEMBER PSAB SHALL BE FORMED UNDER THE AUSPICES OF THE FOLLOWING OFFICIALS TO RENDER FINAL DETERMINATIONS WHEN AN UNFAVORABLE PERSONNEL SECURITY DETERMINATION IS APPEALED UNDER PARAGRAPH 8-201.D. OF THE REGULATION.

1. SECRETARY OF THE ARMY
2. SECRETARY OF THE AIR FORCE
3. SECRETARY OF THE NAVY
4. CHAIRMAN OF THE JOINT CHIEFS OF STAFF
5. DIRECTOR, NSA
6. DIRECTOR, DIA
7. DIRECTOR, WHS
8. GENERAL COUNSEL, DOD (CONTRACTORS ONLY)

G. OFFICIALS AUTHORIZED TO SUSPEND ACCESS TO CLASSIFIED INFORMATION:

1. SECURITY CLEARANCES.

A. CONTRACTOR PERSONNEL. THE DIRECTOR, COUNTERINTELLIGENCE AND SECURITY PROGRAMS; ODASD (I&S); OASD(C3I) AND THE DEPUTY GENERAL COUNSEL (LEGAL COUNSEL), OFFICE OF GENERAL COUNSEL, OSD

B. MILITARY AND/OR CIVILIAN PERSONNEL, COMMANDER AND/OR AGENCY HEAD, HEAD OF THE COMPONENT, OR ADJUDICATIVE AUTHORITY.

2. SCI:

COGNIZANT SOICs, OR THEIR DESIGNEES.

H. OFFICIALS AUTHORIZED TO ISSUE INTERIM CLEARANCES.

1. INTERIM TOP SECRET CLEARANCES MAY BE ISSUED BY THE OFFICIALS LISTED IN SECTION A., ABOVE. THAT MAY BE FURTHER DELEGATED ON DETERMINATION BY THE HEAD OF THE AGENCY.

2. INTERIM SECRET AND/OR CONFIDENTIAL CLEARANCES MAY BE ISSUED BY THE OFFICIALS LISTED IN SECTION A., ABOVE, AS WELL AS BY ORGANIZATIONAL COMMANDERS. Within DCAA, interim Secret and/or Confidential clearances may be issued by the Director and Agency Security Officer to DCAA personnel.

I. OFFICIALS AUTHORIZED TO DESIGNATE NONAPPROPRIATED FUND POSITIONS OF TRUST:

THE HEADS OF THE DOD COMPONENTS, OR THEIR DESIGNEES.

APPENDIX G

GUIDELINES FOR CONDUCTING PRENOMINATION
PERSONAL INTERVIEWS

A. PURPOSE. THE PURPOSE OF THE PERSONAL INTERVIEW IS TO ASSIST IN DETERMINING THE ACCEPTABILITY OF AN INDIVIDUAL FOR NOMINATION AND FURTHER PROCESSING FOR A POSITION REQUIRING AN SBI.

B. SCOPE. QUESTIONS ASKED DURING THE COURSE OF A PERSONAL INTERVIEW MUST HAVE A RELEVANCE TO A SECURITY DETERMINATION. CARE MUST BE TAKEN NOT TO INJECT IMPROPER MATTERS INTO THE PERSONAL INTERVIEW. FOR EXAMPLE, RELIGIOUS BELIEFS AND AFFILIATIONS, BELIEFS AND OPINIONS REGARDING RACIAL MATTERS, POLITICAL BELIEFS AND AFFILIATIONS OF A NONSUBVERSIVE NATURE, OPINIONS REGARDING THE CONSTITUTIONALITY OF LEGISLATIVE POLICIES, AND AFFILIATIONS WITH LABOR UNIONS AND FRATERNAL ORGANIZATIONS ARE NOT PROPER SUBJECTS FOR INQUIRY. DEPARTMENT OF DEFENSE REPRESENTATIVES CONDUCTING PERSONAL INTERVIEWS SHOULD ALWAYS BE PREPARED TO EXPLAIN THE RELEVANCE OF THEIR INQUIRIES. ADVERSE INFERENCES SHALL NOT BE DRAWN FROM THE REFUSAL OF A PERSON TO ANSWER QUESTIONS THE RELEVANCE OF WHICH HAS NOT BEEN ESTABLISHED.

C. THE INTERVIEWER. EXCEPT AS PRESCRIBED IN PARAGRAPH B. ABOVE, PERSONS CONDUCTING PERSONAL INTERVIEWS NORMALLY WILL HAVE BROAD LATITUDE IN PERFORMING THIS ESSENTIAL AND IMPORTANT FUNCTION AND, THEREFORE, A HIGH PREMIUM MUST NECESSARILY BE PLACED UPON THE EXERCISE OF GOOD JUDGMENT AND COMMON SENSE. TO INSURE THAT PERSONAL INTERVIEWS ARE CONDUCTED IN A MANNER THAT DOES NOT VIOLATE LAWFUL CIVIL AND PRIVATE RIGHTS OR DISCOURAGE LAWFUL POLITICAL ACTIVITY IN ANY OF ITS FORMS, OR INTIMIDATE FREE EXPRESSION, IT IS NECESSARY THAT INTERVIEWERS HAVE A KEEN AND WELL-DEVELOPED AWARENESS OF AND RESPECT FOR THE RIGHTS OF INTERVIEWEES. INTERVIEWERS SHALL NEVER OFFER AN OPINION AS TO THE RELEVANCE OR SIGNIFICANCE OF INFORMATION PROVIDED BY THE INTERVIEWEE TO ELIGIBILITY FOR ACCESS TO SCI. IF EXPLANATION IN THIS REGARD IS REQUIRED, THE INTERVIEWER WILL INDICATE THAT THE SOLE FUNCTION OF THE INTERVIEW IS TO OBTAIN INFORMATION AND THAT THE DETERMINATION OF RELEVANCE OR SIGNIFICANCE TO THE INDIVIDUAL'S ELIGIBILITY WILL BE MADE BY OTHER DESIGNATED OFFICIALS. DCAA security specialists will conduct the personal interviews in strict accordance with these provisions.

D. INTERVIEW PROCEDURES

1. THE HEAD OF THE DOD COMPONENT CONCERNED SHALL ESTABLISH UNIFORM PROCEDURES FOR CONDUCTING THE INTERVIEW THAT ARE DESIGNED TO ELICIT INFORMATION RELEVANT TO MAKING A DETERMINATION OF WHETHER THE INTERVIEWEE, ON THE BASIS OF THE INTERVIEW AND OTHER LOCALLY AVAILABLE INFORMATION (DD 398, PERSONNEL SECURITY INVESTIGATION QUESTIONNAIRE, PERSONNEL RECORDS, SECURITY FILE, ETC.), IS CONSIDERED ACCEPTABLE FOR NOMINATION AND FURTHER PROCESSING. Security specialists shall accomplish the following actions prior to conducting the actual interview:

o If interviewee is currently a DCAA employee, review Official Personnel Folder, or have the OPF reviewed by the DCAA security specialist who is at the same locale as the OPF. Reviewer will advise interviewer of review results.

c If interviewee is currently a DCAA employee, the CPS specialist doing interview shall review the CPS security file. PD and regional security specialists preparing for such interview shall request that a CPS specialist review the security file and advise of results of review.

c Review Questionnaire for National Security Positions (SF 86).

c Use SF 86 to conduct interview.

The purpose of the records review is to note items of relevance to the criteria of paragraph 2-200 and Appendix I of this manual. During the course of the personal interview, any items which surfaced as a result of the records reviews should be fully developed, and all questions contained on SF 86 must be addressed.

2. SUCH PROCEDURES SHALL BE STRUCTURED TO INSURE THE INTERVIEWEE HIS FULL RIGHTS UNDER THE CONSTITUTION OF THE UNITED STATES, THE PRIVACY ACT OF 1974 (REFERENCE (M)), AND OTHER APPLICABLE STATUTES AND REGULATIONS. To ensure compliance with this paragraph, security specialists shall use the Privacy Act Statement attached to the SF 86 to advise the interviewee of their rights, immediately prior to the conduct of the interview.

E. PROTECTION OF INTERVIEW RESULTS. ALL INFORMATION DEVELOPED DURING THE COURSE OF THE INTERVIEW SHALL BE MAINTAINED IN PERSONNEL SECURITY CHANNELS AND MADE AVAILABLE ONLY TO THOSE AUTHORITIES WHO HAVE A NEED-TO-KNOW IN CONNECTION WITH THE PROCESSING OF AN INDIVIDUAL'S NOMINATION FOR DUTIES REQUIRING ACCESS TO SCI OR THOSE WHO NEED ACCESS TO INFORMATION EITHER TO CONDUCT THE REQUIRED SBI, OR TO ADJUDICATE THE MATTER OF THE INTERVIEWEE'S ELIGIBILITY FOR ACCESS TO SCI, OR AS OTHERWISE AUTHORIZED BY EXECUTIVE ORDER OR STATUTE. The interview results will be recorded in item 10, DD Form 1879. Unfavorable information developed during the interview will be summarized on a continuation sheet, marked FOR OFFICIAL USE ONLY, and attached to the DD Form 1879. A copy of DD Form 1879 with continuation sheet, if any, and SF 86 will be forwarded to CPS in an envelope marked to be opened only by the Agency Security Officer.

F. ACCEPTABILITY DETERMINATION

1. THE DETERMINATION OF THE INTERVIEWEE'S ACCEPTABILITY FOR NOMINATION FOR DUTIES REQUIRING ACCESS TO SENSITIVE INFORMATION SHALL BE MADE BY THE COMMANDER, OR DESIGNEE, OF THE DOD ORGANIZATION THAT IS CONSIDERING NOMINATING THE INTERVIEWEE FOR SUCH DUTIES.

2. CRITERIA GUIDELINES CONTAINED IN DCID 1/14 (REFERENCE (L)), UPON WHICH THE ACCEPTABILITY FOR NOMINATION DETERMINATION IS TO BE BASED SHALL BE PROVIDED TO COMMANDERS OF DOD ORGANIZATIONS WHO MAY NOMINATE INDIVIDUALS FOR ACCESS TO SCI AND SHALL BE CONSISTENT WITH THOSE ESTABLISHED BY THE SENIOR OFFICER OF THE INTELLIGENCE COMMUNITY OF THE COMPONENT CONCERNED WITH RESPECT TO ACCEPTABILITY FOR NOMINATION TO DUTIES REQUIRING ACCESS TO SCI.

APPENDIX H

LIST OF DESIGNATED COUNTRIES

[DELETED BY CH.2, DOD 5200.2-R, 14 JULY 1993.]

APPENDIX I

ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

PURPOSE

THE FOLLOWING ADJUDICATIVE GUIDELINES ARE ESTABLISHED FOR ALL U.S. GOVERNMENT CIVILIAN AND MILITARY PERSONNEL, CONSULTANTS, CONTRACTORS, EMPLOYEES OF CONTRACTORS, LICENSEES, CERTIFICATE HOLDERS OR GRANTEES AND THEIR EMPLOYEES AND OTHER INDIVIDUALS WHO REQUIRE ACCESS TO CLASSIFIED INFORMATION. THEY APPLY TO PERSONS BEING CONSIDERED FOR INITIAL OR CONTINUED ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION, TO INCLUDE SENSITIVE COMPARTMENTED INFORMATION AND SPECIAL ACCESS PROGRAMS, AND ARE TO BE USED BY GOVERNMENT DEPARTMENTS AND AGENCIES IN ALL FINAL CLEARANCE DETERMINATIONS.

ADJUDICATIVE PROCESS

THE ADJUDICATIVE PROCESS IS AN EXAMINATION OF A SUFFICIENT PERIOD OF A PERSON'S LIFE TO MAKE AN AFFIRMATIVE DETERMINATION THAT THE PERSON IS AN ACCEPTABLE SECURITY RISK. ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION IS PREDICATED UPON THE INDIVIDUAL MEETING THESE PERSONNEL SECURITY GUIDELINES. THE ADJUDICATION PROCESS IS THE CAREFUL WEIGHING OF A NUMBER OF VARIABLES KNOWN AS THE WHOLE PERSON CONCEPT. ALL AVAILABLE, RELIABLE INFORMATION ABOUT THE PERSON, PAST AND PRESENT, FAVORABLE AND UNFAVORABLE, SHOULD BE CONSIDERED IN REACHING A DETERMINATION. IN EVALUATING THE RELEVANCE OF AN INDIVIDUAL'S CONDUCT, THE ADJUDICATOR SHOULD CONSIDER THE FOLLOWING FACTORS:

- THE NATURE, EXTENT, AND SERIOUSNESS OF THE CONDUCT
- THE CIRCUMSTANCES SURROUNDING THE CONDUCT, TO INCLUDE KNOWLEDGEABLE PARTICIPATION
- THE FREQUENCY AND RECENCY OF THE CONDUCT
- THE INDIVIDUAL'S AGE AND MATURITY AT THE TIME OF THE CONDUCT
- THE VOLUNTARINESS OF PARTICIPATION
- THE PRESENCE OR ABSENCE OF REHABILITATION AND OTHER PERTINENT BEHAVIORAL CHANGES
- THE MOTIVATION FOR THE CONDUCT
- THE POTENTIAL FOR PRESSURE, COERCION, EXPLOITATION, OR DURESS
- THE LIKELIHOOD OF CONTINUATION OR RECURRENCE

EACH CASE MUST BE JUDGED ON ITS OWN MERITS AND FINAL DETERMINATION REMAINS THE RESPONSIBILITY OF THE SPECIFIC DEPARTMENT OR AGENCY. ANY DOUBT CONCERNING PERSONNEL BEING CONSIDERED FOR ACCESS TO CLASSIFIED INFORMATION WILL BE RESOLVED IN FAVOR OF THE NATIONAL SECURITY AND CONSIDERED FINAL.

THE ULTIMATE DETERMINATION OF WHETHER THE GRANTING OR CONTINUING OF ELIGIBILITY FOR A SECURITY CLEARANCE IS CLEARLY CONSISTENT WITH THE INTERESTS OF NATIONAL SECURITY MUST BE AN OVERALL COMMON SENSE DETERMINATION BASED UPON CAREFUL CONSIDERATION OF THE FOLLOWING:

- A. ALLEGIANCE TO THE UNITED STATES
- B. FOREIGN INFLUENCE
- C. FOREIGN PREFERENCE
- D. SEXUAL BEHAVIOR
- E. PERSONAL CONDUCT
- F. FINANCIAL CONSIDERATIONS
- G. ALCOHOL CONSUMPTION
- H. DRUG INVOLVEMENT
- I. EMOTIONAL, MENTAL, AND PERSONALITY DISORDERS
- J. CRIMINAL CONDUCT
- K. SECURITY VIOLATIONS
- L. OUTSIDE ACTIVITIES
- M. MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

EACH OF THE FOREGOING SHOULD BE EVALUATED IN THE CONTEXT OF THE WHOLE PERSON.

ALTHOUGH ADVERSE INFORMATION CONCERNING A SINGLE CRITERION MAY NOT BE SUFFICIENT FOR AN UNFAVORABLE DETERMINATION, THE INDIVIDUAL MAY BE DISQUALIFIED IF AVAILABLE INFORMATION REFLECTS A RECENT OR RECURRING PATTERN OF QUESTIONABLE JUDGMENT, IRRESPONSIBILITY, OR EMOTIONALLY UNSTABLE BEHAVIOR.

HOWEVER, NOTWITHSTANDING THE WHOLE PERSON CONCEPT, PURSUIT OF FURTHER INVESTIGATION MAY BE TERMINATED BY AN APPROPRIATE ADJUDICATIVE AGENCY IN THE FACE OF RELIABLE, SIGNIFICANT, DISQUALIFYING, ADVERSE INFORMATION.

WHEN INFORMATION OF SECURITY CONCERN BECOMES KNOWN ABOUT AN INDIVIDUAL WHO IS CURRENTLY ELIGIBLE FOR ACCESS TO CLASSIFIED INFORMATION, THE ADJUDICATOR SHOULD CONSIDER WHETHER THE PERSON:

- (1) VOLUNTARILY REPORTED THE INFORMATION;
- (2) SOUGHT ASSISTANCE AND FOLLOWED PROFESSIONAL GUIDANCE, WHERE APPROPRIATE;
- (3) RESOLVED OR APPEARS LIKELY TO FAVORABLY RESOLVE THE SECURITY CONCERN;

- (4) HAS DEMONSTRATED POSITIVE CHANGES IN BEHAVIOR AND EMPLOYMENT;
- (5) SHOULD HAVE HIS OR HER ACCESS TEMPORARILY SUSPENDED PENDING FINAL ADJUDICATION OF THE INFORMATION.

IF AFTER EVALUATING INFORMATION OF SECURITY CONCERN, THE ADJUDICATOR DECIDES THAT THE INFORMATION IS NOT SERIOUS ENOUGH TO WARRANT A RECOMMENDATION OF DISAPPROVAL OR REVOCATION OF THE SECURITY CLEARANCE, IT MAY BE APPROPRIATE TO RECOMMEND APPROVAL WITH A WARNING THAT FUTURE INCIDENTS OF A SIMILAR NATURE MAY RESULT IN REVOCATION OF ACCESS.

THE INFORMATION IN BOLD PRINT AT THE BEGINNING OF EACH ADJUDICATIVE GUIDELINE PROVIDES A BRIEF EXPLANATION OF ITS RELEVANCE IN DETERMINING WHETHER IT IS CLEARLY CONSISTENT WITH THE INTEREST OF NATIONAL SECURITY TO GRANT OR CONTINUE A PERSON'S ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION.

**Adjudicative Guidelines
For Determining Eligibility for Access
To Classified Information
Approved December 29, 2005**

A. Introduction

The following adjudicative guidelines are established for all U.S. Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees, and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by government departments and agencies in all final clearance determinations. Government departments and agencies may also choose to apply these guidelines to analogous situations regarding persons being considered for access to other types of protected information.

Decisions regarding eligibility for access to classified information take into account factors that could cause a conflict of interest and place a person in the position of having to choose between his or her commitments to the United States, including the commitment to protect classified information, and any other compelling loyalty. Access decisions also take into account a person's reliability, trustworthiness and ability to protect classified information. No coercive policing could replace the self-discipline and integrity of the person entrusted with the nation's secrets as the most effective means of protecting them. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on and trusted to exercise the responsibility necessary for working in a secure environment where protecting classified information is paramount.

B. Adjudicative Process

(a) The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole-person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

- (1) the nature, extent, and seriousness of the conduct;
- (2) the circumstances surrounding the conduct, to include knowledgeable participation;
- (3) the frequency and recency of the conduct;
- (4) the individual's age and maturity at the time of the conduct;
- (5) the extent to which participation is voluntary;
- (6) the presence or absence of rehabilitation and other permanent behavioral changes;

- (7) the motivation for the conduct;
- (8) the potential for pressure, coercion, exploitation, or duress; and
- (9) the likelihood of continuation or recurrence;

(b) Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security.

(c) The ability to develop specific thresholds for action under these guidelines is limited by the nature and complexity of human behavior. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person.

(1) **GUIDELINE A: Allegiance to the United States;**

(2) **GUIDELINE B: Foreign Influence;**

(3) **GUIDELINE C: Foreign Preference;**

(4) **GUIDELINE D: Sexual Behavior;**

(5) **GUIDELINE E: Personal Conduct;**

(6) **GUIDELINE F: Financial Considerations;**

(7) **GUIDELINE G: Alcohol Consumption;**

(8) **GUIDELINE H: Drug Involvement;**

(9) **GUIDELINE I: Psychological Conditions;**

(10) **GUIDELINE J: Criminal Conduct;**

(11) **GUIDELINE K: Handling Protected Information;**

(12) **GUIDELINE L: Outside Activities;**

(13) **GUIDELINE M: Use of Information Technology Systems**

(d) Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole-person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

(e) When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

- (1) voluntarily reported the information;
- (2) was truthful and complete in responding to questions;
- (3) sought assistance and followed professional guidance, where appropriate;
- (4) resolved or appears likely to favorably resolve the security concern;
- (5) has demonstrated positive changes in behavior and employment;
- (6) should have his or her access temporarily suspended pending final adjudication of the information.

(f) If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

Guideline A
Allegiance to the United States

3. The Concern. An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

4. Conditions that could raise a security concern and may be disqualifying include:

- (a) involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States of America;
- (b) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;
- (c) association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to:
 - (1) overthrow or influence the government of the United States or any state or local government;
 - (2) prevent Federal, state, or local government personnel from performing their official duties;
 - (3) gain retribution for perceived wrongs caused by the Federal, state, or local government;
 - (4) prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

5. Conditions that could mitigate security concerns include:

- (a) the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;
- (b) the individual's involvement was only with the lawful or humanitarian aspects of such an organization;
- (c) involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;
- (d) the involvement or association with such activities occurred under such unusual circumstances, or so much time has elapsed, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or loyalty.

Guideline B
Foreign Influence

6. The Concern. Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. Adjudication under this Guideline can and should consider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.

7. Conditions that could raise a security concern and may be disqualifying include:

- (a) contact with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion;
- (b) connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information;
- (c) counterintelligence information, that may be classified, indicates that the individual's access to protected information may involve unacceptable risk to national security;
- (d) sharing living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion;
- (e) a substantial business, financial, or property interest in a foreign country, or in any foreign-owned or foreign-operated business, which could subject the individual to heightened risk of foreign influence or exploitation;
- (f) failure to report, when required, association with a foreign national;
- (g) unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence service;
- (h) indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, inducement, manipulation, pressure, or coercion;
- (i) conduct, especially while traveling outside the U.S., which may make the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.

8. Conditions that could mitigate security concerns include:

- (a) the nature of the relationships with foreign persons, the country in which these persons are located, or the positions or activities of those persons in that country are such that it is unlikely the individual will be placed in a position of having to choose between the interests of a foreign individual, group, organization, or government and the interests of the U.S.;
- (b) there is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the U.S., that the individual can be expected to resolve any conflict of interest in favor of the U.S. interest;
- (c) contact or communication with foreign citizens is so casual and infrequent that there is little likelihood that it could create a risk for foreign influence or exploitation;
- (d) the foreign contacts and activities are on U.S. Government business or are approved by the cognizant security authority;
- (e) the individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons, groups, or organizations from a foreign country;
- (f) the value or routine nature of the foreign business, financial, or property interests is such that they are unlikely to result in a conflict and could not be used effectively to influence, manipulate, or pressure the individual.

Guideline C
Foreign Preference

9. The Concern. When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

10. Conditions that could raise a security concern and may be disqualifying include:

(a) exercise of any right, privilege or obligation of foreign citizenship after becoming a U.S. citizen or through the foreign citizenship of a family member. This includes but is not limited to:

- (1) possession of a current foreign passport;
- (2) military service or a willingness to bear arms for a foreign country;
- (3) accepting educational, medical, retirement, social welfare, or other such benefits from a foreign country;
- (4) residence in a foreign country to meet citizenship requirements;
- (5) using foreign citizenship to protect financial or business interests in another country;
- (6) seeking or holding political office in a foreign country;
- (7) voting in a foreign election;

(b) action to acquire or obtain recognition of a foreign citizenship by an American citizen;

(c) performing or attempting to perform duties, or otherwise acting, so as to serve the interests of a foreign person, group, organization, or government in conflict with the national security interest;

(d) any statement or action that shows allegiance to a country other than the United States: for example, declaration of intent to renounce United States citizenship; renunciation of United States citizenship.

11. Conditions that could mitigate security concerns include:

(a) dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(b) the individual has expressed a willingness to renounce dual citizenship;

(c) exercise of the rights, privileges, or obligations of foreign citizenship occurred before the individual became a U.S. citizen or when the individual was a minor;

(d) use of a foreign passport is approved by the cognizant security authority.

(e) the passport has been destroyed, surrendered to the cognizant security authority, or otherwise invalidated.

(f) the vote in a foreign election was encouraged by the U.S. Government

Guideline D

Sexual Behavior

12. The Concern. Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference concerning the standards in this Guideline may be raised solely on the basis of the sexual orientation of the individual.

13. Conditions that could raise a security concern and may be disqualifying include:

- (a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;
- (b) a pattern of compulsive, self-destructive, or high risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder;
- (c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;
- (d) sexual behavior of a public nature and/or that reflects lack of discretion or judgment.

14. Conditions that could mitigate security concerns include:

- (a) the behavior occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature;
- (b) the sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;
- (c) the behavior no longer serves as a basis for coercion, exploitation, or duress.
- (d) the sexual behavior is strictly private, consensual, and discreet.

Guideline E
Personal Conduct

15. The Concern. Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

- (a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, including financial disclosure forms, if required, and cooperation with medical or psychological evaluation;
- (b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

16. Conditions that could raise a security concern and may be disqualifying include

- (a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;
- (b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;
- (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information;
- (d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:
 - (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information;
 - (2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations;

(4) evidence of significant misuse of Government or other employer's time or resources;

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing; or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group;

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment;

(g) association with persons involved in criminal activity.

17. Conditions that could mitigate security concerns include:

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;

(f) the information was unsubstantiated or from a source of questionable reliability;

(g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

Guideline F
Financial Considerations

18. The Concern. Failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Compulsive gambling is a concern as it may lead to financial crimes including espionage. Affluence that cannot be explained by known sources of income is also a security concern. It may indicate proceeds from financially profitable criminal acts.

19. Conditions that could raise a security concern and may be disqualifying include:

- (a) inability or unwillingness to satisfy debts;
- (b) indebtedness caused by frivolous or irresponsible spending and the absence of any evidence of willingness or intent to pay the debt or establish a realistic plan to pay the debt.
- (c) a history of not meeting financial obligations;
- (d) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;
- (e) consistent spending beyond one's means, which may be indicated by excessive indebtedness, significant negative cash flow, high debt-to-income ratio, and/or other financial analysis;
- (f) financial problems that are linked to drug abuse, alcoholism, gambling problems, or other issues of security concern;
- (g) failure to file annual Federal, state, or local income tax returns as required or the fraudulent filing of the same;
- (h) unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that cannot be explained by subject's known legal sources of income;
- (i) compulsive or addictive gambling as indicated by an unsuccessful attempt to stop gambling, "chasing losses" (i.e. increasing the bets or returning another day in an effort to get even), concealment of gambling losses, borrowing money to fund gambling or pay gambling debts, family conflict or other problems caused by gambling.

20. Conditions that could mitigate security concerns include:

- (a) the behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the conditions that resulted in the financial problem were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation), and the individual acted responsibly under the circumstances;

(c) the person has received or is receiving counseling for the problem and/or there are clear indications that the problem is being resolved or is under control;

(d) the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts;

(e) the individual has a reasonable basis to dispute the legitimacy of the past-due debt which is the cause of the problem and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue;

(f) the affluence resulted from a legal source of income.

Guideline G
Alcohol Consumption

21. The Concern. Excessive alcohol consumption often leads to the exercise of questionable judgment or the failure to control impulses, and can raise questions about an individual's reliability and trustworthiness.

22. Conditions that could raise a security concern and may be disqualifying include:

- (a) alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace, or other incidents of concern, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;
- (b) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;
- (c) habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;
- (d) diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;
- (e) evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;
- (f) relapse after diagnosis of alcohol abuse or dependence and completion of an alcohol rehabilitation program;
- (g) failure to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.

23. Conditions that could mitigate security concerns include:

- (a) so much time has passed, or the behavior was so infrequent, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;
- (b) the individual acknowledges his or her alcoholism or issues of alcohol abuse, provides evidence of actions taken to overcome this problem, and has established a pattern of abstinence (if alcohol dependent) or responsible use (if an alcohol abuser);
- (c) the individual who is a current employee who is participating in a counseling or treatment program, has no history of previous treatment and relapse, and is making satisfactory progress;
- (d) the individual has successfully completed inpatient or outpatient counseling or rehabilitation along with any required aftercare, has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations, such as participation in meetings of Alcoholics Anonymous or a similar organization and has received a

favorable prognosis by a duly qualified medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

Guideline H
Drug Involvement

24. The Concern. Use of an illegal drug or misuse of a prescription drug can raise questions about an individual's reliability and trustworthiness, both because it may impair judgment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations.

(a) Drugs are defined as mood and behavior altering substances, and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

(2) inhalants and other similar substances;

(b) drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

25. Conditions that could raise a security concern and may be disqualifying include:

(a) any drug abuse (see above definition);

(b) testing positive for illegal drug use;

(c) illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia;

(d) diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

(e) evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

(f) failure to successfully complete a drug treatment program prescribed by a duly qualified medical professional;

(g) any illegal drug use after being granted a security clearance;

(h) expressed intent to continue illegal drug use, or failure to clearly and convincingly commit to discontinue drug use.

26. Conditions that could mitigate security concerns include:

(a) the behavior happened so long ago, was so infrequent, or happened under such circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) a demonstrated intent not to abuse any drugs in the future, such as:

(1) disassociation from drug-using associates and contacts;

(2) changing or avoiding the environment where drugs were used;

(3) an appropriate period of abstinence;

(4) a signed statement of intent with automatic revocation of clearance for any violation;

(c) abuse of prescription drugs was after a severe or prolonged illness during which these drugs were prescribed, and abuse has since ended;

(d) satisfactory completion of a prescribed drug treatment program, including but not limited to rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a duly qualified medical professional.

Guideline I
Psychological Conditions

27. The Concern. Certain emotional, mental, and personality conditions can impair judgment, reliability, or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline. A duly qualified mental health professional (e.g., clinical psychologist or psychiatrist) employed by, or acceptable to and approved by the U.S. Government, should be consulted when evaluating potentially disqualifying and mitigating information under this guideline. No negative inference concerning the standards in this Guideline may be raised solely on the basis of seeking mental health counseling.

28. Conditions that could raise a security concern and may be disqualifying include:

- (a) behavior that casts doubt on an individual's judgment, reliability, or trustworthiness that is not covered under any other guideline, including but not limited to emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre behavior;
- (b) an opinion by a duly qualified mental health professional that the individual has a condition not covered under any other guideline that may impair judgment, reliability, or trustworthiness;
- (c) the individual has failed to follow treatment advice related to a diagnosed emotional, mental, or personality condition, e.g., failure to take prescribed medication.

29. Conditions that could mitigate security concerns include:

- (a) the identified condition is readily controllable with treatment, and the individual has demonstrated ongoing and consistent compliance with the treatment plan;
- (b) the individual has voluntarily entered a counseling or treatment program for a condition that is amenable to treatment, and the individual is currently receiving counseling or treatment with a favorable prognosis by a duly qualified mental health professional;
- (c) recent opinion by a duly qualified mental health professional employed by, or acceptable to and approved by the U.S. Government that an individual's previous condition is under control or in remission, and has a low probability of recurrence or exacerbation;
- (d) the past emotional instability was a temporary condition (e.g., one caused by death, illness, or marital breakup), the situation has been resolved, and the individual no longer shows indications of emotional instability;
- (e) there is no indication of a current problem.

Guideline J
Criminal Conduct

30. The Concern. Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

31. Conditions that could raise a security concern and may be disqualifying include:

- (a) a single serious crime or multiple lesser offenses;
- (b) discharge or dismissal from the Armed Forces under dishonorable conditions;
- (c) allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted;
- (d) individual is currently on parole or probation;
- (e) violation of parole or probation, or failure to complete a court-mandated rehabilitation program.

32. Conditions that could mitigate security concerns include:

- (a) so much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
- (b) the person was pressured or coerced into committing the act and those pressures are no longer present in the person's life;
- (c) evidence that the person did not commit the offense;
- (d) there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement.

Guideline K
Handling Protected Information

33. The Concern. Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

34. Conditions that could raise a security concern and may be disqualifying include:

- (a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;
- (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
- (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;
- (d) inappropriate efforts to obtain or view classified or other protected information outside one's need to know;
- (e) copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings;
- (f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;
- (g) any failure to comply with rules for the protection of classified or other sensitive information;
- (h) negligence or lax security habits that persist despite counseling by management.
- (i) failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

35. Conditions that could mitigate security concerns include:

- (a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;
- (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;
- (c) the security violations were due to improper or inadequate training.

Guideline L
Outside Activities

36. The Concern. Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

37. Conditions that could raise a security concern and may be disqualifying include:

(a) any employment or service, whether compensated or volunteer, with:

(1) the government of a foreign country;

(2) any foreign national, organization, or other entity;

(3) a representative of any foreign interest;

(4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology;

(b) failure to report or fully disclose an outside activity when this is required.

38. Conditions that could mitigate security concerns include:

(a) evaluation of the outside employment or activity by the appropriate security or counterintelligence office indicates that it does not pose a conflict with an individual's security responsibilities or with the national security interests of the United States;

(b) the individual terminated the employment or discontinued the activity upon being notified that it was in conflict with his or her security responsibilities.

Guideline M
Use of Information Technology Systems

39. The Concern. Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

40. Conditions that could raise a security concern and may be disqualifying include:

- (a) illegal or unauthorized entry into any information technology system or component thereof;
- (b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;
- (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;
- (d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;
- (e) unauthorized use of a government or other information technology system;
- (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization; when prohibited by rules, procedures, guidelines or regulations;
- (g) negligence or lax security habits in handling information technology that persist despite counseling by management;
- (h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

41. Conditions that could mitigate security concerns include:

- (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
- (b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available;
- (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

APPENDIX J

OVERSEAS INVESTIGATIONS1. PURPOSE.

THE PURPOSE OF THIS APPENDIX IS TO ESTABLISH, WITHIN THE FRAMEWORK OF THIS REGULATION, DOD DIRECTIVE 5105.42 AND DEFENSE INVESTIGATIVE SERVICE MANUAL 20-1, (REFERENCES (HH) AND (II)) STANDARDIZED PROCEDURES FOR THE MILITARY INVESTIGATIVE AGENCIES TO FOLLOW WHEN THEY PERFORM ADMINISTRATIVE AND INVESTIGATIVE FUNCTIONS ON BEHALF OF DIS AT OVERSEAS LOCATIONS.

2. TYPE INVESTIGATION.

THIS REGULATION DESCRIBES IN DETAIL BACKGROUND INVESTIGATIONS (BI) WHICH ARE CONDUCTED FOR LIMITED ACCESS AUTHORIZATIONS AND THOSE SPECIAL INVESTIGATIVE INQUIRIES CONDUCTED FOR POST-ADJUDICATIVE PURPOSES. HEREAFTER THEY ARE REFERRED TO A LAA AND POST-ADJUDICATIVE CASES AND ARE BRIEFLY DESCRIBED IN PARAGRAPHS A AND B BELOW:

A. LIMITED ACCESS AUTHORIZATION:

A LEVEL OF ACCESS TO CLASSIFIED DEFENSE INFORMATION THAT MAY BE GRANTED TO A NON-US CITIZEN UNDER CERTAIN CONDITIONS, ONE OF WHICH IS THAT A BI MUST HAVE BEEN COMPLETED WITH SATISFACTORY RESULTS. PARAGRAPH 3-403 FURTHER DESCRIBES LAA CASES.

B. POST-ADJUDICATION INVESTIGATION:

A PERSONNEL SECURITY INVESTIGATION (PSI) PREDICATED ON NEW, ADVERSE OR QUESTIONABLE SECURITY, SUITABILITY OR HOSTAGE INFORMATION THAT ARISES AND REQUIRES THE APPLICATION OF INVESTIGATION PROCEDURES SUBSEQUENT TO ADJUDICATIVE ACTION ON A DOD-AFFILIATED PERSON'S ELIGIBILITY FOR CONTINUED ACCESS TO CLASSIFIED INFORMATION, ASSIGNMENT TO OR RETENTION IN SENSITIVE DUTIES OR OTHER DESIGNATED DUTIES REQUIRING SUCH INVESTIGATION. WHILE THESE CASES ARE NORMALLY PREDICATED ON THE SURFACING OF UNFAVORABLE INFORMATION SUBSEQUENT TO FAVORABLE ADJUDICATION, THEY MAY ALSO BE OPENED WHEN FAVORABLE INFORMATION IS OFFERED TO COUNTER A PREVIOUS UNFAVORABLE ADJUDICATION. PARAGRAPH 2-402.C FURTHER DESCRIBES THESE CASES.

3. GENERAL.

A. AS A RULE, INVESTIGATIVE ACTIVITY IN MOST PSIs OCCURS IN THE U.S. EVEN WHEN THE SUBJECT IS AT AN OVERSEAS LOCATION. THEREFORE, THE SUBMISSION OF REQUESTS FOR INVESTIGATION TO THE PERSONNEL INVESTIGATION CENTER (PIC) AT BALTIMORE IS A REQUIRED PROCEDURE AS IT ENSURES UNIFORM APPLICATION OF DOD PSI POLICY AND THE EFFICIENT DISPATCH AND COORDINATION OF LEADS.

B. WHEN THE PURPOSE OF THE INVESTIGATION IS FOR AN LAA OR POST-ADJUDICATION ON A SUBJECT OVERSEAS, MUCH, IF NOT ALL OF THE LEADS ARE AT AN OVERSEAS LOCATION. WHILE THESE CASES ALSO MAY BE SUBMITTED DIRECTLY TO PIC FOR ACTION, THERE IS AN INHERENT DELAY IN THE MAILING OF THE REQUEST, THE EXCHANGE OF LEADS AND REPORTS WITH PIC, AND TRANSMITTAL OF THE REPORTS BACK TO THE REQUESTER. TO AVOID THIS DELAY, THE MILITARY INVESTIGATIVE AGENCIES, WHEN

ACTING FOR DIS OVERSEAS IN ACCORDANCE WITH DOD DIRECTIVE 5105.42 (REFERENCE (HH)) MAY, WITH THEIR HEADQUARTERS APPROVAL, ACCEPT THESE REQUESTS FOR INVESTIGATIONS, INITIATE THEM AND DISSEMINATE THE RESULTS FROM THE SAME LEVEL AS THEY OPEN, CLOSE, AND DISSEMINATE THEIR OWN CASES. USUALLY THIS WILL GREATLY IMPROVE RESPONSE TIME TO THE REQUESTER.

C. UNDER THE PROCEDURES IN PARAGRAPH B, ABOVE, DIS WILL NOT OFTEN BE IN A POSITION TO DIRECTLY EXERCISE ITS RESPONSIBILITY FOR CONTROL AND DIRECTION UNTIL THE CASE OR LEAD IS IN PROGRESS OR EVEN COMPLETED; THEREFORE, ADHERENCE TO THE POLICY STATED IN REFERENCED DOCUMENTS, AND AS MODIFIED HEREIN, IS MANDATORY. WHEN THE POLICY OF THE MILITARY INVESTIGATIVE AGENCY IS AT VARIANCE WITH THE ABOVE, THE MATTER WILL BE REFERRED TO THE RESPECTIVE HEADQUARTERS FOR RESOLUTION.

D. SINCE DIS IS ULTIMATELY RESPONSIBLE FOR THE PERSONNEL SECURITY PRODUCT, IT MUST BE KEPT INFORMED OF ALL SUCH MATTERS REFERRED TO IN THIS APPENDIX. FOR INSTANCE, WHEN THE INVESTIGATIVE AGENCY OVERSEAS RECEIVES A DD FORM 1879, REQUEST FOR PERSONNEL SECURITY INVESTIGATION, WHICH SETS FORTH AN ISSUE OUTSIDE DIS JURISDICTION, IT WILL REJECT THE REQUEST, INFORM THE REQUESTER OF THE REASON AND FURNISH AN INFORMATION COPY OF THE DD FORM 1879 AND REJECTION LETTER TO PIC. WHEN THE ISSUE/JURISDICTION IS UNCLEAR TO THE INVESTIGATIVE AGENCY, THE DD FORM 1879 AND THE PERCEIVED JURISDICTIONAL QUESTION SHOULD BE PROMPTLY FORWARDED TO DIS FOR ACTION AND, IF APPROPRIATE, TO THE COMPONENT'S HEADQUARTERS FOR INFORMATION. QUESTIONS ON THE INTERPRETATION OF DIS OR DOD POLICY AND DIRECTIVES PERTAINING TO INDIVIDUAL PSI CASES CAN USUALLY BE RESOLVED THROUGH DIRECT COMMUNICATIONS WITH PIC.

E. DOD DIRECTIVE 5105.42 (REFERENCE (HH)), ESTABLISHES THE SUPPORTING RELATIONSHIP OF THE MILITARY INVESTIGATIVE AGENCIES TO DIS IN OVERSEAS AREAS, AND DIS PROVIDES THESE AGENCIES WITH COPIES OF RELEVANT POLICY AND INTERPRETIVE GUIDANCE. FOR THESE REASONS, THE INVESTIGATIVE AGENCY VICE THE REQUESTER, IS RESPONSIBLE FOR EVALUATING THE REQUEST, PROCESSING IT, COLLECTING AND EVALUATING THE RESULTS WITHIN THEIR JURISDICTION FOR SUFFICIENCY, AND FORWARDING THE COMPLETED PRODUCT TO THE APPROPRIATE ACTIVITY.

F. THE MAGNITUDE OF OPERATIONS AT PIC REQUIRES THAT METHODS OF HANDLING LAA AND POST-ADJUDICATIVE CASES BE CONSISTENT TO THE MAXIMUM EXTENT POSSIBLE. FOR THIS REASON, THE PROCEDURES FOR LAA CASES ARE NEARLY IDENTICAL TO THOSE FOR POST-ADJUDICATIVE CASES. BRIEFLY, THE MAIN EXCEPTIONS ARE:

(1) THE NOTIFICATION TO PIC THAT A POST-ADJUDICATION CASE HAS BEEN OPENED WILL BE BY MESSAGE, SINCE AN ISSUE IS PRESENT AT THE OUTSET, WHEREAS NOTIFICATION OF AN LAA CASE SHOULD NORMALLY BE BY MAIL.

(2) THE SCOPE OF THE LAA INVESTIGATION IS 10 YEARS OR SINCE THE PERSON'S 18TH BIRTHDAY, WHICHEVER IS SHORTEST, WHEREAS THE LEADS IN A POST-ADJUDICATION CASE ARE LIMITED TO RESOLVING THE ISSUE.

4. JURISDICTION.

A. AS SET FORTH IN DOD DIRECTIVE 5105.42 (REFERENCE (HH)), DIS IS RESPONSIBLE FOR CONDUCTING ALL DOD PSIs IN THE 50 STATES, DISTRICT OF COLUMBIA, AND PUERTO RICO, AND WILL REQUEST THE MILITARY DEPARTMENTS TO ACCOMPLISH

INVESTIGATIVE REQUIREMENTS ELSEWHERE. THE MILITARY INVESTIGATIVE AGENCIES IN OVERSEAS LOCATIONS ROUTINELY RESPOND TO PERSONNEL SECURITY INVESTIGATIVE LEADS FOR DIS.

B. DIS JURISDICTION ALSO INCLUDES INVESTIGATION OF SUBVERSIVE AFFILIATIONS, SUITABILITY INFORMATION, AND HOSTAGE SITUATIONS WHEN SUCH INQUIRIES ARE REQUIRED FOR PERSONNEL SECURITY PURPOSES; HOWEVER, JURISDICTION WILL REST WITH THE MILITARY INVESTIGATIVE AGENCIES, FBI AND/OR CIVIL AUTHORITIES AS APPROPRIATE WHEN THE ALLEGED SUBVERSION OR SUITABILITY ISSUE REPRESENTS A VIOLATION OF LAW OR, IN THE CASE OF A HOSTAGE SITUATION, THERE IS AN INDICATION THAT THE PERSON CONCERNED IS ACTUALLY BEING PRESSURED, COERCED, OR INFLUENCED BY INTERESTS INIMICAL TO THE UNITED STATES, OR THAT HOSTILE INTELLIGENCE IS TAKING ACTION SPECIFICALLY DIRECTED AGAINST THAT PERSON. SPECIFIC POLICY GUIDANCE ON THE APPLICABILITY OF THESE PROCEDURES AND THE JURISDICTIONAL CONSIDERATIONS ARE STATED IN CHAPTER II, SECTION 4.

5. CASE OPENING.

A. A REQUEST FOR INVESTIGATION MUST BE SUBMITTED BY USING DD FORM 1879 AND ACCOMPANIED BY SUPPORTING DOCUMENTATION UNLESS SUCH DOCUMENTATION IS NOT IMMEDIATELY AVAILABLE, OR THE OBTAINING OF DOCUMENTATION WOULD COMPROMISE A SENSITIVE INVESTIGATION. UPON RECEIPT OF THE REQUEST, THE MILITARY INVESTIGATIVE COMPONENT WILL IDENTIFY THE ISSUE(S), SCOPE THE LEADS, AND ENSURE THAT THE PROPOSED ACTION IS THAT WHICH IS AUTHORIZED FOR DIS AS DELINEATED IN THIS REGULATION, DOD DIRECTIVE 5105.42 AND DEFENSE INVESTIGATIVE SERVICE MANUAL 20-1-M (REFERENCES (HH) AND (II)).

B. UPON SUCH DETERMINATION, THE COMPONENT WILL PREPARE AN ACTION LEAD SHEET (ALS) WHICH FULLY IDENTIFIES THE SUBJECT AND THE SCOPE OF THE CASE, AND SPECIFIES PRECISELY THE LEADS WHICH EACH INVESTIGATIVE COMPONENT (INCLUDING DIS/PIC WHEN APPROPRIATE) IS TO CONDUCT.

C. CASE OPENING PROCEDURES DESCRIBED ABOVE ARE IDENTICAL FOR LAA AND POST-ADJUDICATION CASES EXCEPT WITH RESPECT TO NOTIFICATION OF CASE OPENING TO PIC:

(1) POST-ADJUDICATION CASES. THESE CASES, BECAUSE THEY INVOLVE AN ISSUE, ARE POTENTIALLY SENSITIVE AND MUST BE EXAMINED AS EARLY AS POSSIBLE BY PIC FOR CONFORMITY TO THE LATEST DOD POLICY. ACCORDINGLY, THE INITIAL NOTIFICATION TO PIC OF CASE OPENINGS WILL ALWAYS BE BY MESSAGE. THE MESSAGE WILL CONTAIN AT A MINIMUM:

- (A) FULL IDENTIFICATION OF THE SUBJECT;
- (B) A NARRATIVE DESCRIBING THE ALLEGATION/FACTS IN SUFFICIENT DETAIL TO SUPPORT OPENING OF THE CASE; AND
- (C) A BRIEF LISTING OF THE LEADS THAT ARE PLANNED.

THE DD FORM 1879 AND SUPPORTING DOCUMENTS, ALONG WITH THE AGENCY'S ALS, SHOULD BE SUBSEQUENTLY MAILED TO PIC.

(2) LAA CASES. THE NOTIFICATION TO PIC OF CASE OPENING WILL NORMALLY BE ACCOMPLISHED BY MAILING THE DD FORM 1879, DD FORM 398 (PERSONAL HISTORY STATEMENT), A COPY OF THE ALS, AND ANY OTHER SUPPORTING DOCUMENTS TO

PIC. MESSAGE NOTIFICATION TO PIC IN LAA CASES WILL ONLY BE REQUIRED IF THERE IS A SECURITY OR SUITABILITY ISSUE APPARENT IN THE DD FORM 1879 OR SUPPORTING DOCUMENTS.

D. BEYOND INITIAL ACTIONS NECESSARY TO TEST ALLEGATION FOR INVESTIGATIVE MERIT AND JURISDICTION, NO FURTHER INVESTIGATIVE ACTION SHOULD COMMENCE UNTIL THE NOTIFICATION OF CASE OPENING TO PIC HAS BEEN DISPATCHED.

E. PIC WILL PROMPTLY RESPOND TO THE NOTIFICATION OF CASE OPENING BY MAIL OR MESSAGE SPECIFYING ANY QUALIFYING REMARKS ALONG WITH A SUMMARY OF PREVIOUSLY EXISTING DATA. PIC WILL ALSO PROVIDE A DIS CASE CONTROL NUMBER (CCN). THIS NUMBER MUST BE USED BY ALL COMPONENTS ON ALL CASE RELATED PAPERWORK/REPORTS.

(THE INVESTIGATING AGENCY MAY ASSIGN ITS UNIQUE SERVICE CCN FOR INTERIM INTERNAL CONTROL; HOWEVER, THE CASE WILL BE PROCESSED, REFERENCED, AND ENTERED INTO THE DCII BY THE DIS CASE CONTROL NUMBER. THE FIRST FIVE DIGITS OF THE DIS CCN WILL BE THE JULIAN DATE OF THE CASE OPENING WHEN RECEIVED AT DIS.)

6. CASE PROCESSING.

A. THE EXPECTED COMPLETION TIME FOR LEADS IN LAA CASES IS 50 CALENDAR DAYS AND FOR POST-ADJUDICATION CASES, 30 DAYS, AS COMPUTED FROM THE DATE OF RECEIPT OF THE REQUEST. IF CONDITIONS PRECLUDE COMPLETION IN THIS TIME PERIOD, A PENDING REPORT OF THE RESULTS TO DATE, ALONG WITH AN ESTIMATED DATE OF COMPLETION WILL BE SUBMITTED TO PIC.

B. COPIES OF ALL ALSs WILL BE FURNISHED TO PIC. IN ADDITION, PIC WILL BE PROMPTLY NOTIFIED OF ANY SIGNIFICANT CHANGE IN THE SCOPE OF THE CASE, OR THE DEVELOPMENT OF AN INVESTIGATIVE ISSUE.

C. THE PROCEDURES FOR IMPLEMENTING THE PRIVACY ACT IN PSI CASES ARE SET IN DIS MANUAL 20-1-M (REFERENCE (II)). ANY OTHER RESTRICTIONS ON THE RELEASE OF INFORMATION IMPOSED BY AN OVERSEAS SOURCE OR BY REGULATIONS OF THE COUNTRY WHERE THE INQUIRY TAKES PLACE WILL BE CLEARLY STATED IN THE REPORT.

D. THE REPORT FORMAT FOR THESE CASES WILL BE THAT USED BY THE MILITARY INVESTIGATIVE AGENCY.

E. INVESTIGATIVE ACTION OUTSIDE THE JURISDICTIONAL AREA OF AN INVESTIGATIVE COMPONENT OFFICE MAY BE DIRECTED ELSEWHERE BY ALS AS NEEDED IN ACCORDANCE WITH THAT AGENCY'S PROCEDURES AND WITHIN THE FOLLOWING GEOGRAPHICAL CONSIDERATIONS:

(1) LEADS WILL BE SENT TO PIC IF THE INVESTIGATIVE ACTION IS IN THE UNITED STATES, DISTRICT OF COLUMBIA, PUERTO RICO, AMERICAN SAMOA, BAHAMA ISLANDS, THE U.S. VIRGIN ISLANDS, AND THE FOLLOWING ISLANDS IN THE PACIFIC: WAKE, MIDWAY, KWAJALIN, JOHNSTON, CAROLINES, MARSHALLS, AND ENIWETOK.

(2) LEADS TO AREAS NOT LISTED ABOVE MAY BE DISPATCHED TO OTHER UNITS OF THE INVESTIGATIVE AGENCY OR EVEN TO ANOTHER MILITARY AGENCY'S FIELD UNITS IF THERE IS AN AGREEMENT OR MEMORANDUM OF UNDERSTANDING THAT PROVIDES FOR SUCH ACTION. FOR CASE ACCOUNTABILITY PURPOSES, COPIES OF SUCH "LATERAL" LEADS MUST BE SENT TO THE PIC.

(3) LEADS THAT CANNOT BE DISPATCHED AS DESCRIBED IN SUBPARAGRAPH (2) ABOVE, AND THOSE THAT MUST BE SENT TO A NON-DOD INVESTIGATIVE AGENCY SHOULD BE SENT TO PIC FOR DISPOSITION.

F. THE DEFENSE INVESTIGATIVE MANUAL (REFERENCE (II)) CALLS FOR OBTAINING PIC APPROVAL BEFORE CONDUCTING A SUBJECT INTERVIEW ON A POST-ADJUDICATIVE INVESTIGATION. TO AVOID THE DELAY THAT COMPLIANCE WITH THIS PROCEDURE WOULD CREATE, A MILITARY INVESTIGATIVE COMPONENT MAY CONDUCT THE INTERVIEW PROVIDED:

(1) ALL OTHER INVESTIGATIVE LEADS HAVE BEEN COMPLETED AND REVIEWED.

(2) THE CCM HAS BEEN RECEIVED, SIGNIFYING DIS CONCURRENCE WITH THE APPROPRIATENESS OF THE INVESTIGATION.

(3) CONTRARY INSTRUCTIONS HAVE NOT BEEN RECEIVED FROM THE PIC.

(4) THE INTERVIEW IS LIMITED TO THE RESOLUTION OF THE RELEVANT ISSUES DISCLOSED BY THE INVESTIGATION.

G. NOTWITHSTANDING THE PROVISIONS OF PARAGRAPH F. (1) THROUGH (4), ABOVE, IF TIME IS OF THE ESSENCE DUE TO IMMINENT TRANSFER OF THE SUBJECT, A SUBJECT INTERVIEW MAY BE CONDUCTED AT THE DISCRETION OF THE INVESTIGATIVE AGENCY.

7. CASE RESPONSIBILITY LAA AND PA.

PARAGRAPH 3, ABOVE, DESCRIBES THE ADVANTAGES OF TIMELY HANDLING WHICH ACCRUE WHEN THE MILITARY INVESTIGATIVE COMPONENTS ACT FOR DIS OVERSEAS. THESE ACTIONS FOR DIS MAY, HOWEVER, BE LIMITED BY THE COMPONENT'S STAFFING AND RESOURCE LIMITATIONS, ESPECIALLY SINCE SOME CASES REQUIRE MORE ADMINISTRATION AND MANAGEMENT THAN OTHERS. POST-ADJUDICATION CASE LEADS, FOR INSTANCE, WILL NORMALLY BE WITHIN THE GEOGRAPHICAL JURISDICTION OF THE COMPONENT THAT ACCEPTED THE REQUEST FOR INVESTIGATION; THEREFORE, RELATIVELY LITTLE CASE MANAGEMENT IS REQUIRED. IN CONTRAST, LAA CASES MAY REQUIRE LEADS WORLD-WIDE, AND, THEREFORE, CREATE MORE COMPLEX CASE MANAGEMENT AND ADMINISTRATION, ESPECIALLY IN THE TRACKING, MONITORING AND REVIEWING OF LEADS OUTSIDE THE COMPONENT'S GEOGRAPHICAL AREA. ACCORDINGLY, AN INVESTIGATIVE COMPONENT WILL ACCEPT THE CASE FROM THE REQUESTER, BUT ONLY ASSIGN ITSELF THE APPROPRIATE LEADS WITHIN ITS OWN GEOGRAPHICAL JURISDICTION AND SEND THE BALANCE TO PIC FOR APPROPRIATE DISPOSITION IN ACCORDANCE WITH THE FOLLOWING:

(1) THE INVESTIGATIVE AGENCY WILL ACCEPT THE REQUEST FOR INVESTIGATION (THEREBY SAVING TIME OTHERWISE LOST IN MAILING TO PIC) BUT LIMIT ITS INVOLVEMENT IN CASE MANAGEMENT BY EXTRACTING ONLY THOSE LEADS IT WILL CONDUCT OR MANAGE LOCALLY.

(2) THE AGENCY SHOULD THEN PREPARE AN ALS THAT SHOWS CLEARLY WHAT LEADS IT WILL COVER AND SEND PIC A COPY OF THIS ALS, ALONG WITH THE REQUEST FOR INVESTIGATION AND ANY OTHER APPROPRIATE DOCUMENTATION. IT MUST BE CLEAR IN THE ALS THAT PIC IS TO ACT ON ALL THOSE LEADS THAT THE UNIT HAS NOT ASSIGNED TO ITSELF.

(3) PIC, AS CASE MANAGER, WILL ASSUME RESPONSIBILITY FOR THE COMPLETE INVESTIGATIVE PACKAGE AND, UPON RECEIPT OF THE LAST LEAD, WILL SEND THE RESULTS TO THE APPROPRIATE ACTIVITY.

(4) THE AGENCY THAT ACCEPTED THE CASE AND ASSIGNED ITSELF LEADS MAY SEND A COPY OF ITS REPORT TO THE ACTIVITY IN THE "RESULTS TO" BLOCK AT THE SAME TIME IT SENDS THE ORIGINALS TO PIC. IF SO, THE LETTER OF TRANSMITTAL MUST INFORM THE RECIPIENT THAT THESE REPORTS ARE ONLY A PORTION OF THE INVESTIGATION, AND THAT THE BALANCE WILL BE FORTHCOMING FROM PIC. SIMILARLY, PIC MUST BE INFORMED OF WHICH INVESTIGATIVE REPORTS WERE DISSEMINATED. (THIS IS NORMALLY DONE BY SENDING PIC A COPY OF THE LETTER OF TRANSMITTAL.)

8. SCOPE.

A. LAA. THE SCOPE OF INVESTIGATION IS 10 YEARS OR FROM AGE 18, WHICHEVER IS THE SHORTEST PERIOD.

B. POST-ADJUDICATION CASES. THERE IS NO STANDARD SCOPE. THE INQUIRIES CONDUCTED WILL BE LIMITED TO THOSE NECESSARY TO RESOLVE THE ISSUE(S).

9. CASE CLOSING: LAA AND PA.

A. WHETHER THE INVESTIGATIVE COMPONENT OR PIC CLOSES OUT AN INVESTIGATION, THERE ARE THREE KEY ELEMENTS TO CONSIDER:

(1) THE INVESTIGATIVE RESULTS MUST BE REVIEWED FOR QUALITY AND CONFORMANCE TO POLICY.

(2) THE RESULTS MUST BE SENT TO THE ACTIVITY LISTED IN THE "RESULTS TO" BLOCK OF THE DD FORM 1879.

(3) PIC MUST BE INFORMED WHETHER OR NOT ANY DISSEMINATION WAS MADE BY THE INVESTIGATIVE AGENCY AND, IF SO, WHAT REPORTS WERE FURNISHED.

B. INVESTIGATIVE RESULTS MAY ALSO BE SENT TO A REQUESTER OR HIGHER LEVEL ACTIVITY THAT MAKES A STATEMENT OF NEED FOR THE RESULTS. IN SUCH INSTANCES, A COPY OF THE LETTER REQUESTING THE RESULTS AND THE CORRESPONDING LETTER OF TRANSMITTAL MUST BE SENT TO PIC FOR RETENTION.

C. WHEN AN INVESTIGATIVE AGENCY DISSEMINATES REPORTS FOR PIC, IT MAY USE THE TRANSMITTAL DOCUMENTS, LETTERS, OR COVER SHEETS IT CUSTOMARILY USES FOR ITS OWN CASES.

D. THE MATERIAL THAT IS TO BE PROVIDED TO PIC WILL CONSIST OF: THE ORIGINALS OF ALL REPORTS, AND ALL OTHER CASE DOCUMENTATION SUCH AS ORIGINAL STATEMENTS, CONFIDENTIAL SOURCE SHEETS, INTERVIEW LOGS, REQUESTS FOR INVESTIGATION, LETTERS OF TRANSMITTAL TO ADJUDICATORS/REQUESTERS, OR COMMUNICATIONS WITH THE REQUESTER, SUCH AS THOSE THAT MODIFY THE SCOPE OF THE INVESTIGATION.

E. FOR DIS TO FULFILL ITS RESPONSIBILITIES UNDER DOD 5220.22-R (REFERENCE (A)) AND THE PRIVACY ACT OF 1974 (REFERENCE (M)), ALL INQUIRIES CONDUCTED IN ITS BEHALF MUST BE SET FORTH IN AN ROI FOR THE PERMANENT FILE, WHETHER THE CASE IS COMPLETED, TERMINATED EARLY, OR REFERRED TO ANOTHER AGENCY.

10. REFERRAL.

A CASE MAY REQUIRE PREMATURE CLOSING AT ANY TIME AFTER RECEIPT OF THE DD FORM 1879 BY THE INVESTIGATIVE COMPONENT IF THE INFORMATION ACCOMPANYING THE REQUEST, OR THAT WHICH IS LATER DEVELOPED, IS OUTSIDE DIS JURISDICTION. FOR EXAMPLE, ALLEGED VIOLATIONS OF LAW, A COUNTERINTELLIGENCE MATTER, OR ACTUAL COERCION/INFLUENCE IN A HOSTAGE SITUATION (SEE PARAGRAPH 4.B., ABOVE) MUST BE REFERRED TO THE APPROPRIATE AGENCY, AND DIS INVOLVEMENT TERMINATED. THE REQUESTER WILL BE INFORMED BY LETTER OR INDORSEMENT TO THE DD FORM 1879 OF THE INFORMATION DEVELOPED THAT, DUE TO JURISDICTIONAL CONSIDERATION, THE CASE WAS REFERRED TO (FILL IN APPROPRIATE ADDRESS) AND THAT THE DIS CASE IS CLOSED. THE AGENCY TO WHICH REFERRAL WAS MADE AND PIC WILL BE FURNISHED WITH THE RESULTS OF ALL INVESTIGATIONS CONDUCTED UNDER DIS AUSPICES. DIS, HOWEVER, HAS AN INTEREST IN THE REFERRAL AGENCY'S ACTIONS AND NO INFORMATION SHOULD BE SOLICITED FROM THAT AGENCY.

APPENDIX K

ADP POSITION CATEGORIES
AND
CRITERIA FOR DESIGNATING POSITIONS

OMB CIRCULAR A-71 (AND TRANSMITTAL MEMO #1), JULY 1978 OMB CIRCULAR A-130, DECEMBER 12, 1985, AND FPM LETTER 732, NOVEMBER 14, 1978 CONTAIN THE CRITERIA FOR DESIGNATING POSITIONS UNDER THE EXISTING CATEGORIES USED IN THE PERSONNEL SECURITY PROGRAM FOR FEDERAL CIVILIAN EMPLOYEES AS WELL AS THE CRITERIA FOR DESIGNATING ADP AND ADP RELATED POSITIONS. THIS POLICY IS OUTLINED BELOW:

ADP POSITION CATEGORIES

1. CRITICAL-SENSITIVE POSITIONS.

ADP-I POSITIONS. THOSE POSITIONS IN WHICH THE INCUMBENT IS RESPONSIBLE FOR THE PLANNING, DIRECTION, AND IMPLEMENTATION OF A COMPUTER SECURITY PROGRAM; MAJOR RESPONSIBILITY FOR THE DIRECTION, PLANNING AND DESIGN OF A COMPUTER SYSTEM, INCLUDING THE HARDWARE AND SOFTWARE; OR, CAN ACCESS A SYSTEM DURING THE OPERATION OR MAINTENANCE IN SUCH A WAY, AND WITH A RELATIVELY HIGH RISK FOR CAUSING GRAVE DAMAGE, OR REALIZE A SIGNIFICANT PERSONAL GAIN.

2. NONCRITICAL-SENSITIVE POSITIONS.

ADP-II POSITIONS. THOSE POSITIONS IN WHICH THE INCUMBENT IS RESPONSIBLE FOR THE DIRECTION, PLANNING, DESIGN, OPERATION, OR MAINTENANCE OF A COMPUTER SYSTEM, AND WHOSE WORK IS TECHNICALLY REVIEWED BY A HIGHER AUTHORITY OF THE ADP-I CATEGORY TO INSURE THE INTEGRITY OF THE SYSTEM.

3. NONSENSITIVE POSITIONS.

ADP-III POSITIONS. ALL OTHER POSITIONS INVOLVED IN COMPUTER ACTIVITIES.

IN ESTABLISHING THE CATEGORIES OF POSITIONS, OTHER FACTORS MAY ENTER INTO THE DETERMINATION, PERMITTING PLACEMENT IN HIGHER OR LOWER CATEGORIES BASED ON THE AGENCY'S JUDGMENT AS TO THE UNIQUE CHARACTERISTICS OF THE SYSTEM OR THE SAFEGUARDS PROTECTION THE SYSTEM.

CRITERIA FOR DESIGNATING POSITIONS

THREE CATEGORIES HAVE BEEN ESTABLISHED FOR DESIGNATING COMPUTER AND COMPUTER-RELATED POSITIONS -- ADP-I, ADP-II, AND ADP-III. SPECIFIC CRITERIA FOR ASSIGNING POSITIONS TO ONE OF THESE CATEGORIES IS AS FOLLOWS:

CATEGORY

CRITERIA

ADP-I

RESPONSIBILITY OR THE DEVELOPMENT AND ADMINISTRATION OF AGENCY COMPUTER SECURITY PROGRAMS, AND ALSO INCLUDING DIRECTION AND CONTROL OF RISK ANALYSIS AND/OR THREAT ASSESSMENT.

SIGNIFICANT INVOLVEMENT IN LIFE-CRITICAL OR MISSIONCRITICAL SYSTEMS.

CATEGORY

CRITERIA

SIGNIFICANT INVOLVEMENT IN LIFE-CRITICAL OR MISSIONCRITICAL SYSTEMS.

RESPONSIBILITY FOR THE PREPARATION OR APPROVAL OF DATA FOR INPUT INTO A SYSTEM WHICH DOES NOT NECESSARILY INVOLVE PERSONAL ACCESS TO THE SYSTEM, BUT WITH RELATIVELY HIGH RISK FOR EFFECTING GRAVE DAMAGE OR REALIZING SIGNIFICANT PERSONAL GAIN.

RELATIVELY HIGH RISK ASSIGNMENTS ASSOCIATED WITH OR DIRECTLY INVOLVING THE ACCOUNTING, DISBURSEMENT, OR AUTHORIZATION FOR DISBURSEMENT FROM SYSTEMS OF (1) DOLLAR AMOUNTS OF \$10 MILLION PER YEAR OR GREATER, OR (2) LESSER AMOUNTS IF THE ACTIVITIES OF THE INDIVIDUAL ARE NOT SUBJECT TO TECHNICAL REVIEW BY HIGHER AUTHORITY IN THE ADP-I CATEGORY TO INSURE THE INTEGRITY OF THE SYSTEM.

POSITIONS INVOLVING MAJOR RESPONSIBILITY FOR THE DIRECTION, PLANNING, DESIGN, TESTING, MAINTENANCE, OPERATION, MONITORING, AND/OR MANAGEMENT OF SYSTEMS HARDWARE AND SOFTWARE.

OTHER POSITIONS AS DESIGNATED BY THE AGENCY HEAD THAT INVOLVE RELATIVELY HIGH RISK FOR EFFECTING GRAVE DAMAGE OR REALIZING SIGNIFICANT PERSONAL GAIN.

ADP-II

RESPONSIBILITY FOR SYSTEMS DESIGN, OPERATION, TESTING, MAINTENANCE, AND/OR MONITORING THAT IS CARRIED OUT UNDER TECHNICAL REVIEW OF HIGHER AUTHORITY IN THE ADP-I CATEGORY, INCLUDES, BUT IS NOT LIMITED TO:

(1) ACCESS TO AND/OR PROCESSING OF PROPRIETARY DATA, INFORMATION REQUIRING PROTECTION UNDER THE PRIVACY ACT OF 1974, AND GOVERNMENT-DEVELOPED PRIVILEGED INFORMATION INVOLVING THE AWARD OF CONTRACTS;

(2) ACCOUNTING, DISBURSEMENT, OR AUTHORIZATION FOR DISBURSEMENT FROM SYSTEMS OF DOLLAR AMOUNTS LESS THAN \$10 MILLION PER YEAR. OTHER POSITIONS ARE DESIGNATED BY THE AGENCY HEAD THAT INVOLVE A DEGREE OF ACCESS TO A SYSTEM THAT CREATES A SIGNIFICANT POTENTIAL FOR DAMAGE OR PERSONAL GAIN LESS THAN THAT IN ADP-I POSITIONS.

ADP-III

ALL OTHER POSITIONS INVOLVED IN FEDERAL COMPUTER ACTIVITIES.

APPENDIX L

LIST OF SAMPLE NOTIFICATIONS

INITIAL PACKAGE TO NOTIFY ORGANIZATION AND INDIVIDUAL

LOCAL ORGANIZATION LETTER WITH SOR	L-2
SAMPLE SOR (ENCLOSURE 1 TO LETTER)	L-4
SECURITY CONCERNS AND SUPPORTING ADVERSE INFORMATION	L-5
INSTRUCTIONS FOR RESPONDING TO SOR	L-6
SAMPLE APPLICABLE PERSONNEL SECURITY GUIDELINES (ENCLOSURE 2 TO LETTER)	L-9
SOR RECEIPT AND STATEMENT OF INTENTION (ENCLOSURE 3 TO LETTER)	L-10
FORM REQUESTING PERSONNEL SECURITY INVESTIGATION	L-11

PACKAGE TO INFORM ORGANIZATION AND INDIVIDUAL OF DENIAL

LOCAL ORGANIZATION LETTER WITH LOD	L-12
SAMPLE LETTER OF DENIAL (ENCLOSURE TO LETTER)	L-13
NOTICE OF INTENT TO APPEAL	L-15
INSTRUCTIONS FOR APPEALING A LETTER OF DENIAL/REVOCATION (LOD)	L-16

LOCAL ORGANIZATION LETTER WITH STATEMENT OF REASONS (SOR)

FROM: DIRECTOR, (COMPONENT) CENTRAL ADJUDICATION FACILITY
TO: DIRECTOR, SERVICE GRAPHICS FACILITY, WASHINGTON, DC
SUBJECT: RESPONSIBILITY FOR HANDLING STATEMENT OF REASONS (SOR)
REFERENCE: (A) (COMPONENT PERSONNEL SECURITY REGULATION)
ENCLOSURE: 1. SOR
2. SOR RECEIPT AND STATEMENT OF INTENTION
3. FORM FOR REQUESTING (PERSONNEL SECURITY INVESTIGATION)

1. THE PURPOSE OF THIS LETTER IS TO PROVIDE INSTRUCTIONS FOR ACTIONS REQUIRED BY YOUR ORGANIZATION RELATED TO THE INDIVIDUAL NAMED IN THE ENCLOSED SOR. SINCE DENIAL OR REVOCATION OF ACCESS ELIGIBILITY CAN HAVE A SEVERE IMPACT ON INDIVIDUALS AND THEIR CAREERS, PROCEDURES REQUIRED BY REFERENCE (A) MUST BE CLOSELY FOLLOWED TO ENSURE THAT BOTH SECURITY AND FAIRNESS REQUIREMENTS ARE MET.

2. YOUR ORGANIZATION IS RESPONSIBLE FOR COMPLETING THE FOLLOWING ACTIONS WITH REGARD TO THE INDIVIDUAL NAMED IN THE SOR:

A. CONSIDER WHETHER OR NOT TO SUSPEND ACCESS TO CLASSIFIED INFORMATION AND ASSIGNMENT OF THE INDIVIDUAL TO NONSENSITIVE DUTIES PENDING A FINAL PERSONNEL SECURITY DECISION. FAILURE TO DO SO COULD RESULT IN AN INCREASED LEVEL OF SECURITY RISK.

B. DESIGNATE A PERSON FROM YOUR ORGANIZATION AS THE POINT OF CONTACT (POC) IN THIS MATTER PURSUANT TO PARAGRAPH 8-201(A), REFERENCE (A), ABOVE. THIS PERSON WILL SERVE AS A LIAISON BETWEEN THE (COMPONENT) CENTRAL ADJUDICATION FACILITY (CAF) AND THE INDIVIDUAL.

3. THE POC FROM YOUR ORGANIZATION SHOULD:

A. PROMPTLY DELIVER ENCLOSURE (1) TO THIS LETTER, THE SOR AND ITS ENCLOSURES, TO THE NAMED INDIVIDUAL.

B. COMPLETE AND FORWARD ENCLOSURE (2) TO THIS LETTER TO THE CAF WITHIN 10 CALENDAR DAYS. ENSURE THAT PARTS I, II, AND III ARE ALL COMPLETED. THIS FORM NOTIFIES THE CAF WHETHER THE INDIVIDUAL INTENDS TO RESPOND TO THE SOR AND WHETHER YOUR ORGANIZATION HAS GRANTED A TIME EXTENSION.

C. ADVISE THE INDIVIDUAL THAT HE OR SHE SHOULD NOT ATTEMPT TO COMMUNICATE DIRECTLY WITH THE CAF EXCEPT IN WRITING, AND THAT, IF NECESSARY, HE OR SHE SHOULD SEEK THE ASSISTANCE OF YOUR ORGANIZATION'S DESIGNATED POC. ALSO, ENSURE THAT THE INDIVIDUAL UNDERSTANDS THAT HE OR SHE IS ENTITLED TO OBTAIN LEGAL COUNSEL OR OTHER ASSISTANCE BUT THAT THIS MUST BE DONE AT THE INDIVIDUAL'S OWN EXPENSE.

D. ENSURE THAT THE INDIVIDUAL UNDERSTANDS THE CONSEQUENCES OF BEING FOUND INELIGIBLE FOR ACCESS TO CLASSIFIED INFORMATION AND PERFORMANCE OF SENSITIVE DUTIES AND THE SERIOUS EFFECT SUCH A DETERMINATION COULD HAVE ON HIS OR HER CAREER.

E. TAKE PARTICULAR CARE TO ENSURE THAT THE INDIVIDUAL FULLY UNDERSTANDS THAT THE PROPOSED DENIAL OR REVOCATION ACTION WILL BECOME FINAL IF YOUR ORGANIZATION NOTIFIES THE CAF VIA ENCLOSURE (2) THAT THE INDIVIDUAL DOES NOT INTEND TO RESPOND TO THE SOR. ENSURE THAT THE INDIVIDUAL UNDERSTANDS THAT FAILURE TO SUBMIT A TIMELY REPLY WILL RESULT IN FORFEITURE OF ANY FURTHER OPPORTUNITY TO CONTEST THIS UNFAVORABLE PERSONNEL SECURITY DETERMINATION.

F. EXPLAIN PROCEDURES FOR REQUESTING A TIME EXTENSION FOR RESPONDING TO THE SOR. IF THE INDIVIDUAL REQUIRES ADDITIONAL TIME TO OBTAIN COPIES OF INVESTIGATIVE RECORDS AND/OR TO PREPARE HIS OR HER RESPONSE, YOUR ORGANIZATION MAY GRANT AN EXTENSION OF UP TO 30 ADDITIONAL CALENDAR DAYS. THE CAF MUST BE NOTIFIED OF SUCH AN EXTENSION USING ENCLOSURE (2). SEE REFERENCE (A) FOR MORE DETAIL.

G. ASSIST THE INDIVIDUAL IN OBTAINING APPLICABLE REFERENCES AND COPIES OF PERTINENT INVESTIGATIVE FILES. THE SOR IS USUALLY BASED ON INVESTIGATIVE INFORMATION FROM THE DEFENSE INVESTIGATIVE SERVICE (DIS) AND/OR ANOTHER INVESTIGATIVE AGENCY. IF THE INDIVIDUAL DESIRES COPIES OF RELEASABLE INFORMATION PERTINENT TO THIS SOR, A REQUEST MAY BE SUBMITTED TO THE CAF USING THE RECEIPT AT ENCLOSURE (2). IF THE INDIVIDUAL WANTS TO OBTAIN A COPY OF THE COMPLETE INVESTIGATIVE FILE, PROVIDE HIM OR HER WITH ENCLOSURE (3) WHICH IS THE FORM FOR REQUESTING [DIS AND/OR OTHER INVESTIGATIVE AGENCY] RECORDS UNDER THE PRIVACY ACT (5 U.S.C. 552A.).

4. ENSURE THAT THE INDIVIDUAL'S RESPONSE TO THE SOR IS PROMPTLY ENDORSED BY APPROPRIATE AUTHORITY AND IMMEDIATELY FORWARDED TO THE CAF. SUBMISSIONS TO THE CAF ARE DEEMED TO HAVE BEEN MADE WHEN ACTUALLY RECEIVED BY THE CAF, OR POSTMARKED, WHICHEVER IS SOONER. THIS ENDORSEMENT SHOULD INCLUDE OBSERVATIONS AND COMMENTS REGARDING THE PERSON'S JUDGMENT, RELIABILITY AND TRUSTWORTHINESS AS WELL AS A RECOMMENDATION REGARDING THE DECISION AT HAND. AN ENDORSEMENT THAT DOES NOT INCLUDE COMMENTS AND A RECOMMENDATION WILL BE TAKEN TO MEAN THAT YOUR ORGANIZATION CONCURS WITH THE UNFAVORABLE PERSONNEL SECURITY DETERMINATION.

5. (ADDITIONAL COMPONENT-SPECIFIC REQUIREMENTS)

6. IF YOU HAVE ANY QUESTIONS, THE POINT OF CONTACT AT THE CAF IS MR. JOHN DOE, DSN 000-0000 OR COMMERCIAL (000) 000-0000, E-MAIL DOEJOHN@CAF.DOD.

STATEMENT OF REASONS (SOR)

FROM: DIRECTOR, [COMPONENT] CENTRAL ADJUDICATION FACILITY
THROUGH: DIRECTOR, SERVICE GRAPHICS FACILITY, WASHINGTON, DC
TO: MR. JOHN DOE, SSN 000-00-0000

SUBJECT: INTENT TO (DENY/REVOKE) ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT IN SENSITIVE DUTIES

REFERENCE: (A) COMPONENT PERSONNEL SECURITY REGULATION

ENCLOSURE: 1. SECURITY CONCERNS AND SUPPORTING ADVERSE INFORMATION
2. INSTRUCTIONS FOR RESPONDING TO A STATEMENT OF REASONS
3. APPLICABLE PERSONNEL SECURITY GUIDELINES

1. A PRELIMINARY DECISION HAS BEEN MADE TO (DENY/REVOKE) YOUR ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR EMPLOYMENT IN SENSITIVE DUTIES. ADVERSE INFORMATION FROM AN INVESTIGATION OF YOUR PERSONAL HISTORY HAS LED TO THE SECURITY CONCERNS LISTED IN ENCLOSURE (1) AND HAS RAISED QUESTIONS ABOUT YOUR TRUSTWORTHINESS, RELIABILITY, AND JUDGMENT. IF THIS PRELIMINARY DECISION BECOMES FINAL, YOU WILL NOT BE ELIGIBLE FOR ACCESS TO CLASSIFIED INFORMATION OR EMPLOYMENT IN SENSITIVE DUTIES AS DEFINED BY REFERENCE (A).

2. YOU MAY CHALLENGE THIS PRELIMINARY DECISION BY RESPONDING, IN WRITING, WITH ANY INFORMATION OR EXPLANATION WHICH YOU THINK SHOULD BE CONSIDERED IN REACHING A FINAL DECISION. ENCLOSURE (2) IS PROVIDED TO ASSIST YOU IF YOU CHOOSE TO RESPOND. ENCLOSURE (3) PROVIDES AN EXTRACT FROM REFERENCE (A) OF THE SPECIFIC PERSONNEL SECURITY GUIDELINES USED IN THE PRELIMINARY DECISION TO (DENY/REVOKE) YOUR ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION EMPLOYMENT IN SENSITIVE DUTIES. THE PRELIMINARY DECISION WILL BECOME FINAL IF YOU FAIL TO RESPOND TO THIS LETTER. YOU MAY OBTAIN LEGAL COUNSEL OR OTHER ASSISTANCE; HOWEVER, YOU MUST DO SO AT YOUR OWN EXPENSE.

3. YOU MUST NOTIFY YOUR (COMPONENT) CENTRAL ADJUDICATION FACILITY (CAF) VIA THE HEAD OF YOUR ORGANIZATION WITHIN 10 CALENDAR DAYS AS TO WHETHER OR NOT YOU INTEND TO RESPOND. IF YOU CHOOSE NOT TO RESPOND, YOU WILL FORFEIT AN OPPORTUNITY TO CONTEST THIS UNFAVORABLE PERSONNEL SECURITY DETERMINATION. SHOULD YOU CHOOSE TO RESPOND, YOUR RESPONSE MUST BE SUBMITTED VIA THE HEAD OF YOUR ORGANIZATION WITHIN 30 CALENDAR DAYS FROM THE DATE YOU RECEIVED THIS LETTER. YOUR ORGANIZATION MAY GRANT UP TO 30 ADDITIONAL CALENDAR DAYS IF YOU SUBMIT A WRITTEN REQUEST TO YOUR SECURITY OFFICE. ADDITIONAL TIME EXTENSIONS MAY ONLY BE GRANTED BY THE CAF. CONTACT THE POINT OF CONTACT WITH THE CAF FOR HELP IN PREPARING AND FORWARDING YOUR NOTICE OF AN INTENT TO RESPOND AND YOUR RESPONSE AND IF YOU WISH TO OBTAIN RELEASABLE INVESTIGATIVE RECORDS USED IN YOUR CASE.

4. IF YOU CURRENTLY HAVE ACCESS TO CLASSIFIED INFORMATION, THIS ACCESS (IS/MAY BE) SUSPENDED PENDING THE FINAL DECISION. PLEASE DIRECT QUESTIONS REGARDING THIS LETTER TO YOUR SECURITY OFFICER OR THE POINT OF CONTACT WITH THE CAF.

SECURITY CONCERNS AND SUPPORTING ADVERSE INFORMATION

SUBJECT OF INVESTIGATION: (MR. JOHN DOE, 000-00-0000)

STATEMENT OF REASONS

1. AVAILABLE INFORMATION TENDS TO SHOW CRIMINAL OR DISHONEST CONDUCT ON YOUR PART:

- A. YOU WERE ARRESTED ON 28 MARCH 1985 IN ARLINGTON, VA, FOR ASSAULT ON A POLICE OFFICER. YOU WERE FOUND GUILTY AND FINED \$4,000.
- B. YOU WERE ARRESTED ON 10 JANUARY 1993 IN FAIRFAX, VA, AND CHARGED WITH INTERFERING WITH AN ARREST. YOU WERE RELEASED ON \$300 BAIL WHICH YOU FORFEITED FOR FAILURE TO APPEAR.
- C. YOU WERE ARRESTED ON 22 JUNE 1994 IN FAIRFAX, VA, ON A BENCH WARRANT AND CHARGED WITH FAILURE TO APPEAR (AS SET FORTH ABOVE). YOU WERE FOUND GUILTY OF INTERFERING WITH AN ARREST ON 10 JANUARY 1993 (AS SET FORTH ABOVE) AND FINED \$400. THE CHARGE OF FAILURE TO APPEAR WAS DISMISSED.

2. AVAILABLE INFORMATION TENDS TO SHOW FINANCIAL IRRESPONSIBILITY ON YOUR PART:

- A. YOU FILED FOR BANKRUPTCY UNDER CHAPTER 7 IN THE U.S. DISTRICT COURT, WASHINGTON, DC ON 10 AUGUST 1987. YOU WERE DISCHARGED FROM DEBTS
- B. A JUDGMENT WAS ENTERED AGAINST YOU FOR \$2,500 ON 20 JULY 1992, IN THE SUPERIOR COURT, WASHINGTON, DC. AS OF 30 JANUARY 1995, THE JUDGMENT HAD NOT BEEN PAID.
- C. AS OF 20 JULY 1994, YOUR CREDIT ACCOUNT WITH THE HECHT COMPANY, WASHINGTON, DC WAS \$350 OVERDUE AND REFERRED FOR COLLECTION.
- D. AS OF 20 JULY 1994, YOUR CREDIT ACCOUNT WITH J.C. PENNEY CO., ARLINGTON, VA, WAS \$500 OVERDUE AND REFERRED FOR COLLECTION.

INSTRUCTIONS FOR RESPONDING TO A STATEMENT OF REASONS (SOR)

A PRELIMINARY DECISION HAS BEEN MADE TO DENY OR REVOKE YOUR ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR EMPLOYMENT IN SENSITIVE DUTIES. THIS PRELIMINARY DECISION WILL AUTOMATICALLY BECOME FINAL IF YOU FAIL TO NOTIFY THE CENTRAL ADJUDICATION FACILITY (CAF) WITHIN 10 DAYS THAT YOU INTEND TO RESPOND TO THE SOR. YOU WILL ALSO LOSE YOUR RIGHT TO APPEAL THAT FINAL DECISION IF YOU DO NOT SUBMIT A TIMELY RESPONSE. IF THIS DECISION BECOMES FINAL, YOU WILL NOT BE ELIGIBLE TO HANDLE CLASSIFIED INFORMATION OR PERFORM SENSITIVE DUTIES. THIS COULD PREVENT YOU FROM CONTINUING IN YOUR PRESENT POSITION OR PURSUING YOUR CURRENT CAREER.

THE SOR IS BASED ON ADVERSE INFORMATION REVEALED BY AN INVESTIGATION INTO YOUR PERSONAL HISTORY. SPECIFIC SECURITY CONCERNS ABOUT YOUR CONDUCT OR BACKGROUND, ALONG WITH SUPPORTING ADVERSE INFORMATION, ARE LISTED IN ENCLOSURE (1) TO THE STATEMENT OF REASONS.

THESE INSTRUCTIONS ARE INTENDED TO HELP YOU PROVIDE THE MOST ACCURATE AND RELEVANT INFORMATION AS TO WHY THE PRELIMINARY DECISION SHOULD BE OVERTURNED. HOWEVER, IT IS ONLY A GUIDE. YOU SHOULD PROVIDE WHATEVER INFORMATION YOU THINK OUGHT TO BE CONSIDERED IN REACHING THE FINAL DECISION.

IT IS IN YOUR BEST INTEREST TO PROVIDE THE MOST COMPLETE AND ACCURATE INFORMATION POSSIBLE AT THIS STAGE IN THE DECISION-MAKING PROCESS. THEREFORE, IF YOU DECIDE TO CHALLENGE THE PRELIMINARY DECISION, YOU MUST RESPOND TO THE STATEMENT OF REASONS AS COMPLETELY AS POSSIBLE.

A. BEFORE RESPONDING

(1) FOLLOW THE INSTRUCTIONS. THE SOR AND THESE INSTRUCTIONS PROVIDE SPECIFIC REQUIREMENTS AND DEADLINES FOR COMPLIANCE. YOU WILL FORFEIT YOUR RIGHT TO APPEAL IF YOU FAIL TO FOLLOW THESE INSTRUCTIONS. YOU MUST NOTIFY THE CAF VIA THE POINT OF CONTACT (POC) WITHIN 10 CALENDAR DAYS AS TO WHETHER OR NOT YOU INTEND TO RESPOND. SHOULD YOU CHOOSE TO RESPOND, YOUR RESPONSE MUST BE SUBMITTED VIA THE HEAD OF YOUR ORGANIZATION WITHIN 30 CALENDAR DAYS FROM THE DATE YOU RECEIVED THE SOR, UNLESS YOU REQUESTED AND WERE GRANTED AN EXTENSION OF TIME.

(2) REVIEW ADVERSE INFORMATION. YOU SHOULD CAREFULLY READ THE SECURITY CONCERNS AND SUPPORTING ADVERSE INFORMATION (ENCLOSURE 1) TO THE SOR TO DETERMINE IF THE FINDINGS ARE ACCURATE AND WHETHER THERE ARE CIRCUMSTANCES THAT WERE NOT INCLUDED AND WHICH MIGHT HAVE A FAVORABLE BEARING IN YOUR CASE. YOU MAY OBTAIN RELEVANT INVESTIGATIVE OR OTHER INFORMATION PERTINENT TO THE ADVERSE INFORMATION LISTED IN ENCLOSURE (1) TO THE SOR. IN ADDITION, YOU MAY OBTAIN A COMPLETE COPY OF RELEASABLE INVESTIGATIVE RECORDS CONCERNING YOUR PERSONAL HISTORY UNDER THE PROVISIONS OF THE PRIVACY ACT. YOUR SECURITY OFFICER OR POINT OF CONTACT WITH THE CAF CAN HELP YOU OBTAIN COPIES OF THESE RECORDS. IF YOU DO SUBMIT A REQUEST FOR YOUR INVESTIGATIVE RECORDS, MAKE SURE TO ASK THE POC FOR A TIME EXTENSION TO THE DEADLINE FOR RESPONDING TO THE SOR SINCE IT MAY TAKE UP TO 30 CALENDAR DAYS TO RECEIVE THESE RECORDS.

(3) OBTAIN AND ORGANIZE SUPPORTING DOCUMENTS. GATHER ANY DOCUMENTATION THAT SUPPORTS YOUR CASE. DOCUMENTATION SHOULD BE ORGANIZED ACCORDING TO THE SECURITY CONCERNS PRESENTED IN ENCLOSURE (1). THE MOST USEFUL DOCUMENTS WILL BE THOSE THAT REFUTE, CORRECT, EXPLAIN, EXTENUATE, MITIGATE, OR UPDATE THE ADVERSE

INFORMATION PRESENTED IN ENCLOSURE (1). EXAMPLES OF USEFUL DOCUMENTATION INCLUDE COPIES OF CORRESPONDENCE; COURT RECORDS WITH DETAILS OR DISPOSITIONS OF ARRESTS AND STATUS OF PROBATION; RECEIPTS; COPIES OF CANCELED CHECKS OR LETTER FROM CREDITORS VERIFYING THE STATUS OF DELINQUENT ACCOUNTS; CERTIFICATES OF COMPLETION FOR REHABILITATION PROGRAMS; RELEASES FROM JUDGMENT OR ATTACHMENT; TRANSCRIPTS OF COURT TESTIMONY TAKEN UNDER OATH; PROBATION REPORTS; COPIES OF NEGOTIATED PLEA BARGAINS; ETC. MERE STATEMENTS, SUCH AS "I PAID THOSE BILLS," "I DIDN'T DO IT," OR "IT WASN'T MY FAULT," WILL NOT CARRY AS MUCH WEIGHT AS SUPPORTING DOCUMENTATION. YOU MAY PROVIDE STATEMENTS FROM CO-WORKERS, SUPERVISORS, YOUR COMMANDER, FRIENDS, NEIGHBORS AND OTHERS CONCERNING YOUR JUDGMENT, RELIABILITY AND TRUSTWORTHINESS, AND ANY OTHER INFORMATION THAT YOU THINK OUGHT TO BE CONSIDERED BEFORE A FINAL DECISION IS MADE.

(4). SEEK ASSISTANCE. AN INDIVIDUAL AT YOUR ORGANIZATION HAS BEEN DESIGNATED AS A POINT OF CONTACT WITH THE CAF ON THIS MATTER. IF THIS PERSON CANNOT ANSWER YOUR QUESTIONS, HE OR SHE CAN REQUEST ASSISTANCE FROM HIGHER AUTHORITY. THE PROCESS IS DESIGNED SO THAT INDIVIDUALS CAN REPRESENT THEMSELVES. NONETHELESS, YOU MAY OBTAIN LEGAL COUNSEL OR OTHER ASSISTANCE IN PREPARING YOUR RESPONSE. HOWEVER, IF YOU OBTAIN ASSISTANCE, IT MUST BE AT YOUR OWN EXPENSE.

REMEMBER --- IT IS UP TO YOU TO DECIDE WHETHER TO RESPOND. YOU ARE RESPONSIBLE FOR THE SUBSTANCE OF YOUR RESPONSE AND IT MUST BE SIGNED BY YOU.

B. WRITING A RESPONSE

(1) YOUR RESPONSE SHOULD BE IN THE FORM OF A LETTER FROM YOU TO THE CAF. YOU SHOULD ADDRESS EACH SECURITY CONCERN SEPARATELY. YOU SHOULD ADMIT OR DENY EACH SECURITY CONCERN AND ADMIT OR DENY EACH ITEM OF SUPPORTING ADVERSE INFORMATION.

(2) IT IS ESSENTIAL THAT YOU ADDRESS EACH SECURITY CONCERN AND THE ADVERSE INFORMATION CITED TO SUPPORT IT. PROVIDE ANY INFORMATION THAT EXPLAINS, REFUTES, CORRECTS, EXTENUATES, MITIGATES OR UPDATES EACH SECURITY CONCERN. INCLUDE, WHEREVER POSSIBLE, COPIES OF THE TYPES OF DOCUMENTS DESCRIBED ABOVE. ORGANIZE SUPPORTING DOCUMENTS IN THE ORDER THAT THEY ARE REFERRED TO IN YOUR LETTER AND ENCLOSE COPIES WITH YOUR LETTER. FINALLY, BE SURE TO SIGN AND DATE YOUR LETTER.

(3) THE IMPACT OF YOUR RESPONSE WILL DEPEND ON THE EXTENT TO WHICH YOU CAN SPECIFICALLY REFUTE, CORRECT, EXTENUATE, MITIGATE, OR UPDATE SECURITY CONCERNS AND ADVERSE INFORMATION PRESENTED IN ENCLOSURE (1). INFORMATION THAT IS UNTRUE SHOULD BE SPECIFICALLY REFUTED. IF YOU BELIEVE THAT THE ADVERSE INFORMATION, THOUGH TRUE, DOES NOT SUPPORT THE SECURITY CONCERN OR PRESENTS AN INCOMPLETE PICTURE, YOU SHOULD PROVIDE INFORMATION THAT EXPLAINS YOUR CASE. THIS ADDITIONAL INFORMATION COULD HELP YOU DISPROVE OR LESSEN THE SECURITY CONCERN.

(4) PERSONNEL SECURITY GUIDELINES ARE USED BY DECISION-MAKERS TO DETERMINE WHETHER CERTAIN ADVERSE INFORMATION IS OF SECURITY CONCERN. THE GUIDELINES PERTINENT TO SECURITY CONCERNS IN YOUR CASE ARE LISTED IN ENCLOSURE (3) TO THE SOR. THESE GUIDELINES ARE GENERAL RULES USED BY DECISION-MAKERS IN DETERMINING WHETHER AN INDIVIDUAL SHOULD BE GRANTED ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR PERMITTED TO PERFORM SENSITIVE DUTIES. THE GUIDELINES

PROVIDE A FRAMEWORK FOR WEIGHING ALL AVAILABLE INFORMATION, BOTH FAVORABLE INFORMATION AS WELL AS ADVERSE INFORMATION THAT IS OF SECURITY CONCERN. THE GUIDELINES HELP DECISION-MAKERS MAKE A COMMON-SENSE DETERMINATION CONCERNING AN INDIVIDUAL'S ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION AND PERFORMANCE OF SENSITIVE DUTIES BASED UPON ALL THAT IS KNOWN ABOUT AN INDIVIDUAL'S PERSONAL HISTORY.

(5) PLACE YOUR WRITTEN RESPONSE AND SUPPORTING DOCUMENTS IN A SINGLE ENVELOPE OR PACKAGE AND FORWARD IT TO THE CAF VIA THE HEAD OF YOUR ORGANIZATION. YOUR ORGANIZATION WILL ADD ITS COMMENTS AT THAT TIME. AN ENDORSEMENT BY YOUR ORGANIZATION THAT DOES NOT INCLUDE SUBSTANTIVE COMMENTS AND A RECOMMENDATION WILL BE INTERPRETED TO MEAN THAT YOUR ORGANIZATION CONCURS WITH THE SOR. BE SURE TO MEET THE TIME DEADLINES. YOU WILL BE NOTIFIED IN WRITING OF THE FINAL DECISION. IN MOST CASES THIS DECISION WILL BE MADE WITHIN 60 DAYS. IF THE DECISION IS IN YOUR FAVOR, YOUR ACCESS ELIGIBILITY WILL BE GRANTED OR RESTORED. IF NOT, YOU MAY APPEAL THE DECISION TO A HIGHER AUTHORITY.

APPLICABLE PERSONNEL SECURITY GUIDELINES

THE RELEVANT PERSONNEL SECURITY GUIDELINES ARE LISTED BELOW FOR EACH AREA OF SECURITY CONCERN IN YOUR CASE. THE SECURITY CONCERNS AND SUPPORTING ADVERSE INFORMATION ARE PROVIDED IN ENCLOSURE (1).

SECURITY CONCERN: AVAILABLE INFORMATION TENDS TO SHOW CRIMINAL CONDUCT ON YOUR PART.

A HISTORY OR PATTERN OF CRIMINAL ACTIVITY CREATES DOUBT ABOUT A PERSON'S JUDGMENT, RELIABILITY AND TRUSTWORTHINESS. CONDITIONS THAT SIGNAL SECURITY CONCERN AND MAY BE DISQUALIFYING INCLUDE: (1) ANY CRIMINAL CONDUCT, REGARDLESS OF WHETHER THE PERSON WAS FORMALLY CHARGED; (2) A SINGLE SERIOUS CRIME OR MULTIPLE LESSER OFFENSES.

CONDITIONS THAT COULD MITIGATE SECURITY CONCERNS INCLUDE: (1) THE CRIMINAL BEHAVIOR WAS NOT RECENT; (2) THE CRIME WAS AN ISOLATED INCIDENT; (3) THE PERSON WAS PRESSURED OR COERCED INTO COMMITTING THE ACT AND THOSE PRESSURES ARE NO LONGER PRESENT IN THAT PERSON'S LIFE; (4) THE PERSON DID NOT INTENTIONALLY COMMIT THE ACT AND THE FACTORS LEADING TO THE UNINTENTIONAL VIOLATION ARE NOT LIKELY TO RECUR; (5) THERE IS CLEAR EVIDENCE OF SUCCESSFUL REHABILITATION.

SECURITY CONCERN: AVAILABLE INFORMATION TENDS TO SHOW FINANCIAL IRRESPONSIBILITY OR UNEXPLAINED AFFLUENCE ON YOUR PART.

AN INDIVIDUAL WHO IS FINANCIALLY OVEREXTENDED IS AT GREATER RISK OF HAVING TO CHOOSE BETWEEN SIGNIFICANTLY REDUCING LIFESTYLE OR ENGAGING IN ILLEGAL ACTS TO GENERATE FUNDS. UNEXPLAINED AFFLUENCE IS OFTEN LINKED TO PROCEEDS FROM FINANCIALLY PROFITABLE CRIMINAL ACTS. CONDITIONS THAT SIGNAL SECURITY CONCERN AND MAY BE DISQUALIFYING INCLUDE: (1) A HISTORY OF NOT MEETING FINANCIAL OBLIGATIONS RESULTING IN BANKRUPTCY; (2) DECEPTIVE OR ILLEGAL FINANCIAL PRACTICES SUCH AS EMBEZZLEMENT, EMPLOYEE THEFT, CHECK FRAUD, INCOME TAX EVASION, EXPENSE ACCOUNT FRAUD, FILING DECEPTIVE LOAN STATEMENTS, AND OTHER INTENTIONAL FINANCIAL BREACHES OF TRUST; (3) BEING UNABLE TO SATISFY DEBTS INCURRED TO CREDITORS; (4) UNEXPLAINED AFFLUENCE; (5) FINANCIAL PROBLEMS THAT ARE LINKED TO GAMBLING, DRUG ABUSE, ALCOHOLISM, OR OTHER ISSUES OF SECURITY CONCERN.

CONDITIONS THAT COULD MITIGATE SECURITY CONCERNS INCLUDE: (1) THE BEHAVIOR WAS NOT RECENT; (2) IT WAS AN ISOLATED INCIDENT; (3) THE CONDITIONS THAT RESULTED IN THE BEHAVIOR WERE LARGELY BEYOND THE PERSON'S CONTROL (E.G., LOSS OF EMPLOYMENT, A BUSINESS DOWNTURN, UNEXPECTED MEDICAL EMERGENCY, OR A DEATH, DIVORCE OR SEPARATION); (4) THE PERSON HAS RECEIVED OR IS RECEIVING COUNSELING FOR THE PROBLEM AND THERE ARE CLEAR INDICATIONS THAT THE PROBLEM IS BEING RESOLVED OR IS UNDER CONTROL; (5) THE AFFLUENCE RESULTED FROM A LEGAL SOURCE; AND (6) THE INDIVIDUAL INITIATED A GOOD-FAITH EFFORT TO REPAY OVERDUE CREDITORS.

SOR Receipt and Statement of Intention

From: Director, Service Graphics Facility
To: Director, (Component) Central Adjudication Facility

Subject: Acknowledgment of Receipt for Statement of Reasons

1. I acknowledge receipt and delivery of your Statement of Reasons (SOR) to Mr. John Doe, SSN 000-00-0000. Parts I, II, III and IV of this form have been completed as requested.

PART I

I have received an SOR on this date from the (Component) Central Adjudication Facility.

(Signature)

(Date)

PART II

I intend to:

- a. ☐ submit no reply to the SOR.
- b. ☐ respond to the SOR but have requested an extension for the following reasons:

- c. ☐ respond via my organization head within 30 calendar days of the date I acknowledged receipt of the SOR.

(Signature)

(Date)

PART III

Check one of the following:

- a. ☐ I request relevant copies of documents and records upon which the SOR is based;
- b. ☐ I do not desire relevant copies of documents and records upon which the SOR is based.

PART IV

This organization

- a. ☐ has not granted an extension.

- b. ☐ has granted an extension until _____

(Date)

Point of Contact: _____

(Print Name)

(Position)

REQUEST FOR NOTIFICATION OF ACCESS TO PERSONAL RECORDS		
SUBMIT TO: DEFENSE INVESTIGATIVE SERVICE, PERSONNEL INVESTIGATIONS CENTER ATTN: D0801.0, P.O. BOX 1211, BALTIMORE, MD 21203-1211		
SECTION I - PRIVACY ACT ADVISEMENT		
<p>Requesting personal information concerning you including your social security number (SSN) is authorized by 5 U.S.C. 552a. Providing all or part of this information is voluntary. However, without it the Defense Investigative Service (DIS) may not be able to identify records. The information provided herein will be used to identify and release records pertaining to the individual identified in the request and to protect the privacy of individuals to whom DIS extends records. This information will be retained in the files of DIS and may be released to other components or agencies for official purposes.</p>		
SECTION II - RECORD IDENTIFICATION AND REQUEST FOR ACTION		
1. FULL NAME(S) AND MAILING ADDRESS <small>(Please print or type)</small>	2. TEL NO. (Area code)	3. SOCIAL SECURITY NUMBER
4. DATE OF BIRTH	5. SERVICE NUMBER	
6. TITLE/RANK	7. PLACE OF BIRTH	
8. DESCRIPTION OF RECORD(S) SOUGHT <small>(Investigation Reports, etc.)</small>		
9. INFORMATION WHICH MAY ASSIST IN LOCATING RECORD(S) <small>(Assignment/contract with DIS or military service, dates) of investigation(s), maiden name, alias, etc.)</small>		
10. ACTIONS REQUESTED <input type="checkbox"/> NOTIFICATION OF EXISTENCE OF RECORD(S) <input type="checkbox"/> IDENTITY OF ACTIVITIES TO WHICH RECORDS DISCLOSED <input type="checkbox"/> OTHER		<input type="checkbox"/> REVIEW OF RECORDS AT DIS <input type="checkbox"/> COPY OF RECORDS
11. I AUTHORIZE THE FOLLOWING PERSON TO RECEIVE THE REQUESTED RECORDS FOR ME <small>(Name, address, and tel no.)</small>		SIGNATURE
12. CERTIFICATION: I certify that the above information is correct and that I am the person described in Steps 1 through 7.		SECTION III - NOTARY CERTIFICATION OF REQUESTER IDENTIFICATION <small>Federal warrantless subject to criminal penalties, See Pub Law 93-579, 88 Stat 1962, U.S.C. 91a(1)</small> I, _____ a Notary Public in and for the County (City) and State of _____ hereby certify that on the _____ day of _____ 19____, before me personally appeared _____ who is known by me to be the identical person whose name is subscribed to, and who signed and executed the foregoing instrument, in witness whereof, I have hereunto set my hand and official seal this day and year above. My commission expires _____ <div style="text-align: right;">Notary Public</div>
SECTION IV - AGENCY RECEIPT		
DATE RECEIVED AT DIS	IDENTITY VERIFIED AT DIS	DIS CONTROL NUMBER

LOCAL ORGANIZATION LETTER WITH LOD

FROM: DIRECTOR, (COMPONENT) CENTRAL ADJUDICATION FACILITY
TO: DIRECTOR, SERVICE GRAPHIC FACILITY, WASHINGTON, DC

SUBJECT: RESPONSIBILITIES FOR HANDLING LETTER OF (DENIAL/REVOCATION)

ENCLOSURE: 1. LETTER OF DENIAL/REVOCATION (LOD)
2. LOD RECEIPT

1. A DECISION HAS BEEN MADE BY THE CENTRAL ADJUDICATION FACILITY (CAF) TO (DENY/REVOKE) THE (SECURITY CLEARANCE, SCI ACCESS, EMPLOYMENT IN SENSITIVE DUTIES) OF THE INDIVIDUAL NAMED IN THE ENCLOSED LOD. THE PURPOSE OF THIS LETTER IS TO PROVIDE INSTRUCTIONS FOR ACTIONS REQUIRED BY YOUR ORGANIZATION.

2. IF NOT ALREADY ACCOMPLISHED, YOUR ORGANIZATION IS RESPONSIBLE FOR COMPLETING THE FOLLOWING ACTIONS WITH REGARD TO THE INDIVIDUAL NAMED IN THE LOD:

A. TERMINATE ACCESS TO CLASSIFIED INFORMATION AND/OR ASSIGNMENT TO SENSITIVE DUTIES.

B. DESIGNATE A PERSON FROM YOUR ORGANIZATION AS THE POINT OF CONTACT IN THIS MATTER.

3. YOUR POINT OF CONTACT (POC) ON THIS MATTER SHOULD PROMPTLY DELIVER ENCLOSURE (1) TO THE NAMED INDIVIDUAL. HAVE THE INDIVIDUAL SIGN AND DATE ENCLOSURE (2) UPON RECEIPT OF THE LOD. THIS SIGNATURE VERIFIES RECEIPT OF THE LOD AND SHOULD BE RETAINED BY YOUR ORGANIZATION UNTIL THE FINAL DISPOSITION OF THE APPEAL.

4. IF THE SUBJECT RESPONDED TO THE STATEMENT OF REASONS, YOUR POC SHOULD:

A. ENSURE THE INDIVIDUAL UNDERSTANDS THAT HE HAS 10 CALENDAR DAYS, FROM RECEIPT OF THE LOD, TO SUBMIT A NOTICE OF INTENT TO APPEAL AND TO ELECT WHETHER TO APPEAL IN WRITING TO THE PERSONNEL SECURITY APPEALS BOARD (PSAB) OR TO APPEAR IN PERSON BEFORE A DEFENSE OFFICE OF HEARINGS AND APPEALS (DOHA) ADMINISTRATIVE JUDGE (AJ). HE MUST NOTIFY YOUR ORGANIZATION OF HIS INTENDED ACTION. ANY EXTENSIONS TO THIS DEADLINE MUST BE SUBMITTED IN WRITING TO THE PSAB.

B. ENSURE THAT THE INDIVIDUAL UNDERSTANDS THAT HE MAY ELECT TO APPEAL IN WRITING DIRECTLY TO THE PSAB OR TO REQUEST A PERSONAL APPEARANCE BEFORE A DOHA AJ. IF THE INDIVIDUAL DESIRES A PERSONAL APPEARANCE, THE REQUEST MUST BE IN WRITING. IT MUST BE SENT TO DOHA WITHIN 10 CALENDAR DAYS OF THE INDIVIDUAL'S RECEIPT OF THE LOD. IF THE INDIVIDUAL DESIRES TO APPEAL IN WRITING DIRECTLY TO THE PSAB, IT MUST BE FILED WITHIN 30 CALENDAR DAYS OF RECEIPT OF THE LOD. A FORM FOR THE NOTICE OF INTENT TO APPEAL HAS BEEN PROVIDED AS AN ENCLOSURE TO THE LOD.

5. IF THE SUBJECT DID NOT RESPOND TO THE STATEMENT OF REASONS, YOUR POC SHOULD INFORM THE INDIVIDUAL THE DECISION IS FINAL AND THE APPEAL PROCESS IS CONCLUDED. EXCEPTIONS MAY ONLY BE GRANTED BY THE CAF.

6. IF YOUR ORGANIZATION OR THE NAMED INDIVIDUAL HAS ANY QUESTIONS, THE POC SHOULD COMMUNICATE WITH THE PRESIDENT, PSAB, AT DSN 000-0000 OR COMMERCIAL 000-00-0000, OR THE DIRECTOR, DOHA, AT AUTOVON 226-4598 OR COMMERCIAL 703-696-4598.

LETTER OF DENIAL/REVOCATION(LOD)

FROM: DIRECTOR (COMPONENT) CENTRAL ADJUDICATION FACILITY
THROUGH: DIRECTOR, SERVICE GRAPHIC FACILITY, WASHINGTON, D.C.
TO: MR. JOHN DOE, SSN 000-00-0000

SUBJECT: FINAL (DENIAL/REVOCATION) OF ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR (EMPLOYMENT IN SENSITIVE DUTIES)

REFERENCE: (A) OUR LTR (SER XXX) OF (DATE)
(B) PERSONNEL SECURITY REGULATION
(C) YOUR LTR OF (DATE)

ENCLOSURE: 1. NOTICE OF INTENT TO APPEAL
2. INSTRUCTIONS FOR APPEALING A LETTER OF (DENIAL/REVOCATION)

1. REFERENCE (A) INFORMED YOU OF OUR INTENT TO [DENY/REVOKE] YOUR ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION (OR EMPLOYMENT IN SENSITIVE DUTIES). AN ENCLOSURE OF THIS REFERENCE LISTED SECURITY CONCERNS AND SUPPORTING ADVERSE INFORMATION SUPPORTING THIS PRELIMINARY DECISION. THE CONTENTS OF YOUR RESPONSE HAVE BEEN CAREFULLY CONSIDERED. OUR FINAL ASSESSMENT OF THE SECURITY CONCERNS PRESENTED IN REFERENCE (A) IS AS FOLLOWS:

A. CRIMINAL CONDUCT - THE INFORMATION YOU PROVIDED SUCCESSFULLY MITIGATED THE SECURITY CONCERNS RELATED TO YOUR ARREST ON 28 MARCH 1985. HOWEVER, YOU DID NOT SUFFICIENTLY ADDRESS OR PROVIDE ANY NEW INFORMATION TO EXPLAIN OR MITIGATE THE OTHER ADVERSE INFORMATION (ITEMS 1B AND 1C). YOUR CRIMINAL CONDUCT IS STILL OF SECURITY CONCERN.

B. FINANCIAL IRRESPONSIBILITY - WHILE YOU PROVIDED AN EXPLANATION FOR THE SUPERIOR COURT JUDGMENT, YOU DID NOT SUFFICIENTLY ADDRESS OR PROVIDE ANY NEW INFORMATION TO EXPLAIN THE OTHER ADVERSE INFORMATION (ITEMS 2A, 2C AND 2D). YOUR FINANCIAL IRRESPONSIBILITY IS STILL OF SECURITY CONCERN.

2. GIVEN THE REMAINING SECURITY CONCERNS, EFFECTIVE THIS DATE, WE HAVE (DENIED/REVOKED) YOUR ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION AND FOR ASSIGNMENT TO A SENSITIVE POSITION USING THE PROVISIONS OF REFERENCE (B).

3. YOU MAY APPEAL THIS LETTER OF DENIAL (LOD) IN ONE OF TWO WAYS: (1) BY NOTIFYING THE PERSONNEL SECURITY APPEAL BOARD (PSAB) WITHIN 10 CALENDAR DAYS AFTER YOU RECEIVE THIS LOD OF YOUR INTENT TO APPEAL DIRECTLY TO THE PSAB AND BY PROVIDING THE PSAB WITHIN THE NEXT 30 CALENDAR DAYS WITH ANY SUPPORTING MATERIAL NOT ALREADY PROVIDED AS TO WHY THE LOD SHOULD BE OVERTURNED; OR (2) BY REQUESTING A PERSONAL APPEARANCE BEFORE AN ADMINISTRATIVE JUDGE TO PRESENT YOUR CASE. IF YOU REQUEST A PERSONAL APPEARANCE, IT MUST BE SENT TO THE DIRECTOR, DEFENSE OFFICE OF HEARINGS AND APPEALS (DOHA), POST OFFICE BOX 3656, ARLINGTON, VIRGINIA, 22203 (FAX NO. 703-696-6865) WITHIN 10 CALENDAR DAYS OF YOUR RECEIPT OF THE LOD. A FORM (ENCLOSURE 1) FOR REQUESTING A PERSONAL APPEARANCE IS APPENDED. IN EITHER CASE, INFORM THE HEAD OF YOUR EMPLOYING ORGANIZATION THAT YOU ARE SUBMITTING AN APPEAL. INSTRUCTIONS FOR PREPARING AND EXECUTING AN APPEAL ARE PROVIDED AT ENCLOSURE 2.

MARCH 1996

4. IF YOU APPEAL, THE CASE FILE INCLUDING ALL OF THE INFORMATION YOU SUPPLIED IN ACCORDANCE WITH REFERENCE (C) WILL BE FORWARDED TO EITHER THE PSAB OR THE DOHA FOR CONSIDERATION. IF YOU REQUIRE AN EXTENSION TO A DEADLINE, YOU MUST MAKE YOUR REQUEST IN WRITING TO THE PSAB OR THE DOHA AND NOTIFY THE HEAD OF YOUR ORGANIZATION.

5. QUESTIONS REGARDING THIS LOD SHOULD BE DIRECTED TO POC DESIGNATED BY YOUR ORGANIZATION.

USE THE FOLLOWING IF THE INDIVIDUAL DID NOT RESPOND TO SOR:

1. REFERENCE (A) INFORMED YOU OF OUR INTENT TO (DENY/REVOKE) YOUR ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION AND FOR ASSIGNMENT TO SENSITIVE DUTIES.

2. REFERENCE (A) FURTHER INFORMED YOU THAT THE UNFAVORABLE PERSONNEL SECURITY DECISION WOULD BECOME AUTOMATICALLY FINAL IF YOU FAILED TO SUBMIT A TIMELY RESPONSE.

3. BECAUSE WE HAVE RECEIVED NO TIMELY RESPONSE, YOUR ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR PERFORMANCE OF SENSITIVE DUTIES IS HEREBY (DENIED/REVOKED). THIS DECISION IS FINAL AND IS NOT SUBJECT TO FURTHER APPEAL.

MARCH 1996

Notice of Intent to Appeal**PART I**

I, (last name), (first name), (middle initial), social security number (000-00-0000), received a Letter of Denial/Revocation from (Name of CAF) dated MMDDYY. I elect (check one of the following):

() to appeal directly to PSAB

() a personal appearance before a DOHA Administrative Judge

PART II

The following information is provided so that I can be contacted by the PSAB or DOHA:

a. Duty Address:

b. Duty Phone:

c. Home Address:

d. Home Phone:

PART III

This Notice must be sent to the President of the PSAB (address), or the Director, Defense Office of Hearings and Appeals, Post Office Box 3656, Arlington, Virginia 22203 (FAX No. (703)-696-6865) within 10 calendar days from receipt of the Letter of Denial/Revocation (LOD).

Signature

Date

MARCH 1996

INSTRUCTIONS FOR APPEALING A LETTER OF DENIAL/REVOCATION (LOD)

A DECISION HAS BEEN MADE TO DENY OR REVOKE YOUR ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR PERFORMANCE OF SENSITIVE DUTIES. THIS MEANS THAT YOUR ARE NOT ELIGIBLE TO HANDLE CLASSIFIED INFORMATION OR PERFORM SENSITIVE DUTIES. THIS COULD PREVENT YOU FROM CONTINUING IN YOUR PRESENT POSITION OR PURSUING YOUR CURRENT CAREER. THE LETTER OF DENIAL OR REVOCATION (LOD) EXPLAINS THIS DECISION. IT IS BASED ON ADVERSE INFORMATION WHICH RAISES SECURITY CONCERNS ABOUT YOUR TRUSTWORTHINESS, RELIABILITY OR JUDGMENT.

A. HOW TO APPEAL

THE LOD CAN BE APPEALED IN ONE OF TWO WAYS:

1. YOU MAY REQUEST A PERSONAL APPEARANCE BEFORE AN ADMINISTRATIVE JUDGE (AJ) FROM THE DEFENSE OFFICE OF HEARINGS AND APPEALS (DOHA). THIS APPEARANCE IS INTENDED TO PROVIDE YOU WITH AN ADDITIONAL OPPORTUNITY TO PRESENT A FULL PICTURE OF YOUR SITUATION. YOU WILL HAVE AN OPPORTUNITY TO ORALLY RESPOND TO THE SECURITY CONCERNS NOTED IN THE LOD AND SUBMIT SUPPORTING DOCUMENTATION TO THE AJ WHO WILL MAKE A RECOMMENDATION TO THE PERSONNEL SECURITY APPEAL BOARD (PSAB). THE PSAB WILL CONSIDER BOTH YOUR WRITTEN RECORD AND THE RESULTS OF THE PERSONAL APPEARANCE IN MAKING ITS FINAL DECISION.

2. YOU MAY, HOWEVER, PREFER TO SUBMIT A WRITTEN APPEAL TO THE PSAB AND FOREGO THE PERSONAL APPEARANCE. IF YOU SUBMIT A WRITTEN APPEAL, YOU MAY ALSO PROVIDE SUPPORTING DOCUMENTATION. HAVING OR NOT HAVING A PERSONAL APPEARANCE WILL NOT BIAS THE PSAB IN MAKING A FAIR DETERMINATION IN YOUR CASE.

YOU MUST ELECT EITHER (1) OR (2); YOU MAY NOT DO BOTH.

B. APPEALING WITHOUT A PERSONAL APPEARANCE

IF YOU CHOOSE TO APPEAL WITHOUT A PERSONAL APPEARANCE, YOUR WRITTEN RESPONSE SHOULD PROVIDE WHATEVER INFORMATION YOU THINK OUGHT TO BE CONSIDERED IN THE FINAL DECISION. YOU SHOULD TRY TO SPECIFICALLY EXPLAIN, REFUTE, EXTENUATE, MITIGATE OR UPDATE THE SECURITY CONCERNS PRESENTED IN THE LOD.

YOU SHOULD REVIEW ENCLOSURE (2) TO THE SOR, "INSTRUCTIONS FOR RESPONDING TO A STATEMENT OF REASONS (SOR)" TO MAKE SURE THAT YOUR APPEAL FOLLOWS THE GUIDELINES OUTLINED IN THAT DOCUMENT. IT WILL HELP YOU UNDERSTAND HOW TO DEVELOP AND WRITE YOUR APPEAL SO THAT IT CAN BEST ADDRESS THE SECURITY CONCERNS IN YOUR CASE. SUPPORTING DOCUMENTS SHOULD BE PROVIDED IN THE ORDER REFERRED TO IN YOUR WRITTEN RESPONSE.

PLACE YOUR WRITTEN APPEAL AND SUPPORTING DOCUMENTS IN A SINGLE ENVELOPE OR PACKAGE AND FORWARD IT TO THE PSAB VIA THE HEAD OF YOUR ORGANIZATION. BE SURE TO SIGN AND DATE YOUR APPEAL AND SUBMIT IT WITHIN 30 CALENDAR DAYS OF YOUR NOTICE OF APPEAL.

C. APPEALING WITH A PERSONAL APPEARANCE

IF YOU CHOOSE TO HAVE A PERSONAL APPEARANCE, YOU MUST PROVIDE DOHA WITH YOUR REQUEST WITHIN 10 CALENDAR DAYS OF RECEIPT OF THE LOD. YOU WILL RECEIVE A NOTICE DESIGNATING THE TIME, DATE AND PLACE FOR THE PERSONAL APPEARANCE, WHICH GENERALLY WILL BE HELD WITHIN 30 CALENDAR DAYS AFTER YOUR REQUEST. THE PERSONAL

APPEARANCE GENERALLY WILL BE CONDUCTED AT OR NEAR YOUR DUTY STATION IF IT IS IN THE LOWER 48 STATES. FOR PEOPLE STATIONED ELSEWHERE, IT WILL BE HELD AT OR NEAR YOUR DUTY STATION OR AT A DOHA FACILITY IN THE WASHINGTON, D.C. OR LOS ANGELES, CALIFORNIA METROPOLITAN AREA.

AT THE APPEARANCE YOU WILL HAVE AN OPPORTUNITY TO PRESENT ORAL AND DOCUMENTARY INFORMATION ON YOUR OWN BEHALF. WHILE THE PERSONAL APPEARANCE IS DESIGNED SO THAT YOU CAN REPRESENT YOURSELF, YOU MAY OBTAIN LEGAL COUNSEL OR OTHER ASSISTANCE AT YOUR OWN EXPENSE TO BE PRESENT AT THE APPEARANCE. IF YOU DESIRE COUNSEL, ARRANGE FOR IT NOW. POSTPONEMENT OF THE PERSONAL APPEARANCE CAN BE GRANTED ONLY FOR GOOD CAUSE.

IN GETTING READY FOR THE PERSONAL APPEARANCE, MAKE SURE THAT YOU ARE PREPARED TO ADDRESS ALL OF THE SECURITY CONCERNS AND SUPPORTING ADVERSE INFORMATION. ALSO, MAKE SURE THAT YOUR SUPPORTING DOCUMENTS ARE ORGANIZED AND READILY ACCESSIBLE FOR PRESENTATION TO THE AJ PRESIDING AT THE APPEARANCE AND FOR USE IN ANSWERING QUESTIONS.

THE AJ PRESIDING AT THE APPEARANCE WILL HAVE ALREADY REVIEWED YOUR CASE FILE. THEREFORE, YOUR GOAL SHOULD BE TO CLARIFY YOUR REASONS FOR OVERTURNING THE LOD AND ADDING ADDITIONAL INFORMATION AND DOCUMENTATION WHEN APPROPRIATE RATHER THAN MERELY TO REPEAT MATERIAL THAT YOU PREVIOUSLY SUBMITTED. YOU WILL NOT HAVE THE OPPORTUNITY TO PRESENT OR CROSS-EXAMINE WITNESSES. IF YOU WANT THE VIEWS OF OTHERS PRESENTED, MAKE SURE THAT YOU OBTAIN THESE VIEWS IN WRITING (E.G., LETTERS OF REFERENCE, LETTERS FROM MEDICAL AUTHORITIES, ETC.) AND THAT YOU PRESENT THESE DOCUMENTS TO THE AJ.

DURING THE APPEARANCE, YOU WILL BE ALLOWED TO MAKE AN ORAL PRESENTATION AND SUBMIT DOCUMENTATION. YOU MAY BE ASKED QUESTIONS. ANSWER CLEARLY, COMPLETELY, AND HONESTLY. THE AJ IS NOT THERE TO PRESENT THE GOVERNMENT'S SECURITY CONCERNS BUT RATHER TO LISTEN TO ANY EXPLANATIONS THAT YOU MAY HAVE CONCERNING YOUR CASE. THIS INDIVIDUAL DID NOT MAKE THE UNFAVORABLE PERSONNEL SECURITY DETERMINATION SET FORTH IN THE LOD, AND IS THERE TO GIVE YOU AN OPPORTUNITY TO PRESENT YOUR CASE AS FULLY AS POSSIBLE.

AT THE END OF THE PERSONAL APPEARANCE, YOU WILL BE GIVEN AN OPPORTUNITY TO MAKE A CLOSING STATEMENT. YOU SHOULD STRESS THE HIGHLIGHTS RATHER THAN REVIEW YOUR ENTIRE CASE. TRY TO SHOW HOW THE WEIGHT OF ALL AVAILABLE INFORMATION SUPPORTS OVERTURNING THE UNFAVORABLE PERSONNEL SECURITY DETERMINATION IN YOUR CASE.

THE AJ WILL REVIEW THE CASE FILE, LISTEN TO YOUR COMMENTS AND REVIEW ANY ADDITIONAL DOCUMENTATION THAT YOU SUBMIT, AND THEN MAKE A RECOMMENDATION TO THE PSAB AS TO WHETHER THE CLEARANCE, ACCESS, OR EMPLOYMENT IN SENSITIVE DUTIES SHOULD BE DENIED, REVOKED OR REINSTATED. THE PSAB IS NOT BOUND BY THE RECOMMENDATION OF THE AJ BUT WILL CONSIDER IT, AS WELL AS ANY ADDITIONAL INFORMATION YOU PRESENT AT YOUR APPEARANCE.

APPENDIX M

STRUCTURE AND FUNCTIONING OF THE PERSONNEL
SECURITY APPEAL BOARD

COMPONENT PERSONNEL SECURITY APPEAL BOARDS (PSABS) SHALL BE STRUCTURED AND FUNCTION TO MEET THE FOLLOWING REQUIREMENTS:

1. THE PSAB WILL BE COMPRISED OF THREE MEMBERS AT THE MINIMUM MILITARY GRADE OF O-5 OR CIVILIAN GRADE OF GM/GS-14. IN CASES WHERE THE APPELLANT IS AT OR ABOVE THE GRADE OF MILITARY O-5 OR GM/GS-14, AT LEAST ONE MEMBER OF THE BOARD WILL BE EQUIVALENT OR SENIOR IN GRADE TO THE APPELLANT.
2. ONE OF THE THREE MEMBERS WILL BE A PERMANENT BOARD MEMBER AND SERVE AS BOARD PRESIDENT. THIS PERSON SHOULD HAVE A THOROUGH KNOWLEDGE OF AND EXPERIENCE IN THE FIELD OF PERSONNEL SECURITY.
3. ONE OF THE THREE MEMBERS WILL BE AN ATTORNEY, UNLESS THE BOARD HAS ACCESS TO LEGAL COUNSEL, AND NOT MORE THAN ONE MEMBER SHALL BE FROM THE SECURITY CAREER FIELD.
4. THE COMPOSITION OF THE BOARD MAY BE CHANGED IF AN APPELLANT WORKS FOR A COMPONENT WITHOUT A PSAB. A SENIOR OFFICIAL OF THAT COMPONENT WILL BE ENTITLED, BUT NOT REQUIRED, TO OCCUPY ONE OF THE THREE BOARD POSITIONS DURING CONSIDERATION OF THE CASE.
5. OFFICIALS FROM THE CENTRAL ADJUDICATION FACILITY WILL NEITHER SERVE AS A MEMBER OF THE BOARD NOR COMMUNICATE WITH BOARD MEMBERS CONCERNING THE MERITS OF AN OPEN CASE.
6. COMPONENT PSABS WILL MEET REGULARLY TO ASSURE TIMELY DISPOSITION OF APPEALS.
7. EACH CASE SHALL BE REVIEWED BY ALL THREE PSAB MEMBERS. APPEALS WILL BE DECIDED BY MAJORITY VOTE OF THE BOARD MEMBERS PRESENT AT A MEETING TO DISCUSS AND VOTE ON THE CASE.
8. COMPONENT PSABS WILL RENDER A FINAL DETERMINATION AND NOTIFY THE INDIVIDUAL (VIA THE INDIVIDUAL'S LOCAL ORGANIZATION) IN WRITING. THE PSAB WILL GENERALLY NOTIFY INDIVIDUALS WITHIN 60 CALENDAR DAYS OF THE RECEIPT OF APPEAL (WITHOUT PERSONAL APPEARANCE) OR 30 CALENDAR DAYS OF RECEIPT OF THE RECOMMENDATION OF THE ADMINISTRATIVE JUDGE (IF A PERSONAL APPEARANCE IS REQUESTED). THIS WRITTEN NOTIFICATION WILL PROVIDE THE REASONS THAT THE PSAB EITHER SUSTAINED OR OVERTURNED THE ORIGINAL DETERMINATION OF THE COMPONENT CENTRAL ADJUDICATION FACILITY. THE PSAB DETERMINATION WILL BE FINAL AND WILL CONCLUDE THE APPEAL PROCESS.
9. THE PSAB SHALL MAINTAIN A REDACTED FILE OF ALL DECISIONS WHICH WILL BE SUBJECT TO REVIEW IN ACCORDANCE WITH THE FREEDOM OF INFORMATION ACT.

APPENDIX N

CONDUCT OF A PERSONAL APPEARANCE BEFORE AN ADMINISTRATIVE JUDGE (AJ)

1. A PERSON APPEALING A LETTER OF DENIAL (LOD) MAY REQUEST A PERSONAL APPEARANCE BY NOTIFYING THE DEFENSE OFFICE OF HEARINGS AND APPEALS (DOHA) IN WRITING AT THE FOLLOWING ADDRESS: DIRECTOR, DEFENSE OFFICE OF HEARINGS AND APPEALS, POST OFFICE BOX 3656, ARLINGTON, VIRGINIA 22203 (FAX NO. 703-696-6865). THE REQUEST MUST BE SENT TO DOHA WITHIN 10 CALENDAR DAYS OF RECEIPT OF THE LOD. AN EXTENSION OF TIME MAY BE GRANTED BY THE DIRECTOR, DOHA OR DESIGNEE FOR GOOD CAUSE DEMONSTRATED BY THE APPELLANT.
2. UPON RECEIPT OF A REQUEST FOR A PERSONAL APPEARANCE, DOHA SHALL PROMPTLY REQUEST THE APPELLANT'S CASE FILE FROM THE APPROPRIATE CAF, ASSIGN THE CASE TO AN AJ, AND PROVIDE A COPY OF THE REQUEST TO THE APPROPRIATE PSAB. THE CAF SHALL PROVIDE THE CASE FILE TO DOHA NORMALLY WITHIN 10 CALENDAR DAYS.
3. THE AJ WILL SCHEDULE A PERSONAL APPEARANCE GENERALLY WITHIN 30 CALENDAR DAYS FROM RECEIPT OF THE REQUEST AND ARRANGE FOR A VERBATIM TRANSCRIPT OF THE PROCEEDING. FOR APPELLANTS AT DUTY STATIONS WITHIN THE LOWER 48 STATES, THE PERSONAL APPEARANCE WILL BE CONDUCTED AT THE APPELLANT'S DUTY STATION OR A NEARBY SUITABLE LOCATION. FOR INDIVIDUALS ASSIGNED TO DUTY STATIONS OUTSIDE THE LOWER 48 STATES, THE PERSONAL APPEARANCE WILL BE CONDUCTED AT THE APPELLANT'S DUTY STATION OR A NEARBY SUITABLE LOCATION, OR AT DOHA FACILITIES LOCATED IN THE WASHINGTON, D.C. METROPOLITAN AREA OR THE LOS ANGELES, CALIFORNIA METROPOLITAN AREA AS DETERMINED BY THE DIRECTOR, DOHA, OR DESIGNEE.
4. TRAVEL COSTS FOR THE APPELLANT WILL BE THE RESPONSIBILITY OF THE EMPLOYING ORGANIZATION.
5. THE AJ WILL CONDUCT THE PERSONAL APPEARANCE PROCEEDING IN A FAIR AND ORDERLY MANNER:
 - A. THE APPELLANT MAY BE REPRESENTED BY COUNSEL OR PERSONAL REPRESENTATIVE AT HIS OWN EXPENSE;
 - B. THE APPELLANT MAY MAKE AN ORAL PRESENTATION AND RESPOND TO QUESTIONS POSED BY HIS COUNSEL OR PERSONAL REPRESENTATIVE, AND SHALL RESPOND TO QUESTIONS ASKED BY THE AJ;
 - C. THE APPELLANT MAY SUBMIT DOCUMENTS RELATIVE TO WHETHER THE LOD SHOULD BE OVERTURNED;
 - D. THE APPELLANT WILL NOT HAVE THE OPPORTUNITY TO PRESENT OR CROSS-EXAMINE WITNESSES;
 - E. UPON COMPLETION OF THE PERSONAL APPEARANCE, THE AJ WILL GENERALLY FORWARD WITHIN 30 CALENDAR DAYS, A WRITTEN RECOMMENDATION TO THE APPROPRIATE PSAB WHETHER TO SUSTAIN OR OVERTURN THE LOD, ALONG WITH THE CASE FILE AND ANY DOCUMENTS SUBMITTED BY THE APPELLANT. A COPY OF THE AJ'S RECOMMENDATION WILL BE PROVIDED TO THE CAF.
6. THE PSAB WILL RENDER A FINAL WRITTEN DETERMINATION STATING ITS RATIONALE AND NOTIFY THE INDIVIDUAL IN WRITING (VIA THE INDIVIDUAL'S EMPLOYING ORGANIZATION) GENERALLY WITHIN 30 CALENDAR DAYS OF RECEIPT OF THE RECOMMENDATION FROM DOHA. THIS DECISION WILL BE FINAL AND WILL CONCLUDE THE APPEAL PROCESS.

ENCLOSURE 1

EXECUTIVE ORDER 10450

SECURITY REQUIREMENTS FOR GOVERNMENT EMPLOYMENT

WHEREAS the interests of the national security require that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States; and

WHEREAS the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the Federal service:

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, including section 1753 of the Revised Statutes of the United States (5 U.S.C. 631); the Civil Service Act of 1883 (22 Stat. 403; 5 U.S.C. 632, et seq.); section 9A of the act of August 2, 1939, 53 Stat. 1148 (5 U.S.C. 118j); and the act of August 26, 1950, 64 Stat. 476 (5 U.S.C. 22-1, et seq.), and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

SECTION 1. In addition to the departments and agencies specified in the said act of August 26, 1950, and Executive Order No. 10237 of April 26, 1951, the provisions of that act shall apply to all other departments and agencies of the Government.

SECTION 2. The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security.

SECTION 3. (a) The appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to investigation. The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security, but in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation), and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation: Provided, that upon request of the head of the department or agency concerned, the Civil Service Commission may, in its discretion, authorize such less investigation as may meet the requirements of the national security.

with respect to per-diem, intermittent, temporary, or seasonal employees, or aliens employed outside the United States. Should there develop at any stage of investigation information indicating that the employment of any such person may not be clearly consistent with the interests of the national security, there shall be conducted with respect to such person a full field investigation, or such less investigation as shall be sufficient to enable the head of the department or agency concerned to determine whether retention of such person is clearly consistent with the interests of the national security.

(b) The head of any department or agency shall designate, or cause to be designated, any position within his department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position. Any position so designated shall be filled or occupied only by a person with respect to whom a full field investigation has been conducted: Provided, that a person occupying a sensitive position at the time it is designated as such may continue to occupy such position pending the completion of a full field investigation, subject to the other provisions of this order: And provided further, that in case of emergency a sensitive position may be filled for a limited period by a person with respect to whom a full field preappointment investigation has not been completed if the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency.

SECTION 4. The head of each department and agency shall review, or cause to be reviewed, the cases of all civilian officers and employees with respect to whom there has been conducted a full field investigation under Executive Order No. 9835 of March 21, 1947, and, after such further investigation as may be appropriate, shall readjudicate, or cause to be readjudicated, in accordance with the said act of August 26, 1950, such of those cases as have not been adjudicated under a security standard commensurate with that established under this order.

SECTION 5. Whenever there is developed or received by any department or agency information indicating that the retention in employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency or his representative, who, after such investigation as may be appropriate, shall review, or cause to be reviewed, and, where necessary, readjudicate, or cause to be readjudicated, in accordance with the said act of August 26, 1950, the case of such officer or employee.

SECTION 6. Should there develop at any stage of investigation information indicating that the employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, the head of the department or agency concerned or his representative shall immediately suspend the employment of the person involved if he deems such suspension necessary in the interests of the national security and, following such investigation and review as he deems necessary, the head of the department or agency concerned shall terminate the employment of such suspended officer or employee whenever he shall determine such termination necessary or advisable in the interests of the national security, in accordance with the said act of August 26, 1950.

SECTION 7. Any person whose employment is suspended or terminated under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950, or pursuant to the said Executive Order No. 9835 or any other security or loyalty program relating to officers or employees of the Government, shall not be reinstated or restored to duty or reemployed in the same department or agency and shall not be reemployed in any other department or agency, unless the head of the department or agency concerned finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of the national security, which finding shall be made a part of the records of such department or agency: Provided, that no person whose employment has been terminated under such authority thereafter may be employed by any other department or agency except after a determination by the Civil Service Commission that such person is eligible for such employment.

SECTION 8. (a) The investigations conducted pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security. Such information shall relate, but shall not be limited, to the following:

(1) Depending on the relation of the Government employment to the national security:

(i) Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.

(ii) Any deliberate misrepresentations, falsifications, or omissions of material facts.

(iii) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.

(iv) Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case.

(v) Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of the national security.

(2) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat or preparation therefor, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

(3) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation,

¹ As amended by Executive Order 10548 of August 2, 1954.

or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.

(4) Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

(5) Knowing membership with specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons (hereinafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State, or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.²

(6) Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

(7) Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

(8) Refusal by the individual, upon the ground of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of his alleged disloyalty or other misconduct.³

(b) The investigation of persons entering or employed in the competitive service shall primarily be the responsibility of the Civil Service Commission, except in cases in which the head of a department or agency assumes that responsibility pursuant to law or by agreement with the Commission. The Commission shall furnish a full investigative report to the department or agency concerned.

(c) The investigation of persons (including consultants, however employed), entering employment of, or employed by, the Government other than in the competitive service shall primarily be the responsibility of the employing department or agency. Departments and agencies without investigative facilities may use the investigative facilities of the Civil Service Commission, and other departments and agencies may use such facilities under agreement with the Commission.

² As amended by Executive Order 11785 of June 4, 1974.

³ As amended by Executive Order 10491 of October 13, 1953.

(d) There shall be referred promptly to the Federal Bureau of Investigation all investigations being conducted by any other agencies which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information relating to any of the matters described in subdivisions (2) through (8)⁴ of subsection (a) of this section. In cases so referred to it, the Federal Bureau of Investigation shall make a full field investigation.

SECTION 9. (a) There shall be established and maintained in the Civil Service Commission a security-investigations index covering all persons as to whom security investigations have been conducted by any department or agency of the Government under this order. The central index established and maintained by the Commission under Executive Order No. 9835 of March 21, 1947, shall be made a part of the security-investigations index. The security-investigations index shall contain the name of each person investigated, adequate identifying information concerning each such person, and a reference to each department and agency which has conducted an investigation concerning the person involved or has suspended or terminated the employment of such person under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950.

(b) The heads of all departments and agencies shall furnish promptly to the Civil Service Commission information appropriate for the establishment and maintenance of the security-investigations index.

(c) The reports and other investigative material and information developed by investigations conducted pursuant to any statute, order, or program described in section 7 of this order shall remain the property of the investigative agencies conducting the investigations, but may, subject to considerations of the national security, be retained by the department or agency concerned. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto except, with the consent of the investigative agency concerned, to other departments and agencies conducting security programs under the authority granted by or in accordance with the said act of August 26, 1950, as may be required for the efficient conduct of Government business.

SECTION 10. Nothing in this order shall be construed as eliminating or modifying in any way the requirement for any investigation or any determination as to security which may be required by law.

SECTION 11. On and after the effective date of this order the Loyalty Review Board established by Executive Order No. 9835 of March 21, 1947, shall not accept agency findings for review, upon appeal or otherwise. Appeals pending before the Loyalty Review Board on such date shall be heard to final determination in accordance with the provisions of the said Executive Order No. 9835, as amended. Agency determinations favorable to the officer or employee concerned pending before the Loyalty Review Board on such date shall be acted upon by such Board, and whenever the Board is not in agreement with such

⁴ As amended by Executive Order 10531 of May 27, 1954.

MARCH 1996

ENCLOSURE 1

favorable determination the case shall be remanded to the department or agency concerned for determination in accordance with the standards and procedures established pursuant to this order. Cases pending before the regional loyalty boards of the Civil Service Commission on which hearings have not been initiated on such date shall be referred to the department or agency concerned. Cases being heard by regional loyalty boards on such date shall be heard to conclusion, and the determination of the board shall be forwarded to the head of the department or agency concerned: Provided, that if no specific department or agency is involved, the case shall be dismissed without prejudice to the applicant. Investigations pending in the Federal Bureau of Investigation or the Civil Service Commission on such date shall be completed, and the reports thereon shall be made to the appropriate department or agency.

SECTION 12. Executive Order No. 9835 of March 21, 1947, as amended, is hereby revoked.²

SECTION 13. The Attorney General is requested to render to the heads of departments and agencies such advice as may be requisite to enable them to establish and maintain an appropriate employee-security program.

SECTION 14. (a) The Civil Service Commission, with the continuing advice and collaboration of representatives of such departments and agencies as the National Security Council may designate, shall make a continuing study of the manner in which this order is being implemented by the departments and agencies of the Government for the purpose of determining:

- (1) Deficiencies in the department and agency security programs established under this order which are inconsistent with the interests of, or directly or indirectly weaken, the national security.
- (2) Tendencies in such programs to deny to individual employees fair, impartial, and equitable treatment at the hands of the Government, or rights under the Constitution and laws of the United States or this order.

Information affecting any department or agency developed or received during the course of such continuing study shall be furnished immediately to the head of the department or agency concerned. The Civil Service Commission shall report to the National Security Council, at least semiannually, on the results of such study, shall recommend means to correct any such deficiencies or tendencies, and shall inform the National Security Council immediately of any deficiency which is deemed to be of major importance.⁵

(b) All departments and agencies of the Government are directed to cooperate with the Civil Service Commission to facilitate the accomplishment of the responsibilities assigned to it by subsection (a) of this section.

(c) To assist the Civil Service Commission in discharging its responsibilities under this order, the head of each department and agency shall, as soon as possible and in no event later than ninety days after receipt of the

² As amended by Executive Order 11785 of June 4, 1974.

⁵ As amended by Executive Order 10550 of August 5, 1954.

final investigative report on a civilian officer or employee subject to a full field investigation under the provisions of this order, advise the Commission as to the action taken with respect to such officer or employee. The information furnished by the heads of departments and agencies pursuant to this section shall be included in the reports which the Civil Service Commission is required to submit to the National Security Council in accordance with subsection (a) of this section. Such reports shall set forth any deficiencies on the part of the heads of departments and agencies in taking timely action under this order, and shall mention specifically any instances of noncompliance with this subsection.⁵

SECTION 15. This order shall become effective thirty days after the date hereof.

Dwight D. Eisenhower

The White House
April 27, 1953

⁵ As amended by Executive Order 10550 of August 5, 1954.

DCAAM 5210.1
MARCH 1996
ENCLOSURE 1

THE WHITE HOUSE

WASHINGTON

November 3, 1965

Dear Mr. Chairman:

I have read with great interest the
recommendations of the Committee
to study personnel investigations and
security practices in the Executive
Branch, and I approve each of them.
You are directed to take the actions
recommended.

Sincerely,

Lyndon B. Johnson

Honorable John Macy, Jr.
Chairman
Civil Service Commission
Washington, D.C.

U.S. CIVIL SERVICE COMMISSION

OFFICE OF THE CHAIRMAN

Washington, D.C. 20415

November 18, 1965

On the basis of a comprehensive review of the Federal employee security program under Executive Order 10450, the President has directed that certain changes be made in the program. These changes, outlined below, will enable us to --

- Carry out more effectively and equitably the operations of the Government's personnel investigative and security programs within the framework of Executive Order 10450;
- Promote greater uniformity in providing safeguards for the rights of individuals with due regard for the interests of the Government; and
- Facilitate the reciprocal use of security clearances among agencies.

Designation of Sensitive Positions

Each department and agency as a minimum shall classify as "sensitive" all positions whose incumbents have access to classified defense information described in Executive Order 10501, i.e., "CONFIDENTIAL," "SECRET," AND "TOP SECRET."

For the purpose of conducting investigations under the program, sensitive positions shall be divided into two categories, critical-sensitive and noncritical-sensitive, as is now done by the Department of Defense, which has approximately 80 percent of all sensitive civilian positions in the Executive Branch. The criteria to be applied by the head of the department or agency in designating a position as critical-sensitive shall be as follows:

Any position the duties of which include:

- (1) Access to TOP SECRET defense information;
- (2) Development or approval of war plans, plans or particulars of future or major or special operations of war, or critical and extremely important items of war;
- (3) Development or approval of plans, policies or programs which affect the overall operations of a department or agency, i.e., policy-making or policy-determining positions;

- (4) Investigative duties, the issuance of personnel security clearances, or duty on personnel security boards; or
- (5) Fiduciary, public contact, or other duties demanding the highest degree of public trust.

Other sensitive positions which do not fall within the above criteria shall be designated as noncritical-sensitive.

Full field investigations shall be conducted on all persons being considered for critical-sensitive positions. They should be conducted on a preappointment basis and the information developed by the investigation should be considered in the personnel selection process. When not feasible in case of emergency, the requirement for completion of a full field investigation prior to appointment may be waived as provided in Section 3(b) of Executive Order 10450. In the event that such a waiver has been obtained, the investigation shall be initiated as soon as possible and not later than three work days after the individual's entrance on duty.

Persons should not ordinarily be assigned to noncritical-sensitive positions until after completion of the national agency checks.

A national agency check and inquiry as described in Section 3(a) of Executive Order 10450 shall be the minimum investigation for a person employed in a noncritical-sensitive position. However, this shall not be construed to preclude the head of a department or agency from initiating a full field investigation on any employee when he considers such action appropriate.

Reinvestigations

The incumbent of each critical-sensitive position shall be required, five years after his appointment, and at least once each succeeding five years, to submit an updated personnel security questionnaire to the appropriate security officer in his department or agency, and the head of the department or agency shall direct a review of the personnel security questionnaire, together with the personnel file of the incumbent, previous reports of investigation concerning him, and any other appropriate documents. A determination shall then be made regarding what further action, if any, is appropriate--for example, a check of local police and credit records, a national agency check, or an updated full field investigation.

Safeguarding the Rights of Applicants and Employees

A person being considered for a sensitive position should, whenever appropriate, have an opportunity to explain or refute derogatory security information developed in an investigation before being rejected or nonselected on security grounds. This practice prevents errors which might otherwise result from mistakes in identity or mitigating circumstances which are unknown to the prospective employing agency.

Before issuing a letter of charges under Executive Order 10450, the Department of Justice shall be consulted to assure that the rights of employees are fully considered. That Department is in the best position to advise agencies whether the proposed charges are fully supported, and the extent to which confrontation and cross-examination of witnesses will be required.

The Department of Justice has taken the position, in view of court decisions, that it is improper to furnish security hearing boards or the heads of agencies with investigative information not made available to the employee whose removal is sought under Executive Order 10450.

Within 90 days from the date of this memorandum, each agency in consultation with its General Counsel shall review its regulations and revise them to make them consistent with the instructions in this letter.

Any questions concerning this letter or the procedures outlined herein may be directed to me or to Mr. Kimbell Johnson, Director, Bureau of Personnel Investigations.

Sincerely yours,

John W. Macy, Jr.
Chairman

ENCLOSURE 2

DCAA CRITICAL-SENSITIVE POSITIONS (REGIONS)

<u>ORGANIZATIONAL TITLE</u>	<u>PD No.</u>
Regional Directors	
Eastern	8508
Northeastern	8509
Central	8510
Mid-Atlantic	8512
Western	8511
Deputy Regional Directors	
Eastern	8522
Northeastern	8523
Central	8524
Mid-Atlantic	8526
Western	8525
Special Assistant to Regional Director for Quality	5120
Regional Audit Managers	5131
Regional Counsel (GM-14)	5097
Regional Counsel (GM-13)	5098
Branch Managers (GM-14)	5130
Branch Managers (GM-13)	5073
Resident Auditors (GM-14)	5130
Resident Auditors (GM-13)	5103
Office of Regional Special Programs	
Regional Special Programs Manager	5020
Chief, Technical Programs Division	5082
Technical Programs Specialist (GM-13)	5081
Chief, Operations Audit Division	5022
Chief, QM/EDP Programs Division	5056
DIIS Microcomputer (DMS) Auditor (GM-13)	5084
DIIS/DMS Staff Specialist (GS-12)	5107
DIIS/DMS Staff Specialist (GS-11) Western	7264
QM Auditor (GM-13)	5051
Computer Programmer Analyst (GS-12)	5077
Computer Specialist (GM-13)	5078
EDP Auditor (GM-13)	5079
Chief, Investigations Support Division	5101
Supervisory Auditor (GM-13)	5102
Auditor (GS-12)	5108

ORGANIZATIONAL TITLE

PD No.

Office of Regional Resources Manager	
Regional Resources Manager	5039
Chief, Information Management Division	5083
Management Analyst (GS-12)	5088
Computer Systems Analyst (GS-12)	5089
Computer Systems Programmer (GS-12)	5109
Chief, Financial Management Division	5091
Chief, Personnel Division	5030
Personnel Management Specialist (GS-12)	5031
Regional Security Officer (RSO)	5106
Security Specialist (GS-11)	5105
Security Specialist (GS-9) (Western)	1267
Security Specialist (GS-9) Central	3038
Security Assistant (Typing) (GS-6) Central	3021
Security Assistant (Typing) (GS-7) Mid-Atlantic	6992
Security Assistant (GS-5) Eastern	1318
Contract Audit Coordinators	
Auditor (Assistant to the Corporate	
Resident Auditor/Contract Audit	
Coordinator) (GM-13)	5122
Supervisory Auditor (Corporate Resident	
Auditor/Contract Audit Coordinator (GM-14)	5123

5136

5137

5138

03-24

03-27

ENCLOSURE 3

DCAA APPOINTMENT AND INVESTIGATION PROCEDURES

Agency personnel and security officers will develop procedures within their respective offices to process the appointments of applicants.

Section 1

Procedures for processing applicants with no prior Federal service or who had a break in Federal service for more than two years

A. Actions by applicants. Applicant's must provide all personal information required by DoD, USOPM and DCAA regulations. This includes completing appropriate investigative forms as quickly as possible, being fingerprinted as required to provide the FBI with an acceptable set of fingerprints, and signing releases as necessary to provide the investigative agency access to relevant records.

B. Actions by personnel officers.

1. Nonsensitive and noncritical-sensitive positions.

a. Review SF 171s, applications, or resumes received from applicants for completeness. If current information is not provided, return for updating prior to initiation of the investigation.

b. Conduct inquiries using guidance in paragraph 3-204.D, if applicant is being considered for appointment.

c. Request SF 85 for nonsensitive positions, or SF 85P or 86 for noncritical-sensitive position, and SF 87. Ensure that the letter forwarding the forms to the applicant does not imply they have been selected for the position, but that they are being considered. Inform the applicant that the forms are needed for review prior to selection and that they will be notified of final selection. The applicant should not be told that he/she is "hired subject to a security investigation," "hired provided a security determination is favorable," or similar wording. Applicants may be told that any offer of employment is subject to favorable results of a required entry security investigation. Advise applicants that if investigation develops suitability information, USOPM or DIS may conduct additional investigation to resolve an issue. Provide guidance to applicant about completing the SF 87.

d. Review the SF 85, 85P or 86 for completeness in accordance with OPM instructions. Complete items A through I on the SF 85 or items A through N on the SF 85P or 86 in accordance with OPM Pamphlet OFI-15. Leave item H blank on the SF 85P and 86. Forward to the financial manager for completion of item J on the SF 85 or item O on the SF 85P or 86.

e. Forward request for/notification of appointment and DCAA Form 5210-43 (the latter if emergency waiver of preappointment security investigation is requested for assignment to a noncritical sensitive position); original of SF 85P or SF 86; one SF 87; one copy of SF 171, application, or

resume; and originals of DCAA Form(s) 5210-20 to the security officer for review and further action. CPO, Headquarters, will prepare DCAA Forms 5210-43 for appointments to noncritical-sensitive positions in FD and forward to the Director, FD, for approval/disapproval.

f. Resolve suitability issues before forwarding to the security officer for action.

g. Notify the security officer no later than ten days after appointment or nonappointment of an applicant. File the completed DCAA Form 5210-43 on the left side of the OPF, if applicant is appointed.

h. Coordinate appointments of individuals from temporary services with the RSO.

2. Critical-sensitive positions. Complete steps for noncritical sensitive positions indicated above, except coordinate with the security officer to obtain forms to initiate a SSBI. The personnel officer will coordinate with the security officer when considering appointments to all critical-sensitive positions.

C. Actions by security officer.

1. Nonsensitive and noncritical-sensitive positions.

a. Review forms for completeness. The SF 87 should be classifiable, properly completed, and signed by the applicant. Resolve any information of security significance before submitting the NACI request to USOPM.

b. Conduct preemployment security inquiries, to include the DCII and OPM SII, on all applicants, whether or not they indicate they have had previous Federal Government employment. Record each inquiry on DCAA Form 5210-46.

c. Complete the "Agency Use Only" section of the SF 85, 85P or SF 86 in accordance with OPM Pamphlet OFI-15 except as follows. On the SF 85 leave item B blank and enter DoD-DCAA in item I. On the SF 85P or 86, enter Code 02B in item A, leave item B blank (unless I&NS check is needed), enter the requesting SOI in item J, enter DD02 in item L, and enter DoD-DCAA in item N. If the applicant cannot provide an approved document shown on DCAA Form 5210-48 to verify citizenship, we can request OPM to conduct an I&NS check by adding Code "H" in item B. of the SF 85/85P/86. If this option is used, the applicant's mother's maiden name must be shown in item 7.b on the SF 85 or in item 8.b on the SF 85P or 86. Forward request for NACI to OPM. Requests for NACIs for appointments to nonsensitive positions should be forwarded to OPM no later than seven days after appointment. When a waiver of preappointment security investigation is processed for appointment to a noncritical-sensitive position, the request for NACI must be forwarded to OPM before the waiver is granted.

d. Forward DCAA Form 5210-43 to the regional director (for regions) or Assistant Director, Resources (for Headquarters) with recommendations whether or not a waiver is in the interest of national security.

e. Return the signed original DCAA Form 5210-43 (if applicable) to the personnel office.

f. Enter dates into the SIS Case Control for notification of the completed NACI from CPS and other incomplete actions.

g. If the NACI is received with incomplete information, WHS will expand the investigation to resolve the issue(s).

"h. For individuals hired from temporary services to perform sensitive duties, obtain SF 86 or SF 85P and FD 258, review for security issues, process request for waiver of required preappointment security investigation, and send all documentation to CPS. For individuals hired from temporary services to perform nonsensitive duties for more than 120 days, obtain SF 85 and send to CPS. CPS will initiate a NAC at DSS for all such individuals appointed to perform sensitive duties and for those appointed to nonsensitive duties for a period to exceed 120 days."

i. After appointment, forward the following to CPS:

(a) One copy of request for/notification of appointment

(b) One copy of DCAA Form 5210-43

(c) One copy of SF 171, application, or resume

(d) One copy of SF 85, 85P, or 86

(e) DCAA Form 5210-31, if clearance is required

(f) One copy of each DCAA Form 5210-46

(g) One copy of each DCAA Form 5210-20, if any

NACIs for Nonsensitive Positions

Forward NACIs completed for assignments to nonsensitive positions to CPO (for Headquarters) or RPO (for Regions) for suitability determination.

After suitability decision, forward the following to CPS:

(1) Original SF 85

(2) One copy of SF 171, application, or resume

(3) One copy of signed Certification of Investigation

(4) One copy of request for/notification of appointment

(5) Original of all other documents pertaining to the NACI received from the USOPM-FIPC Center.

NACIs for Sensitive Positions

NACIs completed for assignments to sensitive positions will be adjudicated by the WHS with notification to CPS. CPS will prepare a C/E Cert for transmission to the appropriate office.

2. Critical-sensitive positions.

a. Upon receipt of request for/notification of appointment and related documentation from the personnel officer, forward the following forms with Privacy Act Statements to the applicant for completion and return as soon as possible:

(1) SF 86 complete with instructions

(2) FD Form 258

(3) PD 70 (for employees who have worked or resided in the Washington, D.C. Area)

Instruct the applicant to retain one copy of the SF 86, as well as the Privacy Act Statements for personal records, and to follow instructions closely when completing the forms in order to prevent delays in completing the investigation and appointment. Instruct the applicant how to obtain fingerprints and offer assistance if necessary. A DCAA Form 5210-48 should also be completed, or a copy of an acceptable I-9 form can be obtained from the OPF at this time to verify citizenship for purpose of SSBI.

b. Upon receipt of the forms identified in subparagraph C.2.a. above, review for completeness and, if necessary, initiate action to have forms completed or corrected.

c. When the forms have been properly completed, prepare DD Form 1879 for SSBI to DIS with an annotation in Item 6 of DD Form 1879 for advance notification of NAC. A confirmation that no other investigation is currently being processed should be shown in Item 17 of the DD Form 1879. The WHS Consolidated Adjudication Facility will be shown in Item 19 "Return Results To" for routine SSBIs and PRs. DD Forms 1879 requesting SSBIs and PRs for SCI access should show DIA Central Clearance Facility in Item 19, "Return Results To", and "DIA SCI", with the SCI billet number, annotated in Item 17. The NAC portion of the SSBI must be favorably adjudicated by WHS before an emergency waiver can be granted. If the applicant has been previously employed in the Federal service, an inquiry should be made with previous employers security offices, the DCII, or OPM SII for previous investigations, and the results recorded on DCAA Form 5210-46.

d. Forward a copy of forms used to request the SSBI with a copy of DCAA Form(s) 5210-46 and DCAA Form(s) 5210-20 to CPS.

e. When the NAC has been adjudicated by WHS and the results received, CPS will notify the office considering appointment. If applicant is still being considered for appointment, the requesting office will forward DCAA Form 5210-43 to the Assistant Director, Resources through CPS.

f. After decision by the Assistant Director, Resources, CPS will forward DCAA Form 5210-43 to the RSO or to CPO (for Headquarters and PD). RSOs will forward DCAA Form 5210-43 to the personnel officer for filing on the left side of the employee's OPF. If for any reason appointment is not made, the personnel office should notify the security office.

D. Requesting Investigation in Hostage Situations.

Applicants or employees who have immediate family members and/or other persons to whom they are bound by ties of affection or obligation residing in a country whose interests are inimical to the U.S., will be requested to complete SF 86 or SF 85P in its entirety. Upon review, the security specialist will determine whether or not an interview and/or additional investigation is necessary. If a determination is made that interview or investigation is necessary, a request will be forwarded to DIS in accordance with paragraph G, Appendix C. The request should specifically refer to the personal interview required in paragraph 2-308.C and 2-304.

Section 2

Processing applicants transferring from another Federal agency or reinstatement to Federal employment with less than two year break in Federal service.

A. Action by applicant. As directed by personnel and security offices.

B. Actions by personnel officer:

All appointments.

1. Resolve suitability issues.

2. Obtain SF 75 information. Investigative data should be recorded verbatim from the OPM stamped SF 171 or Certification of Investigation for NACIS.

3. Prior to appointment, forward request for/notification of appointment and one copy each of SF 171, application, or resume, SF 75, and DCAA Forms 5210-20 to the security officer for completion of preappointment security requirements.

4. Notify the security officer no later than ten days after appointment or nonappointment of applicant.

C. Actions by security officer.

1. Noncritical-sensitive and critical-sensitive positions.

a. Review SF 171, application, or resume and employment inquiries for information of a security significance. If such information exists, resolve (e.g., conduct a subject interview, consider obtaining updated SF 86, or SF 85P, or request additional investigation).

b. Conduct preemployment security inquiry of the applicants releasing security office (if available) to obtain investigation information and determine whether any derogatory information exists. If a security office cannot be located, or if one does not exist, investigative information will be confirmed through the releasing personnel office or by calling the investigating agency central security index. A DCII check should be made on all applicants (including industrial personnel). Security specialists can call CPS for DCII terminal checks. Confirmation of investigations on transferees from IRS will be made through CPS.

c. If adverse suitability or security information is developed during the security inquiry, obtain as much information as possible. A security decision can then be made. In some cases, the decision can be made by obtaining additional information from the employee, but in other cases, it may be necessary to conduct additional formal investigation. If the releasing security office will not discuss adverse information developed by investigation, obtain a copy of the investigation from the investigative agency for transmission to CPS for forwarding to WHS for adjudication prior to appointment. Use OFI Form 79B to request investigations from USOPM and DA Form 1144 to request investigations from DIS. Assistance in obtaining investigations

from other investigative agencies can be obtained by calling CPS. The exception within DoD is that adjudicative determinations made by designated DoD authorities will be mutually and reciprocally accepted without requiring additional investigation unless there has been a break in the individuals military service/civilian employment of greater than two years or unless derogatory information occurred subsequent to the last security determination. In all cases, CPS records will be reviewed prior to hiring a former DCAA employee.

d. Applicants for critical sensitive positions who do not have the required background investigation will be processed in accordance with paragraphs B.2 and C.2, Section 1 of this enclosure.

e. Once a security decision is made, notify the personnel office of approval/disapproval to appoint.

f. If appointment is made based upon satisfactory preemployment security inquiry, forward the following, arranged in the order shown, to CPS no later than ten days after appointment:

- (1) Copy of request for/notification of appointment
- (2) SF 171, application, or resume
- (3) SF 75
- (4) DCAA Form(s) 5210-20
- (5) DCAA Form 5210-31, if clearance is required
- (6) One copy of signature page of a valid classified information nondisclosure agreement, if clearance is required. Forward original SF 312 for filing in OPF. FDSO should forward original SF 312 to CPS.
- (7) DCAA Form 5210-48, if clearance is required
- (8) DCAA Form(s) 5210-46

g. If it is determined during preemployment security inquiries that appropriate security investigation has not been initiated or completed, process the appointment as shown in Section 1, above.

2. Nonsensitive positions.

a. Contact the releasing agency personnel or security office to determine if a NACI has been completed or initiated. If one has not been initiated, request appropriate forms through the personnel office to initiate a NACI. If one has been initiated, request OPM to forward the completed investigation to DCAA.

b. When the NACI is received, forward it to the personnel officer for suitability determination. After suitability determination, forward the following to CPS within ten days of receipt:

- (1) One copy of request for/notification of appointment
- (2) One copy of SF 171, application, or resume
- (3) Original SF 85
- (4) One copy of Certificate of Investigation signed by the personnel officer

DCAAM 5210.1
MARCH 1996
ENCLOSURE 3

- (5) One copy of SF 75, if any
- (6) One copy of DCAA Form(s) 5210-20, if any

If the investigation was confirmed by contacting the releasing office or the investigative agency, forward the following to CPS no later than ten days after applicant is appointed:

- (1) One copy of request for/notification of appointment
- (2) One copy of SF 171, application, or resume
- (3) One copy of SF 75
- (4) One copy of DCAA Form(s) 5210-46
- (5) One copy of DCAA Form(s) 5210-20, if any

Section 3

Processing tentative selectees for regional GM or GS-14 and above critical-sensitive positions who do not have background investigations

A. The CPO, Headquarters, coordinates with CPS to determine if the Director's selectee for a position has the necessary investigation. If not, CPS advises CPO, who ensures that a tentative selection letter is forwarded to the selectee, along with forms to be completed for a SSBI. The selectee is requested to complete the forms and return them to the appropriate RSO. Copies of the letter are furnished the regional personnel and security officers to notify them that a SSBI is necessary prior to appointment, or that a waiver must be granted and a SSBI requested before appointment, if the need to appoint is urgent.

B. When the RPO receives the copy of the tentative selection letter, that official provides the RSO a request for notification of appointment.

C. Upon receipt of completed SSBI forms from the selectee, the RSO reviews the forms for compliance with instructions. The RSO will review the OPF (or ensure its review by the losing region's security office) and forward the request for SSBI to the DIS. If there is sufficient urgency to make the appointment prior to completion of a SSBI (a process that sometimes lasts as long as six months), regional officials will ensure that a DCAA Form 5210-43 is forwarded to the ASO for transmission to the Assistant Director, Resources.

D. DCAA Form 5210-43 must be accompanied by a copy of DD Form 1879 and SF 86 used to request the SSBI, and must adequately justify the need for an emergency appointment instead of awaiting completion of the SSBI. All waivers for these appointments where access to Top Secret is not required, are approved at Headquarters after CPS has reviewed existing information that might preclude a waiver. Appointments that require the incumbent to have interim access to Top Secret information must be approved by the WHS CAP. In those cases, CPS will forward the request and forms to the WHS CAP for action.

E. When the waiver is approved, the original will be forwarded to the RSO. A copy of the waiver is furnished CPO to alert them to prepare a final selection letter to the selectee from the Director. The RSO will forward DCAA Form 5210-43 to the RPO for filing on the left side of the OPF. No final selection letter will be prepared, nor appointment effected, until CPO and regional personnel officials have received a signed DCAA Form 5210-43.

DCAAM 5210.1
MARCH 1996
ENCLOSURE 3

Section 4.

DCAA employees being considered for assignment/reassignment to positions of higher sensitivity

A. Actions by employee. As required by personnel and/or security officers.

B. Actions by personnel officers. In all cases where an incumbent employee is being considered for either temporary or permanent assignment to a position of a higher level of sensitivity, the RPO will provide the RSO a request for/notification of appointment and an updated SF 171, application, or resume, if available, prior to effecting the appointment.

C. Actions by security officer.

1. Upon receipt of request for/notification of appointment and SF 171, application, or resume, review the latter for information of security significance.

2. Prior to appointment, request CPS to review the personnel security file for a record of appropriate investigation and for any adverse information which could preclude the employee's assignment.

3. Notify the personnel officer if appropriate investigation has been completed.

4. If appropriate investigation has not been completed, obtain forms from the employee and request the investigation. If a request for waiver is being considered to make the appointment to a critical-sensitive position and a favorable NAC or NACI has been completed, the original DCAA Form 5210-43, and copies of DD Form 1879 and SF 86 will be forwarded to CPS. The DCAA Form 5210-43 will be forwarded to the Assistant Director, Resources for determination. Once determination is made, the form will be returned to the appropriate security officer for further transmission to the personnel officer. Waivers for appointments to noncritical-sensitive positions will be signed by regional directors.

5. When appointment is made, forward a completed copy of request for/notification of appointment to CPS. In cases where a SSBI was requested, CPS will forward the requesting office a C/E Cert after adjudication of the SSBI by WHS.

Section 5

Hiring foreign national employees in DCAA overseas offices

A. General. Although foreign national employees do not require access to classified information and are not subject to security investigation, it is in the interest of the Agency and national security to hire trustworthy individuals.

B. Procedures. To ensure compliance with the above stated policy, the following procedures will be followed when hiring foreign nationals:

1. Complete a check of local law enforcement and security agencies prior to employment.
2. Request managers in overseas offices to obtain a completed copy of SF 171, application, or resume and SF 85P from the applicant for transmission via fax or mail to the RSO for review.
3. Conduct an inquiry of the DCII.
4. Notify the appropriate personnel management specialists of approval/nonapproval to appoint.
5. Forward the SF 85P, a copy of request for/notification of appointment, DCAA Form 5210-46, if any, and the results of the local agency checks to CPS.

DCAAM 5210.1
MARCH 1996
ENCLOSURE 3

Section 6

Security Processing of Individuals for Special Access Programs (SAPs)

See DCAAI 5205.11, DCAAR 5205.10, and DCAAP 5205.13. Chapter IV, DCAAP 5205.13 provides guidance on the use of DCAA Form 5210-9 for briefings and debriefings of employees selected for participation in SAPs. DCAA Forms 5210-9 completed for employees debriefed from SAPs will be accompanied by a DCAA Form 5210-31, Request for Security Clearance, if clearance is to be retained, or DCAA Form 5210-3, Security Termination Statement, as appropriate.

Section 7

Disposition of Security Clearance and Eligibility Certificates

A. Actions by Agency Security Officer

1. Debrief employees with security clearances who transfer from Headquarters (including FD, DCAI, and TSC) to another DCAA office. Have employee sign DCAA Form 5210-3 and file in CPS. Forward C/E Certs for an uncleared employee to the gaining office if clearance determination has not been made by the gaining office.

2. Determine security clearance requirements for employees transferring from another DCAA office to Headquarters and issue C/E Certs, as appropriate.

3. Issue C/E Certs as needed by the regional offices and FD.

B. Actions by Regional Security Officers

1. Cleared employees transferring to another DCAA region:

Debrief employees with security clearances, destroy C/E Certs (formerly DCAA Form 5210-1 and DCAA Form 5210-6) and forward DCAA Forms 5210-3 to CPS.

2. Cleared employees transferring within the same region:

a. If the same level of clearance is required, forward the C/E Certs to the gaining office; forward DCAA Form 5210-31 to justify retention to CPS.

b. If a different level of clearance is required, forward DCAA Form 5210-31 to CPS for issuance of a new C/E Cert. If no clearance is required at the gaining office, the gaining office will debrief the employee and forward DCAA Form 5210-3 to the RSO for forwarding to CPS.

3. Uncleared employees:

a. For uncleared employees transferring to another DCAA region, forward the C/E Cert to the appropriate RSO who will forward to the gaining office.

b. For uncleared employees who are terminating, annotate the C/E Certs with the termination date and forward to CPS.

4. Determine clearance requirements for employees transferring from another DCAA region or from one office to another within the region.

5. Forward DCAA Form 5210-31, copy of signature page of classified information nondisclosure agreement (if required), and proof of citizenship (if required) to CPS if security clearance is needed at the gaining office. If a clearance is not required, file the RSO copy of the C/E Cert received from the losing office and forward the FAO copy to the appropriate office.

6. Destroy prior certificates when superseded by most recent C/E Certs.

C. Actions by Regional Field Audit Office Security Control Officers

1. Cleared employees transferring to another region:

Debrief employees and forward a signed DCAA Form 5210-3, with FAO copies of C/E Certs, to the RSO.

2. Cleared employees transferring within the same region:

a. The losing office will forward C/E Certs to the RSO.

b. If the same level of clearance is required, the gaining FAO will forward DCAA Form 5210-31 to justify retention to the RSO for forwarding to CPS.

c. If a different level of clearance is required, the gaining FAO will forward DCAA Form 5210-31, with appropriate justification, to the RSO for forwarding to CPS.

d. If no clearance is required at the gaining office, the gaining office will debrief employee and forward DCAA Form 5210-3 to the RSO for forwarding to CPS.

3. When cleared employees terminate employment with DCAA, debrief employee and forward the DCAA Form 5210-3 with the C/E Cert to the RSO.

4. Uncleared employees:

Forward C/E Certs for uncleared employees who are terminating, or transferring to another FAO within the same region, to the RSO with a note reflecting transfer/termination date and reason for leaving.

5. Destroy prior certificates when superseded by most recent C/E Cert.

D. Actions by Field Detachment Security Control Officers

1. When an employee transfers from one FD office to another, the losing office will forward the C/E Cert to the gaining office.

2. If an employee transfers to a DCAA regional office or FAO, debrief the employee, destroy the C/E Cert, and forward DCAA Form 5210-3 through the FDSO to CPS.

3. If an employee terminates employment with DCAA, debrief the employee, and forward the signed DCAA Form 5210-3 through the FDSO to CPS.

4. Destroy prior certificates when superseded by most recent C/E Certs.

ENCLOSURE 4

DCAA BRIEFINGS OUTLINE

I. General: Security education program required by DoDD 5240.6, D.2; DoD 5200.2-R, 9-200; and DoD 5200.1-R, 10-101. Some elements of all three of these apply to all employees, employees in sensitive positions (generally, all of DCAA), and employees with access to classified information.

II. All Employees:

1. Pertinent security regs (general overview, who security manager is, how security regs implemented in DCAA, where they can find regs if needed, obligation to protect official information, telephone monitoring prohibition-DCAAR 4640.2, general office physical security, etc.)
2. Hostile threat briefing (DoDD 5240.6, D and F.1.c "periodic"); reporting requirements of foreign contacts and sanctions for not reporting (DoDD 5240.6, D and F.1 2)
3. Co-worker responsibility to report info with potentially serious security significance (DoD 5200.2-R, 9-104 and Appendix I)

III. Sensitive Incumbents:

1. Initial (DoD 5200.2-R, 9-201)
 - a. All items in II above and standards of conduct (DoD 5200.2-R, 9-103.a, 9-200, 2-200 and Appendix I; and Standards of Conduct)
 - b. Security requirements of particular job (2-R, 9-201.a(1))
 - c. Techniques of hostile intelligence (2-R, 9-201.a(2))
 - d. Prohibitions against disclosure (2-R, 9-201.a(3))
 - e. Penalties for security violations (2-R, 9-201.a(4))
 - f. Obligation to report (2-R, 9-104 and 9-203)
2. Refresher
 - a. Security responsibilities generally (DoD 5200.2-R, 9-200 and 9-203 "periodically")
 - b. The hostile threat (DoD 5240.6, D and F.c "periodic")

IV. Employees With Access to Classified Information:

1. Initial (DoD 5200.1-R, 10-102)
 - a. All items in II and III.a above, DoD 5200.1-R, section 10-101.a - i, as well as following:
 - b. Obligation to report to security manager contacts with individuals of any nationality within or outside the scope of the employee's official activities in which illegal or unauthorized access is sought to classified or otherwise sensitive information and/or the employee is concerned that he

BRIEFINGS OUTLINE continued

or she may be the target of exploitation by a foreign country (DoD 5200.2-R, 9-103.b and 9-203; DoD 5200.1-R, 10-104)

- c. Requirement to report to security manager contacts with individuals of any nationality within or outside the scope of the employee's official activities that appear to indicate an attempt or intention to obtain unauthorized access to proprietary, sensitive, or classified information or technology, offer a reasonable potential for such, or indicate the possibility of continued contact with the foreign national for such purposes (DoD 5200.2-R, 9-103.b and 9-203; added emphasis on DoDD 5240.6, F.1.2 = II.B above)
- d. Information relating to criteria for application of security standards (DoD 5200.2-R, section 9-103.b(2))
- e. Need to sign SF 312 (DoD 5200.1-R, 10-102)

2. Refresher

Annual (DoD 5200.1-R, 10-101 10-103; DoD 5200.2-R, 9-202 and 9-203) [1 hour]

3. Debriefing if any facts or circumstances of a reported contact with a foreign national appear to indicate an attempt or intention to obtain unauthorized access to proprietary, sensitive, or classified information or technology, offer a reasonable potential for such, or indicate the possibility of continued contact with the foreign nation for such purposes (DoD 5200.1-R, 10-104; DoD 5200.2-R, 9-203.b)

4. Termination briefing and need to sign STS (DoD 5200.1-R, 10-105; DoD 5200.2-R, 9-204); [DCAA Form 5210-3]

V. Employees with Access to Special Access Program (SAP) Information:

In addition to briefing/training outlined in IV, above:

- 1. Initial (DCAAI 5205.11, F.6.a and F.3.g and DCAAP 5205.13, Chapter IV).
 - a. Receive a generic briefing administered in accordance with Enclosure 8, DCAAM 5205.1 and DCAAP 5205.13, Chapter IV.**
 - b. Receive a program "read on" briefing administered in accordance with Enclosure 8, DCAAM 5205.1 and DCAAP 5205.13, Chapter IV.
- 2. Refresher (DCAAI 5205.11, F.6.c and DCAAP 5205.13, Chapter IV). Receive periodic SAP oriented security training given either by the RSO, ARSO, or by the senior FAO representative briefed on SAPs.**

BRIEFINGS OUTLINE continued

3. Termination (DCAAI 5205.11, F.S.2 and DCAAP 5205.13, Chapter IV).
Receive a SAP termination briefing when no longer involved in a particular SAP. This briefing will be given by a representative of the government program manager. This representative may be an employee of the government or an employee of the contractor who is "read on" to the program and designated by the program manager to render the debriefing. This debriefing will be arranged by the senior FAO representative "read on" to the particular program.

- ** Any program-unique security aspects of a particular SAP will be presented to all "read on" personnel by the senior FAO representative and/or government customer security representative briefed on the particular program.

- () parentheses = DoD requirements
[] brackets = DCAA requirements

DEPARTMENT OF DEFENSE
DIRECTIVE

USD(P)

February 26, 1986
(Reprinted July 18, 1986)

SUBJECT: Counterintelligence Awareness and Briefing Program

- References:
- (a) National Security Decision Directive 197, "Reporting Hostile Contacts and Security Awareness," November 1, 1985
 - (b) DoD Directive 5240.2, "DoD Counterintelligence," June 6, 1983
 - (c) DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980
 - (d) DoD Directive 5230.24, "Distribution Statements on Technical Documents," November 20, 1984
 - (e) through (j), see enclosure 1

A. PURPOSE

This Directive:

1. Implements reference (a) within the Department of Defense and reference (b) as it pertains to the responsibilities of the Deputy Under Secretary of Defense for Policy, to establish policies and procedures for the conduct and administration of DoD counterintelligence activities.
2. [deleted in reprint of July 18, 1986.]
3. Establishes requirements for the periodic briefing of DoD personnel on hostile intelligence and terrorist threats.
4. Prescribes judicial or administrative sanctions for DoD personnel who fail to comply with the requirements of this Directive.
5. Establishes reporting requirements to the Office of the Secretary of Defense for program oversight and evaluation.

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").
2. It also applies to the extent possible to contractors participating in the Defense Industrial Security Program (reference (c)).

#Reprint (7/18/86)

C. DEFINITIONS

It is DoD policy that:

1. All military personnel, active and reserve (on extended active duty, active duty for training, or inactive duty for training), DoD civilian employees, and DoD contractors report to an appropriate authority information or circumstances that could pose a threat to the security of DoD personnel, resources, or classified or controlled defense information under DoD Directive 5230.24 (reference (d)) and DoD 5400.7-R (reference (e)).
2. All DoD personnel receive periodic briefings on hostile intelligence and terrorist threats, reinforcing the requirements of DoD Directive 2000.12 (reference (f)); and on their responsibility to report any such information to an appropriate authority.
3. Appropriate judicial and administrative action shall be taken when personnel fail to report such required information.

E. RESPONSIBILITIES

1. The Deputy Under Secretary of Defense for Policy (DUSDP) shall:
 - a. Provide policy and direction for reporting, investigating, and exploiting reportable incidents under this Directive, pursuant to National Security Decision Directive 197 (reference (a)) and section F., below.
 - b. Designate one Military Department's foreign counterintelligence (PCI) agency as the Executive Agent for those DoD Components without the counterintelligence capability to implement the investigative aspects of this program.
2. The Secretaries of the Military Departments shall:
 - a. Provide for the conduct, direction, management, coordination, and control of this program, in accordance with this Directive.
 - b. Establish Military Department plans, programs, policies, and procedures to implement this program.
 - c. Ensure that all military and civilian personnel are periodically briefed on the requirements to report the information specified in this Directive.
 - d. Report annually to the OSD as outlined in subsection F.4., below.
3. The Heads of DoD Components (except Military Department Secretaries and the Director, Defense Intelligence Agency) shall:
 - a. Refer reported information involving military personnel assigned to their Components to the Military Department concerned for appropriate investigation and disposition; refer reported information involving

civilian employees employed by their Component in the United States to their servicing DoD FCI agency and, when overseas, to the Military Department responsible for providing administrative and logistical support.

b. Establish policies and procedures to implement this program within their Components. c. Ensure all military and civilian personnel are briefed periodically on the requirements to report the information specified in this Directive.

d. Report annually to the OSD as outlined in subsection F.4., below.

4. The Director, Defense Intelligence Agency (DIA), shall:

a. Coordinate all information reported under this Directive by military personnel assigned to DIA with the appropriate Military Department foreign counterintelligence agency; coordinate all information reported by civilian employees with the Federal Bureau of Investigation (FBI), in accordance with the Joint Agreement (reference (g)); and coordinate internal DIA investigations which uncover evidence that might lead to the arrest or prosecution of a DIA employee with the FBI or a Military Department FCI agency, as appropriate.

b. Establish policies and procedures to implement this Directive within DIA, OJCS, and the headquarters elements of U.S. Unified Commands.

c. Develop for DIA and OJCS a briefing program on security, hostile intelligence, and terrorism threat awareness.

d. Report annually to OSD as required in subsection F.4., below.

5. The Director, Defense Investigative Service (DIS), shall, in addition to the responsibilities outlined in paragraph E.3., above, develop appropriate changes to DoD 5220.22-M (reference (h)) to implement this Directive. Proposed changes shall be referred to the Office of the Deputy Under Secretary of Defense for Policy (ODUSD(P)) for preliminary policy review and approval, in accordance with DoD Directive 5220.22 (reference (c)).

6. The Director, National Security Agency (NSA), shall, in addition to the responsibilities outlined in paragraphs E.3.b., c., and d., above, coordinate all information reported under this Directive by military personnel assigned to NSA with the appropriate Military Department FCI agency, and coordinate all information reported by civilian employees with the FBI.

F. PROCEDURES

1. Reporting Requirements

a. [deleted in reprint of July 18, 1986.]

(1) [deleted in reprint of July 18, 1986.]

(2) Information concerning any international or domestic terrorist organization, sabotage, or subversive activity that is reasonable

believed to pose or have a potential to pose a direct threat to DoD or other U.S. facilities, activities, personnel, or resources.

(3) A request by anyone (regardless of nationality) for illegal or unauthorized access to classified or controlled defense information.

(4) Any contact with an individual (regardless of nationality) under circumstances which suggest the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.

(5) Information indicating the deliberate compromise of classified defense information, attempted or contemplated by DoD personnel, with the intention of conveying classified documents, information, or material to any unauthorized persons.

b. [deleted in reprint of July 18, 1986.]

c. All DoD personnel shall receive periodic briefings on hostile intelligence and terrorist threats and be advised of their personal responsibility to report information, in accordance with paragraphs F.I.a. and b., above.

2. Sanctions

Any DoD personnel who fail to report information required by this Directive shall be subject to judicial (Uniform Code of Military Justice - UCMJ) or administrative action appropriate to the seriousness of the offense.

3. Analysis of Reports

For purposes of analysis and uniformity of reporting among DoD Components, the following categories and subcategories shall be used for reports made under this Directive:

a. CATEGORY I. Includes any reported incident of an approach or request for information in which hostile intelligence service involvement is confirmed.

b. CATEGORY II. Includes any reported incident of an approach or request for information in which some evidence suggests hostile intelligence service involvement (based on the name used by the perpetrator/elicitor, physical description, modus operandi, or the nature of the information requested).

c. CATEGORY III. Includes any reported solicitation of classified or unclassified defense information not made through official channels or under authorized procedures, in which foreign intelligence service involvement is considered to be remote.

d. [deleted in reprint of July 18, 1986.]

e. CATEGORY V. Includes any reported information concerning international or domestic terrorist groups/activities that pose a potential

threat to the security of DoD or other U.S. personnel, resources, or facilities.

f. CATEGORY VI. Includes any reported incident of deliberate compromise of classified defense information by DoD personnel to an unauthorized person or entity.

4. Reporting Requirements

For the purpose of oversight and program evaluation, DoD Components or their servicing DoD FCI agencies shall maintain a record of the incidents and information reported in each category listed in paragraphs F.3.a. through f., above. An annual report containing the following information for the preceding fiscal year shall be provided to the Director of Counterintelligence and Investigative Programs, Office of the Deputy Under Secretary of Defense for Policy, by November 1:

- a. Number of personnel briefed on reporting requirements.
- b. Number of contacts or reports received by category.
- c. Number of investigations initiated as a result of information reported.
- d. Number of investigations resulting in:
 - (1) Planned or actual offensive counterespionage operations.
 - (2) Confirmed instances of espionage.
 - (3) Confirmed deliberate compromise of defense information.
 - (4) Administrative or judicial action against individuals violating reporting requirements.
 - (5) Persons prosecuted or pending prosecution on charges of espionage or related offenses, based upon reports under this Directive.
- e. Reports involving information on terrorist threats to the security of DoD or other U.S. personnel and resources.

G. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of implementing documents to the Under Secretary of Defense for Policy within 120 days.

/s/
William H. Taft, IV
Deputy Secretary of Defense

Enclosures

- 1. References
- 2. Definitions
- 3. [Rescinded by ASD(C3I) memo, 5 Apr 1993, and Change 2, DoD 5200.2-R.]

DCAAM 5210.1
MARCH 1996
ENCLOSURE 5

Feb 26, 86
5240.6 (Encl 1)

REFERENCES, continued

- (e) DoD 5400.7-R, "DoD Freedom of Information Act Program," December 1980, authorized by DoD Directive 5400.7, March 24, 1980
- (f) DoD Directive 2000.12, "Protection of DoD Personnel and Resources Against Terrorist Acts," February 12, 1982
- (g) Agreement Governing the Conduct of Department of Defense Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, April 5, 1979
- (h) DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," March 1984, authorized by DoD Directive 5220.22, December 8, 1980
- (i) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982
- (j) Title 18, United States Code, Sections 150, 792-798, and 2387

Feb 26, 86

5240.6 (Encl 2)

DEFINITIONS

1. Citizen. As used in this Directive, any communist, communist-controlled or designated country representative, diplomat, visitor, tourist, student, scholar, journalist, engineer, scientist, athlete, businessperson, or other person from a communist, communist-controlled, or designated country.
2. Classified Defense Information. Official information requiring protection in the interest of national defense, classified TOP SECRET, SECRET, or CONFIDENTIAL according to DoD 5200.1-R (reference (i)), or designated Sensitive Compartmented Information (SCI) according to DoD TS 5105.21-M2 or DoD TS 5105.21-M3.
3. Contact. Any form of meeting, association, or communication; in person, by radio, telephone, letter or other means, regardless of who initiated the contact or whether it was for social, official, private, or other reasons with a citizen or entity of a communist, communist-controlled, or designated country. A contact has occurred even if no official information was discussed or requested.
4. Controlled Information. As used in this Directive, that information which bears a distribution limitation statement from DoD Directive 5230.24 (reference (d)) or that information which is being marked "For Official Use Only" in accordance with Chapter IV of DoD 5400.7-R (reference (e)).
5. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons; or international terrorist activities, excluding personnel, physical, document, and communications security programs.
6. Counterintelligence Investigation. Includes inquiries and other activities undertaken to determine whether a particular person is acting for or on behalf of a foreign power for purpose of espionage or other intelligence activities, sabotage, assassinations, international terrorist activities; and actions to neutralize such acts.
7. Criminal Subversion. Criminal subversion is defined in 18 U.S.C. 2387 (reference (j)). It generally includes inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities, with the willful intent thereby to interfere with, or impair the loyalty, morale, or discipline, of the military forces of the United States.
8. Deliberate Compromise of Classified Information. Instances in which classified defense information is or could be compromised as a result of willful disclosure to an unauthorized person.
9. Entity. Any embassy; consulate; trade, press, airline, cultural, tourist, or business office; and any organization representing a communist, communist-controlled, or designated country.

Feb 26, 86
5240.6 (Encl 2 continued)

10. Espionage. As set forth in 18 U.S.C. 792-798 (reference (j)), in general:

a. Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies in time of war or peace.

b. The statute makes it an offense to gather, with the requisite intent or belief, national defense information, by going upon, entering, flying over, or obtaining access by any means to any installation or place used by the United States in connection with national defense. The method of gathering information is immaterial.

c. Anyone who lawfully or unlawfully is entrusted with or otherwise has possession of, access to, or control over information about national defense which he or she has reason to believe could be used against the United States or to the advantage of any foreign nation, and willfully communicates or transmits, or attempts to communicate or transmit, such information to any person not entitled to receive it, is guilty of espionage.

d. Anyone entrusted with or having lawful possession or control of information pertaining to national defense, who through gross negligence permits the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of this trust, is guilty of violating the Espionage Act.

e. If two or more persons conspire to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of the Espionage Act.

11. Sabotage. An act or acts with the intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war material, premises, or utilities, to include human or natural resources. Such activity is a violation of 18 U.S.C. 150 (reference (j)).

12. Terrorism. The Unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives.

ENCLOSURE 6

FOREIGN CONTACT/TRAVEL GUIDE FOR DCAA PERSONNEL

DoD 5200.2-R and DoD Directive 5240.6 require that personnel report to their security office contacts with individuals of any nationality, whether within or outside the scope of the employee's official activities in which:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

(2) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

The advice of American law enforcement and security officers on foreign intelligence organizations and techniques will usually not be readily available to the foreign traveler. Some employees mistakenly assume that they would never be a target for foreign intelligence exploitation because (i) they have not had recent access to classified information or perhaps have had access only to unclassified procurement information or (ii) they consider that the classified information to which they have access is not really "sensitive" enough to warrant foreign intelligence interest. Even if an individual's immediate knowledge is of little or no value to a foreign intelligence agency, his or her potential for gaining future access to highly sensitive information is treated as a prime asset by foreign intelligence agencies. The following "Do's and Don'ts" can be applicable to conditions in any country, including the U.S., although certain precautions listed should obviously be taken wherever you travel abroad.

"DO's AND DON'Ts"

1. DON'TS

- a. Do not carry classified material out of the United States.
- b. Do not discuss classified information outside of U.S. approved facilities.
- c. Do not divulge any level of classified information to any individuals who have not been cleared for such level of access by appropriate U.S. authorities and whose need for such access, in connection with their official duties, has not been established to your satisfaction by competent U.S. authorities.
- d. Do not permit a representative of any foreign country to divert an unclassified discussion to topics which would result in your releasing advanced industrial or scientific technology, or other technical data, whether classified or unclassified not otherwise available to the foreign country concerned.
- e. Do not engage in black market activities, particularly the sale of currency or the purchase of art treasures.
- f. Do not accept letters, photographs, packages, or any other material to be smuggled out of any foreign country for any reason.

- g. Do not make any statements or sign any documents which may be exploited for propaganda purposes.
- h. Do not photograph military installations or equipment, other "restricted" areas, or military personnel.
- i. Do not overly befriend tourist guides, interpreters, or other persons you meet during your travel, particularly if they just "happen" to know your special field.
- j. Do not attempt to obtain any information concerning any person, place, object, or organization which might erroneously be construed as an indication that you have undertaken any type of intelligence mission. DCAA personnel traveling on official Agency business will conduct only that business for which the travel was authorized.

DO's

- a. Report any apparent or suspected attempts at subversion while abroad to the U.S. Embassy of the country you are visiting. Remember that if you have been indiscreet or have otherwise become compromised during your visit, you should discuss the situation frankly with U.S. Embassy officials. Their interest is to protect you, any classified information you may possess, and the security of the United States. Follow the advice given you by the U.S. Embassy officials. Unless otherwise directed by U.S. Embassy officials abroad, also report the incident to your supervisor, or to the FBI, upon your return from abroad.
- b. Except when emergency situations make it impossible, obtain medical or dental service only from persons or institutions recommended to you by U.S. Embassy or Consulate officials.
- c. Be careful of what you write and to whom you write in your correspondence abroad. Keeping diaries while traveling in foreign countries is discouraged, except as may be necessary to record travel expenses, transportation arrangements, etc.
- d. Avoid all circumstances (e.g. moral indiscretions, excessive use of intoxicants, etc.) which could lead to attempts to compromise you through blackmail.
- e. Should you be arrested or otherwise detained by police authorities abroad, request that you be permitted to contact the U.S. Embassy or Consulate for assistance. Remember that all U.S. travelers abroad are under the technical jurisdiction of the local U.S. Ambassador or U.S. Consul. Whenever you need assistance in dealing with foreign officials, you can and should seek the advice of the local U.S. Embassy or Consulate.
- f. Read this general guide thoroughly and discuss it with your family members or friends who will be accompanying you in your foreign travel. Do not take it with you abroad; its discovery in your

luggage might inadvertently serve to make you even more of a target for foreign intelligence exploitations. For the same reason, it is recommended that, unless you are traveling on official Agency business you do not carry abroad any identification issued by this Agency which identifies you as being a member of a Department of Defense component. In general, when required to furnish your occupation on hotel registers, etc., the phrase "U.S. Government employee" will be sufficient; however, if your exact affiliation is demanded, furnish it.

TERRORIST ACTIVITIES

Your security officer will discuss with you any information concerning terrorist activities in specific areas. While there are a few basic precautions you can take to reduce the risk of your becoming a specific target for terrorist acts, you must realize that no foolproof defense has been developed and that you may even accidentally become involved in a terrorist act merely by your presence in a target area.

It is difficult to predict the exact type of activities or targets terrorists groups may have. The following are general types of activity that can be anticipated:

Kidnapping for Ransom

The ransom in terrorist kidnapping may range from demands for huge sums of money and safe escape routes, to demands for release of other terrorists in prison, to demands for high level governmental acts.

Assassinations

Assassinations may be anticipated (i) to eliminate key officials who are involved in activities considered undesirable by terrorist groups, (ii) to slow or stall activities adversely affecting terrorist aims, (iii) to shock world opinion and focus attention on terrorist aims, and (iv) for revenge.

Sabotage

Threatened and actual sabotage of specific targets, usually by explosive devices, may be anticipated (i) to eliminate entire groups of individuals engaged in activities adverse to terrorist aims, (ii) to shock world opinion and focus attention on terrorist aims, (iii) to foster fear and lower morale in groups engaged in activities adversely affecting terrorist aims, and (iv) for revenge. A variety of this method is the threat of sabotage for ransom, particularly where the threatened sabotage may affect large areas of population (poisoning of water supplies, explosion of nuclear devices, destruction of dams and power stations, etc.).

1. Kidnapping

Kidnapping of a single individual is generally not conducive to achieving terrorist goals unless the individual concerned is a public figure, occupies a key position, or possesses detailed

intelligence information. However, such pointless kidnapping have been perpetrated in the past, and may be in the future. They are not likely, however, to generate the level of world attention conducive to terrorist aims. More likely to be anticipated is the kidnapping of entire groups of individuals, as has been frequently encountered in the hijacking of commercial aircraft or other common carriers. You will be less likely to find yourself included in such target groups, if you:

- a. Use U.S. military air transportation when traveling on official business to, from, or within overseas areas whenever possible.
- b. Avoid those airports which do not have rigid passenger and baggage inspection procedures, when traveling by commercial airlines. Your security officer may have more information on this subject which will supplement your own previous travel experiences.
- c. Carefully consider the possible consequences of travel as a tourist to any areas in which terrorist activities are widespread.

If you are a passenger aboard a commercial airplane which is hijacked and landed in a foreign country, keep the following in mind:

- a. Remain calm, but alert. While aboard the aircraft, carefully note the location of the emergency exit closest to you; you may have to use it. Be prepared to instantly take cover on the floor, between the seats, if guns are fired.
- b. If you are moved from the aircraft to a building, carefully note the quickest safe way out of the building in the event of an emergency. Also be prepared to seek the best available cover, on the floor, if gunfire or explosions occur.
- c. Take no actions to provoke retaliatory measures by your captors.
- d. Do nothing which would invite attention to your affiliation with the DoD. However, if asked directly if you are affiliated with DoD, do not attempt to deny such affiliation.
- e. Use common sense in responding to interrogation, but do not reveal classified information under any circumstances.
- f. Observe and mentally note the methods and procedures used by the jetliners during your stay in a foreign country.
- g. Remember that rescue operations have been initiated and instantly follow to the letter any instructions which your rescuers may issue.

If you are being assigned to a DCAA office abroad where terrorist kidnapping are prevalent, the office has developed emergency plans and procedures designed to minimize this threat to you. You will be briefed on these plans upon your arrival abroad.

2. Assassinations

Except in the case of psychopathic terrorists, it makes little sense for single individuals to be selected for assassination whose death would not contribute substantially to a terrorist cause. Individuals who are prone to advertise their relative importance and influence, particularly when such claims are exaggerated, may, however, be selected in error by terrorist groups as targets for assassination. Individuals whose activities or affiliations truly place them in the limelight of publicity require special protective measures.

Fortunately, most DCAA personnel are in a "low profile" category as far as being selected as a target for terrorist assassination. However, if they serve in overseas areas where few DoD (or even American) personnel are stationed, their relative position as a possible target increases substantially. Special protective plans have been developed by overseas offices to deter assassination attempts.

The best advice for a casual tourist is to "keep a low profile" by not advertising any affiliations (government, financial, family, social, political, or religious) which would attract terrorist attention. Stay with the established tourist routines, groups, travel routes, and tourist attractions. Seriously consider the consequences of any noncompliance travels in terrorist-prone areas. Avoid known trouble spots which, although possibly picturesque, may place you alone in hostile territory. Don't flash large sums of money or wear expensive jewelry. Avoid controversial subjects in discussions and arguments. In general, the better able you are to blend in with the local environment, the less likely you are to become a target.

3. Sabotage

Terrorist sabotage is generally aimed against locations which (i) are themselves symbols of a nation, organization, or system against which the terrorist group is motivated, or (ii) contain or attract large numbers of individuals against whom terrorist activities are directed.

If you are in a duty status abroad, you will not be able to avoid all such locations. You will be advised of local security measures to protect you in these target areas, and you should follow them to the letter. While they may, in some cases, appear to be time-consuming or excessive, they have been designed on the basis of local experience with terrorist activities and are for your safety.

DCAAM 5210.1

MARCH 1996

ENCLOSURE 6

When abroad as a tourist, try to avoid those areas which have been consistently the targets of local terrorist sabotage, particularly bombings (certain government buildings, banks, police stations, post offices, etc.). If you are in the vicinity of an explosion or fire, don't rush to the scene to view it. In many cases, secondary explosive devices have been positioned to detonate after a crowd develops. If you are at the scene of an explosion, drop to the floor and protect your head against falling debris and glass; more casualties are suffered from flying debris than from blasts.

If you have questions about foreign contacts or your travel plans, please contact your Regional Security Officer or the Agency Security Officer

MARCH 1996

ENCLOSURE 7

DCAA LIST OF FORMS

DA Form 1144	Request for Dossier/Index Check
DIA Form 1557A	Certificate of Clearance and/or Security Determination
DCAA Form 5210-3	Security Termination Statement
DCAA Form 5210-4	Security Briefing Acknowledgment
DCAA Form 5210-9	SAP Involvement Report
DCAA Form 5210-19	Preappointment Security Approval
DCAA Form 5210-20	Inquiry for DCAA Employment
DCAA Form 5210-31	Request for Security Clearance
DCAA Form 5210-43	Waiver of Required Preappointment Security Investigation
DCAA Form 5210-46	Worksheet for Security Inquiry
DCAA Form 5210-48	Proof of Citizenship Certificate
DD Form 1879	Request for Personnel Security Investigation
FD 258	Applicant Fingerprint Chart
OPI Form 79A	Report of Agency Adjudication Action on OPM Personnel Investigations
OPI Form 79B	Request for Search of OPM Records
SD Form 176	Office of the Secretary of Defense Certificate of Clearance
SF 75	Request for Preliminary Employment Data
SF 85	Questionnaire for Nonsensitive Positions
SF 85P	Questionnaire for Public Trust Positions

DCAAM 5210.1
MARCH 1996
ENCLOSURE 7

SF 86

Questionnaire for National
Security Positions

SF 87

Fingerprint Chart

SF 171, Application, or
Resume

Application for Federal
Employment

SF 312

Classified Information
Nondisclosure Agreement



DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

OAID

July 8, 2002

DCAA REGULATION
NO. 5340.1

VIDEO INFORMATION (VI)
(RCS: DD-PA(A)1438)

References: (a) DoD Directive 5040.2 -- Video Information Activities
(b) DoD Directive 5040.3 -- Joint Video Information Services
(c) DoD Directive 5535.4 -- Copyrighted Video Recordings

1. REISSUANCE AND PURPOSE. Establish policies and procedures pertaining to DCAA's acquisition, production, and use of Video Information (VI).

2. CANCELLATION. DCAA Regulation 5340.1, Video Information (VI), dated May 21, 1992, and subsequent changes.

3. APPLICABILITY AND SCOPE. This regulation applies to all DCAA organizational elements. The Department of Defense has authorized DCAA to operate a Type C, Category 2 (production for component distribution) full-production video activity (DVIAN R0301) located at the Defense Contract Audit Institute (DCAI) in Memphis, TN.

4.0. DEFINITIONS. Video Information (VI), hereinafter referred to as videos, consists of three categories:

4.1. Category 1: Off-the-shelf purchases and productions required to support the needs of the agency.

4.2. Category 2: DCAA productions.

4.3. Category 3: Supports DoD and joint-interest programs that are the requirements of more than one DoD organization. This requirement falls under the DoD regulation and is outside the scope of this regulation.

5. POLICY. DCAA's policy is to:

5.1. Authorize the use of videos for communication, training, instruction, orientation, documentation, and motivation purposes.

5.2. Centrally coordinate and approve the purchase or production of videos having Agency-wide application.

5.3. Not record, copy, exhibit, or broadcast copyrighted material in any form, from any source, without a license or prior written agreement.

5.4. Prepare a Department of Defense DD Form 1995 (Visual Information Production Request and Report) to procure all Category 1 videos expected to cost more than \$2,500 and to produce all Category 2 videos when any of the following conditions exist:

5.4.1. The subject has potential for Agency-wide application.

5.4.2. Distribution is anticipated outside the originating element.

5.4.3. Duplication of more than 25 copies will be required.

5.4.4 The estimated cost is expected to exceed \$2,500.

5.4.5 The product is script-controlled to meet specific objectives.

NOTE: Forms, instructions, and assistance to purchase or produce a video are available from DCAI.

6. RESPONSIBILITIES. Video activities are managed by the Chief, Course Development Branch (OAID), under the direction of the Manager, DCAI (OAI), and the Assistant Director, Operations (O).

6.1. The Assistant Director, Operations (O) is responsible for video information services for the Agency. This includes:

6.1.1. Providing direction for the Agency's video services including the establishment and implementation of policy and monitoring compliance with that policy.

6.1.2. Certifying the validity of requests for Category 1 video procurements and Category 2 video productions (which require the DD Form 1995).

6.2. The Manager, Defense Contract Audit Institute (OAI) is responsible for:

6.2.1. Administering the video policies, procedures, and processes.

6.2.2. Providing advice to the Assistant Director, Operations, regarding video policy matters.

6.2.3 Providing advice to the Assistant Director, Operations, as to the validity of requests for Category 1 video procurements and Category 2 video productions (which require the DD Form 1995).

6.2.4. Providing direction over the DCAA video production facility located in Memphis, TN.

6.3. The Chief, Course Development Branch (OAID) is responsible for:

6.3.1. Management of the DCAA video production facility in Memphis, TN.

6.3.2. Supervising video production, including the activities of the Audiovisual Production Specialist.

6.3.3. Providing advice to the Manager, Defense Contract Audit Institute, as to the validity and necessity, of requests for Category 2 video productions.

6.4. The Audiovisual Production Specialist, under the supervision and guidance of the Chief, Course Development Branch, shall:

6.4.1. Plan, coordinate, and oversee video productions and ensure compliance with DoD Directives.

6.4.2. Determine production contract requirements and oversee contract personnel.

6.4.3. Operate and maintain the studio facility.

6.4.4. Develop video script based on a discovery document provided by the video requester's Subject Matter Expert (SME).

6.4.5. Provide advice to management regarding video matters.

6.5. Regional Directors; Director, Field Detachment; and Heads of Principal Staff Elements (HPSEs) are responsible for:

6.5.1. Implementing and monitoring compliance with this regulation and published procedures for video information activity within their organizational element.

6.5.2. Determining the validity of requests for all Category 1 purchased videos. (Videos costing less than \$2,500 do not require a DD Form 1995 and are handled through established non-routine procurement procedures).

6.5.3. Determining the validity of request for Category 2 video productions and initiating the DD Form 1995 approval process.

6.5.4. Selecting the Subject Matter Experts (SMEs) to support video production.

6.5.5. Designating a Video Information Coordinator.

6.6. Video Information Coordinators are responsible for:

6.6.1. Administering the video process for their element and serving as the initial point of contact for those requesting Category 1 video procurements and Category 2 video productions.

6.6.2. Gathering information, coordinating with the video requestor and DCAI (OAID), and advising the cognizant Regional Director; Director, Field Detachment, or HPSE as to the need for the video.

6.6.3. Maintaining awareness of this and referenced DoD video regulations and advising the cognizant Regional Director; Director, Field Detachment, or HPSE as appropriate.

6.7. The Subject Matter Expert (SME) is the individual selected by management who is knowledgeable of the material covered in the video. The SME coordinates with management and the requesting party to define project objectives, document relevance to Agency mission, and determine the pertinent content.

6.7.1. The SME coordinates with DCAI (OAID) and must be available throughout the entire production process.

6.7.2. The SME is responsible for communicating with and obtaining concurrence from the requestor and cognizant Regional Director, Director, Field Detachment, or HPSE throughout the video production process.

6.8. The Executive Officer (DX) is responsible for all video information products that include coverage of DCAA operations, facilities, or personnel, and are intended for release to the news media or the public.

7. PROCEDURES. The following is the approval process for those videos requiring a DD Form 1995.

7.1. Anyone proposing to acquire an off-the-shelf video costing \$2,500 or more, or to produce a video will submit a memorandum through their Chain of Command to the cognizant Visual Information Coordinator.

7.2. The Visual Information Coordinator will coordinate with DCAI who will conduct a search to determine that no video exists that meets the proposed requirement. If the search is negative, the Visual Information Coordinator will gather sufficient information for the Regional Director, Director, Field Detachment, or HPSE to make a decision whether to proceed with the procurement or production of the video.

7.3. If the Regional Director, Director, Field Detachment, or HPSE determines that a need exists, they will submit a memorandum together with the DD Form 1995 to DCAI.

7.4. DCAI will determine the production and scheduling requirements, finalize the production information, and forward the completed DD Form 1995 together with all pertinent data to the Assistant Director, Operations for approval.

7.5. Upon approval by the Assistant Director, Operations, DCAI will coordinate with the requestor to accomplish the production requirements. If the purchase or production request is not approved, the Assistant Director, Operations will advise the requestor as to the reason.

8. EFFECTIVE DATE. This regulation is effective upon receipt.

“signed”

William H. Reed
Director



DEFENSE CONTRACT AUDIT AGENCY
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

CM

March 13, 2013

DCAA INSTRUCTION
NO. 5410.8

DCAA FREEDOM OF INFORMATION ACT PROGRAM

- References:
- (a) Title 5, United States Code, Section 552a
 - (b) DoDD 5400.7, DoD Freedom of Information Act Program
 - (c) DoD 5400.7-R, DoD Freedom of Information Act Program
 - (d) DCAA Freedom of Information Act Processing Guide

1. PURPOSE.

a. To assign responsibilities and establish policies and procedures for a uniform DCAA Freedom of Information Act (FOIA) program pursuant to the provisions of the Freedom of Information Act, 5 U.S.C. § 552, as implemented by DoD Directive 5400.7 and DoD Regulation 5400.7-R.

b. This instruction supersedes DCAAR 5410.8, DCAA Freedom of Information Act Program, dated February 16, 2001, updated May 17, 2000.

2. APPLICABILITY.

a. This instruction applies to DCAA Headquarters, Regional Offices, and Field Audit Offices (FAOs), and is to govern written responses by DCAA officials for requests from members of the public for permission to examine, or to be provided with copies of DCAA records. Supplements and waivers to this policy and procedures contained in this Instruction are not authorized unless issued and approved by Office of Primary Responsibility (OPR).

b. The Office of Primary Responsibility for this instruction is the Assistant Director Resources.

3. DEFINITIONS. See [Glossary](#).
4. POLICY. Agency policy and procedures are consistent with those cited in DoD 5400.7-R. In addition, DCAA will:
 - a. Promote public trust by making the maximum amount of information available to the public, upon request, pertaining to the operation and activities of the Agency.
 - b. Allow a requester to obtain records from the Agency that are available through other public information services without invoking the FOIA.
 - c. Make available, under the procedures established by the DCAA FOIA Processing Guide, those records that are requested by a member of the general public who cites the FOIA.
 - d. Answer promptly all other requests for information and records under established procedures and practices.
5. RESPONSIBILITIES. See [Enclosure 1](#).
6. PROCEDURES. See [Enclosure 2](#).
7. RELEASABILITY. This instruction is approved for public release and will be available on the internet from the DCAA website at <http://www.dcaa.mil>.

8. EFFECTIVE DATE. This instruction is effective upon receipt.

FOR THE DIRECTOR:

/s/

J. Philip Anderson
Assistant Director Resources

Enclosures:

1. Responsibilities
2. Procedures
3. Fees
4. DCAA FOIA Points of Contact

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: RESPONSIBILITIES	5
THE ASSISTANT DIRECTOR, RESOURCES	5
THE DEPUTY ASSISTANT DIRECTOR, RESOURCES	5
THE CHIEF, INFORMATION AND RECORDS BRANCH, ADMINISTRATIVE MANAGEMENT DIVISION	5
THE DCAA FOIA ADVISOR	6
REGIONAL DIRECTORS AND HEADQUARTERS ASSISTANT DIRECTORS	6
THE GENERAL COUNSEL	7
THE EXECUTIVE OFFICER	7
REGIONAL DIRECTORS	7
FOIA COORDINATORS	8
MANAGERS, FIELD AUDIT OFFICES (FAOS)	8
ENCLOSURE 2: PROCEDURES	9
GENERAL	9
REQUESTS FOR AUDIT REPORTS	9
REQUESTS FOR AUDIT WORKING PAPERS	9
PUBLIC INSPECTION AND COPYING	9
REQUESTS FOR THE EXAMINATION OR COPIES OF RECORDS	9
REFERRALS	10
TIME LIMITS	11
INITIAL DISCLOSURE DETERMINATIONS	12
DENIALS	12
ADMINISTRATIVE APPEALS OF DENIALS	13
DELAY IN RESPONDING TO AN APPEAL	13
ENCLOSURE 3: FEES	15
FEES	15
FEE WAIVERS	16
ENCLOSURE 4: DCAA FOIA POINTS OF CONTACT	18
GLOSSARY	20
DEFINITIONS	20
TABLE	
FOIA POC Information	18

ENCLOSURE 1

RESPONSIBILITIES

1. The Assistant Director, Resources is responsible for:

(1) The overall Agency-wide administration of the DCAA FOIA Program through the Chief, Information and Records Branch (CMR), Administrative Management Division, to ensure compliance with the policies and procedures that govern the program.

(2) Acting as the designee for the Director, DCAA, serving as the sole appellate authority for appeals to decisions of the Initial Denial Authority (IDA).

(3) Advising the Department of Defense, Director of Administration and Management (DA&M) of cases of public interest, particularly those on appeal. When the issues raised are unusual or precedent setting, such as matters of disagreement among DoD components or are of concern to agencies outside the Department of Defense, they may require special attention or guidance.

(4) Advising the DA&M and the Executive Officer, DCAA, concurrent with the denial of a request or an appeal, when circumstances suggest a news media interest.

(5) Conferring with the General Counsel; the Assistant Director, Operations; the Assistant Director, Policy and Plans; and the Regional Directors on the desirability of reconsidering a final decision to deny a record, if that decision becomes a matter of special concern because it involves either an issue of public concern or an issue with DoD-wide consequences.

(6) Accomplishing program overview, in cooperation with the General Counsel, to ensure coordinated guidance to components, and to provide the means of assessing the overall conduct of the Agency's FOIA Program.

(7) Responding to corrective action recommended by the Office of Special Counsel for arbitrary or capricious withholding of records by designated employees of the Agency.

2. The Deputy Assistant Director, Resources is responsible for serving as the DCAA FOIA Public Liaison, who serves requesters who have raised concerns of unsatisfactory FOIA service.

3. The Chief, Information and Records Branch, Administrative Management Division , is responsible for:

(1) Establishing, issuing, and updating policies for the DCAA FOIA Program; monitoring compliance with this instruction; and providing policy guidance for the FOIA program.

(2) Resolving conflicts that may arise regarding implementation of DCAA FOIA policy.

(3) Designating an Agency FOIA Advisor, as a single point of contact, to coordinate on matters concerning Freedom of Information Act policy.

4. The DCAA FOIA Advisor , under the supervision and guidance of the Chief, Information and Records Branch, Administrative Management Division, is responsible for:

(1) Managing the DCAA FOIA Program, as the DCAA FOIA Chief Officer, in accordance with this instruction, the DCAA FOIA Processing Guide, applicable DCAA policies as well as DoD and Federal regulations.

(2) Providing guidelines for managing, administering, and implementing the DCAA FOIA program. This would include issuing the DCAA FOIA regulation, developing and conducting training for those individuals who implement the FOIA, and publishing in the Federal Register any instructions necessary for the administration of the FOIA program.

(3) Maintaining and publishing the DCAA Freedom of Information Act Processing Guide.

(4) Preparing the Annual Freedom of Information Report to Congress.

(5) Establishing and maintaining a control system for assigning FOIA case numbers to FOIA requests received by the Agency.

(6) Maintaining a record of FOIA requests received by the Agency. This record is to contain the requester's identification, the date of the request, type of information requested, and type of information furnished. This record will be maintained and disposed of in accordance with DCAA records maintenance and disposition regulations and schedules.

(7) Making available for public inspection and copying in an appropriate facility or facilities, in accordance with rules published in the Federal Register the records specified in paragraph (a)(2) of reference (a), unless such records are published and copies are offered for sale. Maintain and make available for public inspection current indices of these records.

5. Regional Directors and Headquarters Assistant Directors are responsible for:

(1) Reviewing all regulations or other policy and guidance issuances for which they are the proponent to ensure consistency with the provisions of this instruction.

(2) Ensuring that the provisions of the DCAA FOIA Processing Guide and this instruction are followed in processing requests for records.

(3) Forwarding to the DCAA FOIA Advisor, any FOIA requests received directly from a member of the public so that the request may be administratively controlled and processed.

(4) Ensuring the prompt review of all FOIA requests, and when required, coordinating those requests with other organizational elements.

(5) Providing recommendations regarding the releasability of DCAA records to members of the public, along with the responsive documents.

(6) Providing the appropriate documents, along with a written justification for any denial, in whole or in part, of a request for records and the specific exemption or exemptions cited which provide the basis for denying the requested records.

6. The General Counsel is responsible for:

(1) Ensuring uniformity is maintained in the legal position, and the interpretation of the Freedom of Information Act, DoD 5400.7-R, and this instruction.

(2) Consulting with DoD General Counsel on final denials that are inconsistent with decisions of other DoD components, involving issues not previously resolved, or raise new or significant legal issues of potential significance to other Government agencies.

(3) Providing advice and assistance to the Assistant Director, Resources; other Headquarters Assistant Directors; and Regional Directors through the DCAA FOIA Advisor, as required, in the discharge of their responsibilities.

(4) Coordinating Freedom of Information Act litigation with the Department of Justice.

(5) Coordinating on Agency denials of initial requests and administrative appeals.

7. The Executive Officer shall serve as the coordinator for the release of information to the news media.

8. Regional Directors are responsible for:

(1) Implementing and administering the Freedom of Information Act program throughout the region.

(2) Serving as the Initial Denial Authority (IDA). The authority to deny public access to Agency records cannot be delegated.

(3) Delegating signature authority for FOIA correspondence which is considered only to be routine in nature, e.g., referrals and the release of information.

(4) Ensuring that documents are marked FOUO at the time of their creation if information contained within is considered exempt from disclosure.

9. FOIA Coordinators are responsible for:

(1) Conducting training on the FOIA program to the FAOs.

(2) Submitting a DCAA Form 5410-4, Freedom of Information Case Summary, to the DCAA Information and Privacy Advisor at the completion of each FOIA case to facilitate the preparation of the annual FOIA report to Congress. All case summaries must be submitted no later than 10 October for cases completed during the previous fiscal year.

(3) Establishing and maintaining a control system to ensure proper accountability and processing of FOIA requests.

(4) Contacting the DCAA Information and Privacy Act Advisor for a FOIA case number upon receipt of a FOIA request.

10. Managers, Field Audit Offices (FAOs) are responsible for:

(1) Overall management and administration of the FOIA program within organizations under their cognizance.

(2) Ensuring that the regional FOIA Coordinator promptly receives all incoming FOIA requests.

ENCLOSURE 2PROCEDURES

1. General. Procedures for processing material in accordance with the FOIA are outlined in the DCAA FOIA Processing Guide. General provisions are outlined below.

2. Requests for Audit Reports. Audit reports prepared by DCAA are the property of and are prepared for the use of DoD contracting officers. As a result, their release should be at the sole discretion of the DoD contracting activity. Requesters seeking audit reports should send their requests directly to the DoD contracting activity to avoid administrative delay. Typically, requests for copies of DCAA audit reports may be identified by requesting those that relate to a specific contract number (e.g. DLA600-03-P0222). DoD contract numbers may be easily matched to the cognizant DoD contracting activity by referring to Appendix G of the DoD FAR Supplement.

3. Requests for Audit Working Papers. Audit working papers may be sought occasionally in conjunction with an audit report or as an independent demand. Normally, the release of such records is entirely dependent on the releasability of the related audit report. Since the content of audit working paper files can be quite diverse and often voluminous, the DCAA FOIA Advisor should work closely with the requester to ensure that the records produced are narrowly defined and entirely responsive to the requesters needs.

4. Public Inspection and Copying. Section (a)(2) of the Freedom of Information Act requires agencies to make available for public inspection and copying, final opinions made in the adjudication of cases, statements of policy not yet published in the Federal Register, and administrative manuals and instructions. This requirement is satisfied by the publication of DCAAI 5025.2, DCAA Index of Publications and DCAAI 5025.13, Index of DCAA Memorandums for Regional Directors.

5. Requests for the Examination or Copies of Records.

a. Members of the public may make written requests for copies of DCAA records or for permission to examine such records during normal business hours. Such requests must be in writing and either explicitly or implicitly invoke the Freedom of Information Act, or this instruction. These requests should be submitted directly to Headquarters, DCAA, ATTN: CMR, 8725 John J. Kingman Road, Suite 2135, Fort Belvoir, Virginia 22060-6219.

b. When submitting requests, requesters should:

(1) Identify each record sought with sufficient detail to facilitate the location and easy access to the record requested. Information as to where the record originated, subject, date, number, or any other identifying particulars should be provided whenever possible. The DCAA FOIA Advisor when receiving a request which does not reasonably describe the record requested, will advise the requester accordingly. Generally, a record is not reasonably described unless the requester provides information permitting an organized, nonrandom search of DCAA files and/or information systems. In providing descriptions based on events, the requester must provide information which permits DCAA to, at least, infer the specific record sought.

(2) Identify all other Federal agencies subject to the provisions of the FOIA to which the request has been sent. This will reduce both processing and coordination time between agencies and redundant referrals.

(3) Provide a statement of their willingness to pay assessable charges. The statement must include a specific monetary amount if the assessable fees are likely to exceed the fee waiver threshold of \$15.00 or a specific justification for any waiver or reduction of fees sought based on public interest in release or disclosure. DCAA will notify requesters of deficiencies in fee declarations, and provide them the opportunity to amend initial declarations. Determinations on the adequacy of requester fee declarations are not subject to appeal unless DCAA has denied a specific request for the assessment of fees under one of the established requester categories or DCAA has denied a request for the waiver or reduction of fees in the public interest.

(4) When DCAA has no records responsive to a request, the requester will be notified promptly that should he or she determine such request to be adverse in nature, he or she may exercise their appeal rights. In cases where the request has been sent to the incorrect Federal agency and DCAA is aware of the appropriate FOIA respondent, the Agency shall refer the request to the appropriate Federal agency through FOIA channels, and notify the requester of the referral. The 20 working day period allowed for responding to requests will not begin until the DCAA FOIA Advisor receives a request complying with procedural requirements of this instruction, including statements on the payment of fees.

(5) The provisions of the FOIA are intended for parties with private interests. Officials seeking documents or information on behalf of foreign governments, other Federal agencies, and state or local agencies should be encouraged to employ official channels. The release of records to individuals under the FOIA is a public release of information. DCAA will consider FOIA requests from such officials as made in a private, rather than official capacity, and will make disclosure and fee determinations accordingly.

6. Referrals.

a. Records originating in or based on information obtained from other Federal agencies subject to the FOIA may be referred to that agency. In processing FOIA requests for such records, DCAA, after coordinating with the originating agency, may refer the request, along with a copy of the responsive records in its possession, to that agency for direct response. DCAA will notify the requester of the referral. However, if for investigative or intelligence purposes, the

outside agency desires anonymity, DCAA may only respond directly to the requester after coordination with the agency.

b. **Referral of Audit Reports.** Audit reports prepared by DCAA are the property of and are prepared for the use of the DoD contracting officers. Their release is at the discretion of the DoD contracting activity. Therefore, any FOIA request for audit reports prepared for DoD components should be referred to the cognizant DoD contracting activity and the requester notified of the referral. To avoid the delay associated with the referral process, requesters should be advised to send requests for audit reports directly to the cognizant DoD contracting activity.

7. **Time Limits.** The DCAA FOIA Advisor will respond promptly to requesters complying with the procedural requirements outlined in this instruction. When a significant number of requests are being processed, e.g., 10 or more, the requests shall be completed in order of receipt. However, this does not preclude completing action on a request which can be easily answered, regardless of its ranking within the order of receipt. Action may be expedited on a request regardless of its ranking within the order of receipt upon a showing of exceptional need or urgency. Exceptional need or urgency is determined at the discretion of the DCAA FOIA Advisor.

a. Upon receipt of a properly submitted FOIA request, the DCAA FOIA Advisor will place the request under control by issuing a FOIA case number. The IDA should (1) locate and assemble responsive records, (2) determine releasability under the provisions of this instruction, (3) determine the appropriate fees to be charged, and (4) advise the requester accordingly. Initial determinations on either the release or denial of records, and notice to requesters, must be provided within 20 working days following receipt of the request by DCAA FOIA Advisor.

b. In certain cases, the IDA may need to extend the normal 20 working day period cited above. The IDA will notify the requester of the extension within the initial 20 working day provide the circumstances necessitating it, and give an anticipated date of a determination. Approved extensions are not to exceed 10 working days, and all extensions should be indicated on DCAA Form 5410-4, Section 6. Circumstances where such extensions may be approved include:

(1) The record(s) sought are geographically located at places other than the DCAA organizational element processing the request (e.g., the Regions).

(2) The request requires the collection and review of a substantial number of records.

(3) The disclosure determination requires consultation with another Federal agency with a substantial interest.

(4) As an alternative to the above, DCAA may seek informal agreements with requesters for extensions in unusual circumstances when time limits become an issue in the response to the request.

(5) The appropriate IDA will refer misdirected requests within 20 working days to the proper Federal agency through FOIA channels, and the requester notified of the referral. The 20 working day period allowed for responding to requests will not begin until the DCAA FOIA Advisor receives the request.

8. Initial Disclosure Determinations.

a. Initial determinations to make records available may only be made by an IDA designated in this instruction. (Note: Requests for audit reports should be directed to the cognizant contracting officer for release determination). When a decision is made to release records in response to a FOIA request, DCAA will promptly make the records available to the requester. When the request is for the examination of releasable records, DCAA will advise the requester when and where they may appear. Examinations will be held during normal business hours. If a record is not provided in response to a FOIA request, the IDA will advise the requester, in writing, of the rationale for not providing the record.

b. The IDA should consult the Executive Officer, prior to releasing records on matters considered newsworthy or when releasing records to media representatives. Copies of all media requests should be submitted to the Executive Officer.

c. The following reasons, other than the statutory exemptions cited in the FOIA, are provided for not releasing a record in response to a FOIA request.

(1) The request is transferred to another DoD component, or to another Federal agency.

(2) The Agency determines through knowledge of its files and reasonable search efforts that it neither controls nor otherwise possesses the requested record.

(3) A record has not been described with sufficient particularity to enable the Agency to locate it by conducting a reasonable search.

(4) The requester has failed to comply reasonably with procedural requirements, including payment of fees, imposed by this instruction.

(5) The request is withdrawn by the requester.

(6) The information requested is not a record within the meaning of the FOIA and this instruction.

9. Denials.

a. A record in the possession and control of DCAA may be withheld only when the record falls within one or more of the nine categories of records exempt from mandatory disclosure

under the FOIA, and the use of discretionary authority to release the record is determined to be unwarranted. The specific exemptions are detailed in the DCAA FOIA Processing Guide.

b. Although exempt portions of records may be denied, nonexempt portions must be released to the requester when the FOIA Advisor can reasonably deduce that the excised information could not be reconstructed. When a record is denied in whole, the IDA will prepare a response advising the requester of the determination, and the response will specifically state that it is not reasonably possible to segregate meaningful portions for release.

c. When a request for a record is denied in whole or in part, the IDA will inform the requester in writing of the specific exemption(s) on which the denial is based and explain the determination in sufficient detail to permit the requester to make a decision concerning appeal. The determination will also inform the requester of their appeal rights. Appeals should be made within 60 calendar days from the date of the initial denial, contain the reasons for the requester's disagreement with the determination, and be addressed to the Assistant Director, Resources, Headquarters, DCAA, 2135 John J. Kingman Road, Suite 2135, Fort Belvoir, VA 22060-6219.

d. Records or portions of records which have been previously released become part of the public domain and cannot be denied thereafter.

10. Administrative Appeals of Denials.

a. If the IDA declines to provide a record because they consider it exempt, that decision may be appealed by the requester, in writing, to the Assistant Director, Resources, DCAA. The denial authority for such records generally rests with the cognizant DoD contracting activity. The appeal should be accompanied by a copy of the letter denying the initial request. Such appeals should contain the basis for disagreement with the initial refusal. Appeal procedures also apply to the disapproval of a request for waiver or reduction of fees. A "no record" finding may be appealed which allows the requester to challenge the adequacy of the Agency's search. Records which are denied should be retained during the time permitted for appeal.

b. The IDA shall advise the requester that an appeal should be filed so that it reaches the designated appellate authority no later than 60 calendar days after the date of the initial denial letter. At the conclusion of this period, except for good cause shown as to why the appeal was not timely, the case may be considered closed; however, such closure does not preclude the requester from filing litigation for denial of his appeal. If the requester has been provided a series of determinations for a single request, the time for appeal will begin on the date of the last determination of the series. Records which are denied shall be retained for a period of six years to meet the statute of limitations of claims requirement.

c. Final determinations normally shall be made within 20 working days of receipt of an appropriately submitted appeal.

11. Delay in Responding to an Appeal.

a. When additional time is required to respond to the appeal, the final determination may be delayed for the number of working days (not to exceed 10 days) that were not utilized as additional time for responding to the initial request. Requesters shall be advised that, if the delay exceeds the statutory extension provision or is for reasons other than the unusual circumstances previously described, they may consider their administrative remedies exhausted. They may, however, without prejudicing their right of judicial remedy, await a substantive response from the Agency. DCAA shall continue to process the case expeditiously, whether or not the requester seeks a court order for release of the records, but a copy of any response provided subsequent to filing a complaint shall be forwarded to the Department of Justice through the DCAA General Counsel.

b. When the Assistant Director, Resources, DCAA, makes a determination to release all or a portion of the records on appeal, the records shall be made available promptly to the requester after compliance with procedural requirements. The final denial of a request will be made in writing, explain the exemption(s) invoked, advise that the material being denied does not contain meaningful portions that are reasonably segregable, and also advise the requester of the right of judicial review.

c. Judicial Action. A requester will be deemed to have exhausted his administrative remedies after he has been denied the requested record by the Assistant Director, Resources, or when the Agency fails to respond to his request within the time limits prescribed by the FOIA and this instruction. The requester may then seek an order from a U.S. District Court in the district in which he resides or has his principal place of business; the district in which the record is situated; or in the U.S. District Court for the District of Columbia, forbidding the Agency from withholding the record and ordering its production.

ENCLOSURE 3FEES1. Fees.

a. Fees shall be determined in accordance with the DoD fee schedule, which is detailed in the DCAA FOIA Processing Guide. Fees reflect direct costs for search, review (in the case of commercial requesters), and duplication of documents, collection of which is permitted by the FOIA. Fees are subject to limitations on the nature of assessable fees based on the category of the requester; statutory and automatic waivers based on the category determination and cost of routine collection; and either the waiver or reduction of fees when disclosure serves the public interest.

b. Fees will not be charged when direct costs for a FOIA request are \$15.00 or less, the automatic fee waiver threshold, regardless of category.

c. Fee Assessment. In order to be as responsive as possible to FOIA requests, DCAA organizational elements should adhere to the following when assessing fees:

(1) Evaluate each request to determine the requester category and adequacy of the fee declaration. An adequate fee declaration requires a willingness by the requester to pay fees in an amount equal to, or greater than, the assessable charges for the request.

(2) Provide requesters an opportunity to amend inadequate fee declarations and provide estimates of prospective charges when required. When a requester fails to provide an adequate fee declaration within 30 days after notification of a deficiency, the request for information will be considered withdrawn.

(3) A requester's claims for assessment of fees under a specific category will be carefully considered. The IDA may require a requester to substantiate a claim for assessment under a claimed category. In the absence of requester claims, the IDA will determine the category into which a requester falls, basing its determination on all available information.

(4) When DCAA disagrees with a requester claim for fee assessment under a specific category, the IDA will provide the requester with written determination indicating the following: (1) the requester should furnish additional justification to warrant the category claimed; (2) a search for responsive records will not be initiated until agreement has been attained relative to the category of the requester; (3) if further category information has not been received within a reasonable period of time, the component will render a final category determination; and (4) the determination may be appealed to the Assistant Director, Resources, within 60 calendar days of the date of the determination.

d. When a DCAA estimates or determines that allowable charges that a requester may be required to pay are likely to exceed \$250.00, they shall notify the requester of the likely cost and

obtain satisfactory assurance of full payment. This fee declaration generally applies when the requester has a history of prompt payments; however, an advance payment may be required of an amount up to the full estimated charges in the case of requesters with no history of payment.

e. Where a requester has previously failed to pay a fee charged within 30 calendar days from the date of billing, DCAA may require the requester to pay the full amount due, plus any applicable interest or demonstrate satisfaction of the debt, and to make an advance payment of the full amount of estimated fees, before processing begins on a new or pending request.

f. After all work is completed on a request, and the documents are ready for release, DCAA may request payment before forwarding the documents if there is no payment history on the requester, or if the requester has previously failed to pay a fee in a timely fashion (i.e., within 30 calendar days from the date of billing). Documents may not be held for release pending payment from requesters with a history of prompt payment.

g. The administrative time limits for responding to a request will begin only after the DCAA has received an adequate declaration from the requester stating a willingness to pay fees, and satisfaction that all outstanding debts have been paid.

h. DCAA can bill requesters for services provided in responding to a request. Payment of fees may be made by personal check, bank draft drawn on a U.S. bank, or by U.S. Postal money order. All payments of this type are to be made payable to DFAS Columbus, ATTN: CF, and the DCAA FOIA case number (ex. I-12-001-H) written on the payment.

i. Aggregating Requests. Occasionally, a requester may file multiple requests at the same time, each seeking portions of a document or documents, solely to avoid payments of fees. When a DCAA reasonably believes that a requester is attempting to do so, the Agency may aggregate such requests and charge accordingly. One element to be considered would be the time period in which the requests have occurred. In no case may DCAA aggregate multiple requests on unrelated subjects from one requester.

2. Fee Waivers.

a. The determination to waive fees is at the discretion of the IDA designated in this instruction. When direct costs for a FOIA request total the automatic fee waiver threshold, or is less, fees shall be waived automatically for all requesters, regardless of category.

b. Documents will be furnished without charge, or at a charge reduced below fees assessed to the categories of requesters, when the IDA determines that a waiver or reduction of fees is in the public interest because furnishing the information is likely to contribute significantly to public understanding of the operations of DCAA, and is not primarily in the commercial interest of the requester. DCAA should refer to the DCAA FOIA Processing Guide for factors to consider in applying fee waivers due to public interest. Each fee decision must be considered on a case-by-case basis and upon the merits of the information provided in each request. When the

question of whether to charge or waive the fee cannot be clearly resolved, DCAA should rule in favor of the requester.

ENCLOSURE 4DCAA FOIA POINTS OF CONTACTTable. FOIA POC Information.

Office	Contact Information
DCAA HEADQUARTERS AND FIELD DETACHMENT REGION	Defense Contract Audit Agency Attn: CMR/FOIA 8725 John J. Kingman Road, Suite 2135 Fort Belvoir, VA 22060-6219 (703) 767-1022
CENTRAL REGION	Defense Contract Audit Agency Attn: FOIA Service Center 2250 West John Carpenter Freeway Suite 400 Irving, TX 75063 (972) 652-3642
EASTERN REGION	Defense Contract Audit Agency Attn: FOIA Service Center 2400 Lake Park Drive, Suite 300 Smyrna, GA 30080-7644 (770) 319-4510
MID-ATLANTIC REGION	Defense Contract Audit Agency Attn: FOIA Service Center 615 Chestnut Street, Suite 1000

	Philadelphia, PA 19106-4498 (215) 597-5403
NORTHEASTERN REGION	Defense Contract Audit Agency Attn: FOIA Service Center 59 Lowes Way, Suite 300 Lowell, MA 01851-5150 (978) 551-9831
WESTERN REGION	Defense Contract Audit Agency Attn: FOIA Service Center 16700 Valley View Avenue, Suite 300 La Mirada, CA 90638-5833 (714) 228-7033
FOIA PUBLIC LIAISON	Defense Contract Audit Agency Attn: Resources, FOIA Public Liaison 8725 John J. Kingman Road, Suite 2135 Fort Belvoir, VA 22060-6219 (703) 767-2249

GLOSSARY

DEFINITIONS

The terms used in this instruction with the exception of the following are defined in the DCAA FOIA Processing Guide.

Initial Denial Authority (IDA). The Chief, Information and Records Branch, Administrative Management Division, has been delegated the authority by the Director, DCAA, to make initial determinations as to the releasability of DCAA records to the public, including Defense contractors. This authority may not be redelegated.

Appellate authority. The Assistant Director, Resources, or their designee.

Electronic Data. Electronic data are those records and information which are created, stored, and retrievable by electronic means. This does not include computer software, which is the tool by which to create, store, or retrieve electronic data.

FOIA Request. A written request for DCAA records, made by any person, including a member of the public (U.S. or foreign citizen), an organization, or a business, but not including a Federal agency or a fugitive from the law that either explicitly or implicitly invokes the FOIA, DoD Regulation 5400.7-R, or this instruction.

Administrative Appeal. A request by a member of the general public, made under the FOIA, asking the appellate authority to reverse an IDA decision to 1) withhold all or part of a requested record or 2) to deny a request for waiver or reduction of fees.

DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

DL

October 5, 2006

DCAA REGULATION
NO. 5410.11

**RELEASE OF OFFICIAL INFORMATION IN LITIGATION AND
TESTIMONY BY DCAA PERSONNEL AS WITNESSES**

Reference: DoD Directive 5405.2, Release of Official Information in Litigation and Testimony by DoD Personnel as Witnesses, July 23, 1985, certified as current as of November 21, 2003.

1. REISSUANCE AND PURPOSE. This regulation implements the reference and establishes policy, assigns responsibilities, and prescribes procedures for the release of official DoD information in litigation and for testimony by DCAA personnel as witnesses during litigation.

2. CANCELLATION. This cancels DCAA Regulation 5410.11, Release of Official Information in Litigation and Testimony by DCAA Personnel as Witnesses, dated January 29, 2001.

3. APPLICABILITY AND SCOPE.

3.1. This regulation applies to all DCAA organizational elements and all DCAA personnel. For the purposes of this regulation, "DCAA personnel" includes present and former DCAA employees and all other individuals who are hired through contractual agreements by or on behalf of the Defense Contract Audit Agency.

3.2. This regulation applies to litigation requests or demands for official information or the testimony of DCAA personnel as witnesses.

3.2.1. A "demand" is a subpoena, order, or other demand of a court of competent jurisdiction, or other specific authority, for the production, disclosure, or release of official DoD information or for the appearance and testimony of DoD personnel as witnesses.

3.2.2. "Litigation" includes all pretrial, trial, and post-trial stages of all existing or reasonably anticipated judicial or administrative actions, hearings, investigations, or similar proceedings before civilian courts, commissions, boards (including the Armed Services Board of Contract Appeals), or other tribunals, foreign and domestic. This term includes responses to discovery requests, depositions, and other pretrial proceedings, as well as responses to formal or informal requests by attorneys or others in situations involving litigation.

3.2.3. "Official information" is all information of any kind, however stored, that is in the custody and control of the Defense Contract Audit Agency, relates to information in the custody and control of the Agency, or was acquired by DCAA personnel as part of their official duties or because of their official status within DCAA.

3.3. This regulation does not apply:

3.3.1. Before courts-martial convened by the authority of the Military Departments or in administrative proceedings conducted by or on behalf of a DoD Component;

3.3.2. Pursuant to administrative proceedings conducted by or on behalf of the Equal Employment Opportunity Commission (EEOC) or the Merit Systems Protection Board (MSPB), or pursuant to a negotiated grievance procedure under a collective bargaining agreement to which the Government is a party;

3.3.3. In response to requests by Federal Government counsel in litigation conducted on behalf of the United States;

3.3.4. As part of the assistance required in accordance with the Defense Industrial Personnel Security Clearance Program; or

3.3.5. Pursuant to disclosure of information to Federal, State, and local prosecuting and law enforcement authorities, in conjunction with an investigation conducted by a DoD criminal investigative organization.

3.4. This regulation is not intended to infringe upon or displace the responsibilities committed to the Department of Justice in conducting litigation on behalf of the United States in appropriate cases.

3.5. This regulation does not preclude official comment on matters in litigation in appropriate cases.

3.6. This regulation is intended only to provide guidance for the internal operation of the Defense Contract Audit Agency and is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law against the United States or the Department of Defense.

4. POLICY. It is DCAA policy that official information should generally be made reasonably available for use in Federal and State courts and by other governmental bodies unless the information is classified, privileged, or otherwise protected from public disclosure.

5. RESPONSIBILITIES.

5.1. The General Counsel, DCAA (General Counsel) is responsible for:

5.1.1. Determining whether official information originated by DCAA may be released in litigation.

5.1.2. Determining whether DCAA personnel may be interviewed, contacted, or used as witnesses concerning official DoD information or as expert witnesses.

5.1.3. Determining what conditions will be imposed upon the release of information, interview, contact or testimony in connection with litigation.

5.1.4. Forwarding appropriate portions of litigation requests or demands to originating Components for action and receiving such referrals from other Components.

5.1.5. Furnishing the requestor or the court with a copy of this regulation, informing the requestor or court that the request or demand is being reviewed, and seeking a stay, when these actions are determined to be appropriate by the General Counsel.

5.1.6. Providing all legal advice to DCAA personnel for compliance with this regulation.

5.1.7. Consulting and coordinating with the Department of Justice in appropriate cases.

5.1.8. Delegating to the Chief Trial Attorney or other trial attorney representing a contracting activity in a proceeding before a board of contract appeals and to counsel representing the Government in Federal or State court the authority to determine whether official information will be released, DCAA personnel will appear as witnesses concerning official information, and claims of privileges will be asserted in administrative and judicial forums.

5.2. The Regional Directors and Heads of Principal Staff Elements are responsible for ensuring compliance with this regulation by their subordinates.

5.3. All DCAA personnel are responsible for:

5.3.1. Notifying the General Counsel of the receipt of litigation requests and demands.

5.3.2. Complying with the procedures of this regulation and the instructions of the General Counsel.

6. PROCEDURES.

6.1. AUTHORITY TO ACT.

6.1.1. In response to a litigation request or demand for official DCAA information or the testimony of DCAA personnel as witnesses, the General Counsel is authorized – after consulting and coordinating with the appropriate Department of Justice litigation attorneys, as required - to determine whether official information originated by the DCAA may be released in litigation; whether DCAA personnel may be interviewed, contacted, or used as witnesses concerning official DCAA information or as expert witnesses; and what, if any, conditions will be imposed upon such release, interview, contact, or testimony. Delegation of this authority, to include the authority to invoke appropriate claims of privilege before any tribunal, is permitted.

6.1.2. In the event that DCAA receives a litigation request or demand for official information that was originated by another DoD Component but is in the possession of DCAA, the General Counsel shall forward the appropriate portions of the request or demand to the originating

Component for action in accordance with DoD Directive 5405.2. The General Counsel shall also notify the requestor, court, or other authority of DCAA's transfer of the request or demand.

6.1.3. Notwithstanding the provisions of subparagraphs 6.1.1. and 6.1.2., in the event that DCAA receives a litigation request or demand involving terrorism, espionage, nuclear weapons, intelligence means or sources, or otherwise as deemed necessary, shall notify the General Counsel, DoD, who may proceed to assume primary responsibility for coordinating all litigation requests and demands for official DCAA information or the testimony of DCAA personnel, or both, in accordance with DoD Directive 5405.2 or other applicable authority.

6.2. FACTORS TO CONSIDER. In deciding whether to authorize the release of official DoD information or the testimony of DCAA personnel concerning official information (hereafter referred to as "the disclosure") pursuant to paragraph 6.1., the General Counsel and appropriate DCAA officials should consider the following types of factors:

6.2.1. Whether the request or demand is unduly burdensome or otherwise inappropriate under the applicable court rules;

6.2.2. Whether the disclosure, including release in camera, is appropriate under the rules of procedure governing the case or matter in which the request or demand arose;

6.2.3. Whether the disclosure would violate a statute, executive order, regulation, or directive;

6.2.4. Whether the disclosure, including release in camera, is appropriate or necessary under the relevant substantive law concerning privilege;

6.2.5. Whether the disclosure, except when in camera and necessary to assert a claim of privilege, would reveal information properly classified pursuant to the references of DoD Directive 5405.2, or other matters exempt from unrestricted disclosure; and,

6.2.6. Whether disclosure would interfere with ongoing enforcement proceedings, compromise constitutional rights, reveal the identity of an intelligence source or confidential informant, disclose trade secrets or similarly confidential commercial or financial information, or otherwise are inappropriate under the circumstances.

6.3. DECISIONS ON LITIGATION REQUESTS AND DEMANDS.

6.3.1. Upon receipt of a litigation request or demand, DCAA personnel will transmit the request/demand to the General Counsel by the fastest means available. DCAA personnel will not take action until the General Counsel issues specific instructions.

6.3.2. Parties seeking official information by litigation request or demand will be advised that he or she must set forth, in writing and with as much specificity as possible, the nature and relevance of the official information sought.

6 Subject to subparagraph 6.3.5., DCAA personnel shall not, in response to a litigation request or demand, produce, disclose, release, comment upon, or testify concerning any official DCAA information without the prior written approval of the General Counsel. The General Counsel may grant oral approval and, in such cases, the person receiving oral approval will ensure that a record is made and maintained.

6.3.4. In appropriate cases, the General Counsel shall notify the Department of Justice of the request or demands. After due consultation and coordination with the Department of Justice, as required, the General Counsel shall determine whether the individual is required to comply with the request or demand and shall notify the requestor or the court or other authority of the determination reached.

6.3.5. If after DCAA personnel have received a litigation request or demand and have in turn notified the General Counsel in accordance with subparagraph 6.3.1., a response to the request or demand is required before instructions from the General Counsel are received, the General Counsel, or his or her designee, shall furnish the requestor or the court or other authority with copies of DoD Directive 5405.2 and this implementing regulation, inform the requestor or the court or other authority that the request or demand is being reviewed, and seek a stay of the request or demand pending a final release determination by the Component concerned.

6.3.6. If a court of competent jurisdiction or other appropriate authority declines to stay the effect of the request or demand in response to action taken pursuant to subparagraph 6.3.5., or if such court or other authority orders the DCAA employee to comply with a request or demand, notwithstanding the Government's request for a stay, the employee will contact the General Counsel for further instructions.

6.3.7. If the General Counsel determines that no further legal review of or challenge to the court's ruling or order will be sought, the affected DCAA personnel shall comply with the request, demand, or order. If directed by the General Counsel, however, the affected DCAA personnel shall respectfully decline to comply with the demand. *See United States ex rel. Touhy v. Ragen*, 340 U.S. 462 (1951).

6.4. EXPERT OR OPINION TESTIMONY. DCAA personnel shall not provide, with or without compensation, opinion or expert testimony concerning official information, subjects, or activities, except on behalf of the United States or a party represented by the Department of Justice. Upon a showing by the requestor of exceptional need or unique circumstances and that the anticipated testimony will not be adverse to the interests of the Department of Defense or the United States, the General Counsel may, in writing, grant special authorization for DCAA personnel to appear and testify at no expense to the United States. If, despite the final determination of the General Counsel, a court of competent jurisdiction, or other appropriate authority, orders the appearance and expert or opinion testimony of DCAA personnel, the personnel shall notify the General Counsel of such order. If the General Counsel determines that no further legal review of or challenge to the court's order will be sought, the affected DCAA personnel shall comply with the order. If directed by the General Counsel, however, the affected DCAA personnel shall respectfully decline to comply with the demand.

7 Subject to subparagraph 6.3.5., DCAA personnel shall not, in response to a litigation reasonable fees, as established by regulation and to the extent not prohibited by law, to parties seeking, by request or demand, official DCAA information not otherwise available under the DoD Freedom of Information Act. Such fees may include amounts in the manner and types as provided for in DoD Directive 5405.2, such as employee and attorney costs, reproduction costs and other expenses as warranted.

8. EFFECTIVE DATE. This regulation is effective immediately.

/s/

William H. Reed
Director



DCAA FREEDOM OF INFORMATION ACT PROCESSING GUIDE

August 13, 2012

Administrative Management Division

Each year DCAA receives approximately 100 Freedom of Information Act (FOIA) requests for access to its records. Under the terms of the Act, DCAA must decide whether to comply with each request (within 20 working days of receiving it), and must disclose all records requested unless there is a specific statutory reason for exempting the information from disclosure. Gathering and reviewing the information for these FOIA requests may involve DCAA staff in every office and division.

What is the rationale behind the Act, and how can the task of fulfilling the obligations imposed by it be made somewhat easier? How do you find the records that are subject to a request and how do you determine what records or what portions of them should be withheld?

This guide has been prepared to answer these questions. It is designed for both those employees who come in contact with the FOIA infrequently and those who have direct FOIA responsibilities as part of their normal day-to-day duties.

In general, each chapter and section of this guide is organized to highlight the general principles first, followed by more detailed information and exceptions to these principles.

Table of Contents

CHAPTER 1 - OVERVIEW	1
CHAPTER 2 - WHAT RECORDS ARE SUBJECT TO FOIA DISCLOSURE?.....	5
CHAPTER 3 – HOW DOES A FOIA REQUEST GET PROCESSED?.....	10
CHAPTER 4 – HOW DO AGENCIES HANDLE APPEALS TO FOIA REQUESTS?	23
CHAPTER 5 – CAN REQUESTERS APPEAL AGENCY DENIALS IN THE COURTS?	25
CHAPTER 6 – WHAT RECORDS ARE EXEMPT FROM FOIA DISCLOSURE?	31
<u>Exemption 1 – Classified Information</u>	<u>33</u>
<u>Exemption 2 – Internal Rules and Practices</u>	<u>33</u>
<u>Exemption 3 – Information Exempted by Statute.....</u>	<u>34</u>
<u>Exemption 4 – Proprietary Information</u>	<u>34</u>
<u>Exemption 5 – Pre-decisional Information</u>	<u>35</u>
<u>Exemption 6 – Personal Privacy Information</u>	<u>37</u>
<u>Exemption 7 – Investigatory Records.....</u>	<u>39</u>
<u>Exemption 8 – Records of Financial Institutions.....</u>	<u>41</u>
<u>Exemption 9 – Oil and Gas Well Data.....</u>	<u>41</u>
CHAPTER 7 – HOW ARE FEES ASSESSED FOR FOIA SEARCHES?.....	42
CHAPTER 8 – THE PRIVACY ACT AND FOIA	51
CHAPTER 9 – THE FOIA AND CONGRESSIONAL REQUESTS.....	54
 APPENDICES	
Appendix A – The Freedom of Information Act, 5 USC 552 and Code of Federal Regulations, 32 CFR Part 290	55
Appendix B – The Privacy Act of 1974, 5 USC 552a	56
Appendix C – Reference Material	57
Appendix D – Pro Forma Paragraphs	58

Appendix E – Agency Freedom of Information and Privacy Coordinators	59
Appendix F – Boilerplate Letters and Memorandums	60
Appendix G – FOIA Forms	72

CHAPTER 1 - OVERVIEW

The Freedom of Information Act (FOIA) was enacted in 1966 and became law on July 4, 1967. It was the first of four statutes designed to open the processes and records of the Federal government to public scrutiny.

Passage of this landmark legislation was preceded by a decade of study and hearings to pierce what was called the U.S. Government's "paper curtain." In a June 9, 1955, letter from then Congressman William Dawson, Chairman of the House Government Operations Committee, to Congressman John Moss establishing a Special Subcommittee on Government Information to investigate secrecy in the Government, Congressman Dawson stated:

“An informed public makes the difference between mob rule and democratic government. If the pertinent and necessary information on governmental activities is denied the public, the result is a weakening of the democratic process and the ultimate atrophy of our form of government.”

Although Section 3 of the Administrative Procedure Act of 1946 provided that all agency records must be open for public inspection unless the agency found for good cause that the records should be held confidential, the agencies themselves decided what was "good cause." The Subcommittee found that the statute had come to be looked upon as more of a withholding statute than a disclosure statute.

In enacting the FOIA and its subsequent amendments, Congress established for the first time an effective statutory right for public access to government information. The Act provides that all records of a Federal agency must be released upon a request from any person unless the records fall within one of the nine exemptions specified in the Act; that the exemptions are to be interpreted narrowly, and that even if a record is exempt from disclosure, an agency generally has the discretion to release it anyway. In a 1978 case, the Supreme Court described the purpose of the FOIA in words similar to those used by Congressman Dawson in 1955, saying:

“The basic purpose of the FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed.”

Description of the Agency's Regulation

DCAA's regulation implementing the FOIA is set forth in Title 32 of the Code of Federal Regulations (32 CFR Part 290). The regulation discusses the procedures for requesting copies of records, the Act's exemptions, DCAA's initial determination and appeal procedures, fees, and requests for the waiver or reduction of fees.

Summary of the FOIA

The complete Act, as amended, is included in this guide in Appendix A. The main provisions are as follows:

Any person has a right, enforceable in court, of access to Federal agency records, unless those federal records are protected from disclosure by one of nine exemptions.

Federal agencies must automatically disclose the following kinds of information by publication in the Federal Register, descriptions of the agency's organization; how, where, and from whom the public may obtain information; the agency's rules of procedure; and statements of general policy.

Unless these items are published in the Federal Register, a person may not be adversely affected by them unless that person has actual knowledge of their contents.

Each agency must make available for public inspection and copying:

final opinions made in the adjudication of cases;

statements of policy that have been adopted by the agency, but have not been published in the Federal Register;

administrative manuals and instructions to staff that affect members of the public; and

a record of final votes in agency proceedings.

Federal agencies must publish a schedule of FOIA fees in the Federal Register.

Federal agencies have 20 business days, excluding Saturdays, Sundays, and legal holidays to determine whether to comply with a FOIA request for records. (This period does not begin until the request is actually received by the FOIA office). If an agency refuses and there is an appeal, the agency has 20 working days to respond to the appeal. These time limits may be extended for an additional ten business days under "unusual circumstances" (the need to collect records from field facilities, the need to search for or collect a voluminous amount of records, or the need to consult with another agency or another component of the same agency). When such a time extension is needed, the DCAA may notify the requester and offer them the opportunity to modify or limit their request. Alternatively, we may agree to a different timetable for the processing of the request. Nevertheless, if the agency does not comply within these time limits, the requester may sue the agency in court. The key consideration in this process, however, is to keep the requester informed.

There are nine specific exemptions under which an agency may withhold requested information. Exemptions (1), (3), (6), and (7)(c) are mandatory. The other six are discretionary exemptions. These include records that are summarized as follows:

- (1) Specifically authorized to be kept secret in the interest of national defense or foreign policy, and are properly classified;
- (2) Related solely to the internal personnel rules and practices of an agency;
- (3) Specifically exempted from disclosure by statute;
- (4) Trade secrets and commercial or financial information obtained from a person that is privileged or confidential;
- (5) Interagency or intra-agency memorandums or letters which would not be available by law to a party in litigation with the agency;
- (6) Personnel, medical, and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (7) Records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information:
 - (a) could reasonably be expected to interfere with enforcement proceedings,
 - (b) would deprive a person of a right to a fair trial or an impartial adjudication,
 - (c) could reasonably be expected to constitute an unwarranted invasion of personal privacy,
 - (d) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency, or authority, or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,
 - (e) 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 a law, or
 - (f) could reasonably be expected to endanger the life or physical safety of any individual;
- (8) Related to certain reports prepared by or for an agency responsible for regulating financial institutions; or
- (9) Geological and geophysical information and data, including maps, concerning wells.

Any "reasonably segregable" portion of a record must be provided to any person who requests that record after exempt portions have been deleted.

The Act may not be used to withhold information from Congress.

Each agency must submit an annual report to Congress on its FOIA actions, including the names of all agency personnel responsible for the denial of records. Generally, office directors and regional administrators are identified as the officials denying records for which their offices are responsible.

CHAPTER 2 - WHAT RECORDS ARE SUBJECT TO FOIA DISCLOSURE?

Highlights

Agency records refer to all information, including computer records, in the possession and control of DCAA that were created or obtained for an agency purpose.

Records received from applicants, contractors, and others pertaining to DCAA's regulatory functions are also agency records.

An individual's personal records, defined as follows, are not subject to a FOIA request:

Records in the possession of DCAA personnel that have not been circulated, were not required to be created or retained by the Agency, and can be retained or discarded at the author's sole discretion, or records of a personal nature that are not associated with any Government business.

All agency records within the scope of the request must be identified in response to a FOIA request. The staff does not have the discretion to decide what may be important or unimportant to a requester.

The mere fact that a record must be identified does not mean that it must be made public; it may still be withheld under one or more of the nine FOIA exemptions that may be applicable.

Good records management practices require that DCAA's official files and individual staff files be reviewed periodically to remove obsolete and unwanted material.

What is an Agency Record?

The FOIA applies only to agency records. Although the Act does not thoroughly define the word record, "*any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format,*" most agencies have adopted a definition similar to that appearing in the Federal Records Act. DCAA defines "records" as follows:

The products of data compilation, such as all books, papers, maps, and photographs, machine readable materials or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law in connection with the transaction of public business and in DCAA's possession and control at the time the FOIA request is made.

The following are not included within the definition of the word "record":

Objects or articles, such as structures, furniture, vehicles and equipment, whatever their historical value or value as evidence.

Administrative tools by which records are created, stored, and retrieved, if not created or used as sources of information about organizations, policies, functions, decisions, or procedures of the Agency. Normally, computer software, including source code, object code, and listings of source and object codes, regardless of medium are not Agency records. (This does not include the underlying data which is processed and produced by such software and which may in some instances be stored with the software).

Anything that is not a tangible or documentary record, such as an individual's memory or oral communication.

Personal records of an individual not subject to agency creation or retention requirements, created and maintained primarily for the convenience of an Agency employee, and not distributed to other Agency employees for their official use.

Information stored within a computer for which there is no existing computer program for retrieval of the requested information.

In some instances, computer software may have to be treated as an Agency record and processed under the FOIA. These situations are rare, nonetheless, they shall be treated as an Agency record:

When the data is embedded within the software and cannot be extracted without the software. In this situation, both the data and the software must be reviewed for release or denial under the FOIA.

Where the software itself reveals information about organizations, policies, functions, decisions, or procedures of the Agency, such as computer models used to forecast budget outlays, calculate retirement system costs, or optimization models on travel costs.

A record must exist and be in the possession and control of the Agency at the time of the request to be considered subject to the FOIA. There is no obligation to create, compile, or obtain a record to satisfy a FOIA request.

If unaltered publications and processed documents, such as regulations, manuals, maps, charts, and related geophysical materials are available to the public through an established distribution system with or without charge, the provisions of 5 USC 552(a)(3) normally do not apply and they need not be processed under the FOIA. Normally, documents disclosed to the public by publication in the Federal Register also require no processing under the FOIA. In such cases, DCAA organizational elements should direct the requester to the appropriate source to obtain the record.

Must DCAA Possess the Record?

To be subject to the FOIA under DCAA's regulations, a record has to be under the possession and control of the Agency pursuant to Federal law. In other words, it has to be in the physical possession and control of DCAA for an Agency purpose.

Must the Record Exist When Requested?

The FOIA applies only to records in existence at the time a FOIA request is received by the Agency. If the records have already been destroyed, or the record does not yet exist or does not exist in the form requested, there is no obligation to recreate an old record or to create a new record to satisfy a FOIA request. With respect to information contained in a computer system, there is also no obligation under the FOIA to write a special program to obtain a printout of the information in a format desired by the requester. On the other hand, there is no prohibition against creating a new record or writing a special program if it can be done more easily than searching for the original records and deleting large amounts of exempt material.

What Have the Courts Ruled About Agency Records?

The Supreme Court has observed that through the enactment of the FOIA, Congress sought to open agency action to the light of public scrutiny by requiring agencies to adhere to a general philosophy of full agency disclosure. Flowing from this concept, the Supreme Court has held that there are two prerequisites that must be met before a record is considered an agency record. First, the agency must either create or obtain the requested materials. In this regard, the Court noted that in performing their official duties, agencies routinely avail themselves of studies, trade journal reports, and other materials produced outside the agencies both by private and governmental organizations. Therefore, to restrict the term "agency records" to materials generated internally would frustrate Congress' desire to put within public reach the information available to an agency in its decision-making processes.

The second prerequisite is that the agency must be in control of the requested materials at the time the FOIA request is made. By control, the Court stated that it meant that the materials came into the agency's possession in the legitimate conduct of its official duties. Along this line, the Court specifically rejected the contention that the outside materials had to have been prepared to be relied upon in the agency decision-making.

How Do Personal Records Become Agency Records?

In some cases, personal records, regardless of format, can become agency records at a later date:

If the records are shown to another member of the staff. (DCAA then assumes that the records are being used to transmit official agency information.)

If the records are filed in branch or office files as opposed to someone's personal files.

If the records are commingled with agency records as part of an ongoing working file.

If the records are used as the basis of taking an agency action.

On the last point, courts have held that a supervisor's notes of discussions with employees remain the personal property of the supervisor, unless they are filed under the employee's name or other identifier, and thus become subject to the provisions of the Privacy Act. Even when they are personal, they cannot be used to "ambush" an employee. (In a 1982 case, a supervisor gave an employee satisfactory performance ratings for two years while simultaneously collecting adverse data. These data were later used as the basis for firing the employee. The court said that the personal notes lacked the timeliness of incorporation into agency records necessary to assure fairness under the Privacy Act. "Such an approach to the maintaining of records on employee job performance is not consistent with the Privacy Act." Additionally, once the notes are used by the agency to make a decision concerning an individual's employment status, the notes become subject to the provisions of the Freedom of Information Act.)

Saying that, three caveats must be mentioned. First, it is contrary to Federal law to remove from DCAA files the record copy of a record except in accordance with the Records Disposal Act. If such a record is removed and later located, it would still be an Agency record. Second, the intent in removing the records cannot be to avoid the FOIA when the staff person has every intent to bring the records back when later needed for an Agency purpose. Third, an employee should not remove Agency records for non-Agency purposes where the records have not been made public by the Agency and which DCAA must protect from public disclosure.

What Kinds of Records Must be Kept and for How Long?

Under the Federal Records Act, each agency is required to keep records of the agency's organization, decisions, procedures, and practices. Under the Records Disposal Act administered by the General Services Administration (GSA), GSA has provided schedules by which various types of records common to most Federal agencies may be retired or destroyed after a specified number of years. DCAA's records schedule is contained in DCAAM 5015.1, Files Maintenance and Disposition Manual. The official record copy of records listed in the schedule may not be destroyed until the period specified has elapsed, and in some cases the records must first be offered to the Archivist of the United States for permanent retention.

The GSA and DCAA records disposal schedules have a category of records referred to as "non-record material." These are records which are retained by individuals for convenience or reference, and which may be destroyed when the records are no longer needed or when their purpose has been served. Examples of non-record material are:

- extra copies of official records
- drafts
- work papers
- computations
- informal notes

At the time a FOIA request is received by the Agency, all agency records, both official record copies and non-record material, become subject to the request. No records may be destroyed after a FOIA request is received until copies have been provided in response to the

request. While any of these records may be withheld from public disclosure if they fall within one of the nine exemptions specified in the FOIA, the records must be addressed in the response letter.

From a records management standpoint and to avoid unnecessary staff time searching for records, the staff should cull official office files and individual staff files periodically to remove obsolete and unwanted material. Recognizing that many people tend to be savers, some offices may deal with this problem by establishing a policy that all records required to substantiate an office decision or action are to be kept in the office's official files, including both record and non-record material. The advantage of this procedure, if diligently administered, is that it provides a discrete file of all relevant records. It also assures that management is aware of all staff views that could be addressed in a hearing or other public forum.

The disadvantages are that such a procedure is difficult to administer and, even if put in practice, it will always be necessary to search both official and individual staff files in response to FOIA requests.

What are the Guidelines for E-Mail Records Determinations?

The Agency makes extensive use of electronic communications, specifically e-mail, to support its missions and functions. This practice has expanded greatly over the past ten years and is now the primary media utilized by DCAA staff to conduct day to day business. As technology advances, we gain even more latitude in the production of actions that are both highly efficient and effective. Our professional communication standard has evolved and is now almost exclusively supported by the resident attributes of the Agency's e-mail system.

One of the key elements to the successful use of e-mail communications is the understanding of its position as an Agency record. Plainly said, if an e-mail is used to support the missions and functions of the Agency, the communication is likely to be considered a record and subject to the retention standards codified in DCAAM 5015.1, Files Maintenance and Disposition Manual. As a record, it is also subject to public scrutiny under the auspices of the Freedom of Information Act. In consideration of these facts, e-mail communications that have value to the issuing or receiving activity, must be properly filed in approved records management systems.

These approved records system are currently the traditional hard copy folders, displaying labels identifying contents and disposition dates, and electronic filing systems. Although electronic communications can be otherwise maintained on our operating system, they cannot be adequately protected from alteration. Only an approved records management system provides this protection.

CHAPTER 3 - HOW DOES A FOIA REQUEST GET PROCESSED?

Highlights

Requesters must submit FOIA requests in writing. DCAA does not accept oral and telephone requests.

Any FOIA request received directly by DCAA staff should be forwarded immediately to their FOIA Coordinator as indicated at Appendix F. Facsimile transmissions should be used by recipients if a request is received at a management level lower than the Regional level (e.g., FAO, Sub-office).

The Act applies only to requests for existing records. A request for information which has yet to be developed cannot be released or denied under the FOIA. The proper response in this situation is a "no record" determination.

DCAA has 20 working days to make disclosure determinations on each FOIA request.

The FOIA Coordinator sends FOIA requests to the action office which might reasonably be expected to have copies of records subject to the request.

Action officers having questions about the scope or meaning of a FOIA request should contact their FOIA Coordinator immediately. A conference call can be held with the requester to resolve any open issues.

All agency records subject to a FOIA request must be identified. This means that all staff members familiar with the subject matter of the request must be contacted and all files expected to contain records must be searched.

The action office responsible for records requested must identify any information in those records which should be withheld under the FOIA, and must state why the information is being withheld.

Records must be reviewed on a line-by-line basis. Entire pages or paragraphs cannot be withheld if only a few words or phrases are exempt from disclosure.

All records requested should be provided to the FOIA Coordinator, who will prepare a coordinated response for the Agency. The Regional Director or Chief, Information and Records Management Branch, Administrative Management Division, Headquarters, DCAA, who serve as initial denial authorities, will be named in the response as a denying official as applicable.

A requester may appeal to the Assistant Director, Resources, Headquarters, DCAA if any records have been denied under the FOIA. A "no record" determination and denial of a request for a fee waiver may also be appealed.

Where Should FOIA Requests be Sent?

Under DCAA regulations, FOIA requests must be submitted in writing to the FOIA Coordinator. If any other member of the staff receives a FOIA request, he or she should send it immediately to the FOIA Coordinator.

Are FOIA Requests Processed Like Routine Information Requests?

DCAA receives many requests for information; however, only requests which specify that they are FOIA requests are processed as such. Requests which do not specify the FOIA are handled in the normal course of business by the office receiving them. When a FOIA request is received by the FOIA Coordinator, it is logged in and given a sequential FOIA number. After the request is logged, DCAA has 20 working days in which to respond to the request. Logging the request also commences the period during which records subject to the request may not be destroyed by the Agency.

How are FOIA Requests Placed under Control?

Each request received within the Agency should be placed under administrative control to ensure processing is in compliance with the time limits imposed by the Act. Upon receipt, a request should be time and date stamped by the FOIA Coordinator. All subsequent correspondence received from the requester or related to the request should also be time and date stamped.

Agency control is centrally maintained by the Information and Privacy Advisor, Administrative Management Division (CM), Headquarters, DCAA. This facilitates the production of the Annual Freedom of Information Act Report to Congress which is developed by this office. The centralization further relieves the regional offices of the annual reporting requirement.

When a request is received by a FOIA Coordinator, the FOIA Coordinator should call the Information and Privacy Advisor, CM (FOIA), (703) 767-1022. The sequential control number (e.g. I-12-001-H) should be entered in the upper right hand corner of the original request. Normally this information should be entered on the label of the case file as follows:

FOIA Request I-12-001-H

A copy of the original request should be forwarded to CM using pouch mail once it is placed under control. DCAA Form 5410-4, Freedom of Information Case Summary, which summarizes FOIA activity, and a copy of the initial determination, is also forwarded to CM (FOIA) upon completion of processing. This form is used as a feeder document to the annual report.

The sequential numbering system used to control FOIA cases is designated by various alpha and numeric codes and is divided into four parts separated by hyphens.

The first part identifies the type of request:

I for initial requests (signed by Chief, Administrative Management Division in Headquarters and the Regional Directors);

A for Appeals (processed only by Headquarters and signed by the Assistant Director, Resources).

The second part represents the year the request was received for processing by the Agency (e.g., 12 for 2012).

The third part identifies the sequential number (e.g., 298).

Finally, the processing office is designated by one of the following symbols:

H - HQS; E - Eastern; C - Central; M - Mid-Atlantic; N - Northeastern; W - Western

If it is necessary for one region to refer a FOIA request to another region, the alpha indicator will reflect both offices, e.g., H/E indicates the request was received in Headquarters and referred to Eastern.

How are FOIA Requests Evaluated?

The request is reviewed by the FOIA Coordinator to determine a number of factors:

Is the request for records, or for information that would have to be specially developed? If it is a request for information that must be developed, the FOIA Coordinator will notify the requester that there is no record. The letter may be forwarded then to the appropriate DCAA office for response.

Is the request for records which DCAA might reasonably be expected to have, or does the request deal with a subject that is primarily within the jurisdiction of another Federal agency?

Is the request understandable and reasonable in scope? If it is not clear what the requester wants, or if the request is excessively broad in scope, the FOIA Coordinator may call the requester to obtain specifics or to limit the scope of the request. Frequently, requesters will have only a vague idea of what they want or the type of records available in DCAA files. In those cases it is normally helpful to set up a conference call between the requester, the FOIA Coordinator, and the action office to discuss DCAA's files and procedures, and to seek ways to clarify the scope of the request.

Does the request deal with specific records that have been requested before or that can be readily retrieved by the action office? If the records have been requested before, and are readily available, such as with requests to Headquarters for Memorandums for Regional Directors (MRDs), the FOIA Coordinator will

respond to the requests directly. At present, approximately one quarter of DCAA's FOIA requests are handled in this way.

If the FOIA Coordinator cannot respond to a request immediately, copies of the request will be forwarded by memorandum to the office which might reasonably be expected to have the records requested. The memorandum will request a response within eight working days. The memorandum will also advise offices that the FOIA Coordinator should be kept informed of any problems or delays incurred in processing the request.

What is the Role of the Action Office?

When the FOIA Coordinator forwards a FOIA request to an action office, it should be distributed immediately to the divisions, branches, sections, or persons who have or may have the records that the requester is seeking, or who may be knowledgeable about the subject matter of the request. Offices that hold daily meetings with senior staff find the meetings an excellent opportunity to discuss any new FOIA requests, since those attending are most knowledgeable about who participated in various activities. It is also the action office's responsibility to assure that any retired records which may be subject to the request are also reviewed.

If the FOIA Coordinator neglects to forward a FOIA request to an office that may have records subject to the request, the action office should notify the FOIA Coordinator immediately. If known, the name of a staff member in another office who may have records or information concerning the request should be sent to the FOIA Coordinator. Because of the changes in personnel, action offices in other offices may not be aware of the staff's previous work assignments.

Action offices should telephone the FOIA Coordinator as soon as possible, if the request is ambiguous; or if the technical staff involved in the search believes the scope should be clarified or narrowed. As noted previously, the FOIA Coordinator can arrange a conference call with the requester to clarify the request so that it may be possible to save time that will otherwise be wasted in unnecessary searching. In the case of a lengthy search or one involving a voluminous number of records, the requester may have to agree beforehand to pay fees for searching, reviewing for release, and for copying records.

The action office should set a deadline--normally three to five working days--for their staff to make their submissions. This deadline should allow time to obtain necessary concurrences, so that a punctual submission to the FOIA Coordinator is made. If the deadline cannot be met, the action office should notify the FOIA Coordinator as soon as possible.

If the action office knows that it has not originated records subject to the request, and has received no records from sources outside DCAA, it need not search for records. However, if they have the name of a specific individual to contact, the action office must forward that information to the FOIA Coordinator.

The names of the action office's staff members who originate or receive records must be provided to the FOIA Coordinator. When the staff has submitted the results of its search, the

action office should prepare a memorandum to the FOIA Coordinator listing all the records by categories and in chronological order, oldest record on top, as follows:

- records to be released;
- records withheld in part;
- records withheld in full; and
- records from other sources (other DCAA offices or other agencies to whom the FOIA Coordinator should refer the records for review and disclosure determinations).

In reviewing the records submitted by the action office, the FOIA Coordinator should look for obvious omissions and question the action office as to the whereabouts of any missing records. For example, if a memorandum refers to an incoming letter or memorandum, has that record been produced? Are listed enclosures included?

A copy of each record listed should be enclosed, or an explanation should be provided as to why it is not enclosed. When the record is not enclosed, it must be specifically identified by date, subject, and author. (Although one office is not required to search for records originated by another office, if such records are found, they should be identified to the FOIA Coordinator in order to assure that no records are overlooked.)

The FOIA Coordinator should ensure that all records or portions of records withheld are clearly marked, and that the reason they are withheld is noted in the memorandum and appendices (i.e., the list of documents). Recommended withholdings by different members of the staff must be consistent and in accordance with office policy. If recommended withholdings are suspected to be incorrect, they should be discussed immediately with the issuing office.

Action offices should obtain all required concurrences in their own office. The office Director, or Designated Senior Official, if the function has been delegated, is responsible for making the office recommendation as to what is released or withheld.

The office Director or the Designated Senior Official will look to the FOIA Coordinator as the FOIA expert, and will seek his or her advice. FOIA Coordinators in turn may direct questions to the Information and Privacy Advisor, Headquarters, DCAA. The action office's job is to identify correctly all responsive records while the FOIA Coordinator is required to protect the Agency from releasing information that should be withheld and denying information that should be released.

What are the Roles of the Technical and Administrative Staffs?

If there are any questions concerning the scope of a request, the action office should arrange to clarify it with the FOIA Coordinator. Once any questions concerning the scope of the request are resolved, the search for records should proceed immediately.

The FOIA Coordinator will specify the date by which the search and review must be completed. If it is impossible to meet the deadline because of significant work conflicts or for other valid reasons, the FOIA Coordinator should be notified immediately. An estimate of the date by which the search is expected to be completed should be made and, if necessary, scheduling priorities should be resolved with higher level management.

All Agency records that are subject to the request must be identified. Under the FOIA, the Agency does not have the discretion to decide whether or not a record is significant or insignificant, important or trivial. If it is an Agency record and it falls within the scope of the request, it must be submitted and dealt with in the response letter.

The test of the legal adequacy of a FOIA record search is one that includes all records which a person, who is familiar with the subject matter of the request, can be expected to locate in a reasonable amount of time. A good faith effort is required to meet this test. This means that:

All persons knowledgeable about the subject of the request and likely to have records are contacted.

The search for records includes all files (to include computer) that are likely to have records responsive to the request.

The adequacy of an Agency's search is measured by the standard of reasonableness, and is dependent upon the circumstances of the case.

Normally, the action office need only look for records prepared up to the date of the request. (The FOIA does not require that a request be open-ended for records yet to be created or those of a continuing nature). However, if there is an extended delay in responding to the request, the FOIA Coordinator should be informed so that he or she can assign a new due date.

If personal notes are intermingled with Agency records, there is a presumption that they are Agency records and are subject to the request.

If the request is only for a specified report, other information such as drafts, background material, or other records, need not be furnished, even though the requester may find them useful.

A record does not have to comply in every detail with a request to satisfy the request. For example, if a requester asks for certain information in alphabetical order, and the staff

organizes it in some other sequence, it is not necessary to alphabetize it. Similarly, the Agency does not have to produce a computer printout in the exact format specified by the requester if a new program has to be written to put it in that format. The staff need only furnish those existing records which pertain to the subject of the request.

The issue of whether records are actually created or merely extracted, with respect to electronic records, from an existing database is not always readily apparent. Consequently, when responding to FOIA requests for electronic data where creation of a record, programming, or particular format is questionable, activities should apply a standard of reasonableness. In other words, if the capability exists to respond to the request, and the effort would be "a business as usual" approach, then the request should be processed.

A record may not be destroyed once a FOIA request is received, even though it could be destroyed under the terms of the Federal Records Act and the DCAA Files Maintenance and Disposition Manual (DCAAM 5015.1). Once a FOIA request covering that record has been received, it must be released unless it can be exempted under one of the FOIA exemptions.

Special categories of records:

Records originated by another DCAA office - These should be identified in a listing separate from records originated by the action office, and copies forwarded to the FOIA Coordinator. The action office need not search for records from other offices. Thus, the action office, knowing it would otherwise have a negative reply to the request, may ignore searching for the records received from other DCAA offices. The FOIA Coordinator should be informed, however, and provided the name of the individual or branch in another office who should be contacted, if known.

Records received from other agencies - Normally, these are referred back to those agencies for direct response to the requester. The requester should be advised in writing by the FOIA Coordinator of such a referral. If such information is contained in a DCAA record, the FOIA Coordinator will consult the other agency as to its availability. DCAA will then respond to the request for both agencies or refer the document to the originating agency.

Draft records - Drafts still in DCAA's possession are subject to the FOIA. They must be included in a submission to the FOIA Coordinator even though they have been superseded by subsequent drafts or final records.

When all the records subject to the request have been assembled, the action office staff should review them to identify all sensitive records and to recommend what records or portions thereof should be withheld.

The information to be withheld under one of the FOIA exemptions must be segregated from those parts of a record which can be released. Therefore, those portions to be withheld from public disclosure should be bracketed in red (preferably with a red pencil that can be whited

out if necessary). The complete record, exempt and nonexempt, must be furnished to the FOIA Coordinator for review and concurrence when information is to be withheld.

What are the Roles of the HPSEs and Regional Directors?

Each DCAA office subject to a FOIA request (e.g., FAO or Division within a HPSE or Regional Headquarters) is responsible for recommending whether to disclose or withhold, in whole or in part, each Agency record identified in that office.

Each HPSE or Regional Director is responsible for ensuring that the office meets its obligations under the FOIA.

FOIA exemptions are, for the most part, discretionary; meaning that if there is no harm to the Government or any member of the public, then the record should be released. For example, a predecisional record need not be withheld merely because it might be exempt under Exemption 5. Records must be reviewed for withholding on a line-by-line basis. Entire pages or paragraphs cannot be withheld if only a few words are legally withholdable.

Care must be taken to exercise discretionary release of otherwise exempt records. However, Exemptions 1 and 3 have no discretionary latitude. Likewise, Exemptions 4, 6, and 7(c) may lose their discretionary latitude after the results of a predisclosure notification or the conduct of balancing tests (balancing the public's right to disclosure against the individual's right to privacy) are determined.

Care also should be taken to delete personal privacy information, such as birth dates, home addresses, phone numbers, and social security numbers.

The responsibility for identifying sensitive records and information belongs to the office in which the records originated or which is principally responsible for the records. Because of the volume of records involved, the FOIA Coordinator's review is limited to determining if information proposed to be withheld is consistent with Agency regulation and policy. Therefore, it is very important that action offices conduct a general review of documents responsive to FOIA requests to ensure that all sensitive information is identified. If information is inadvertently released, it normally cannot be recalled.

Who Coordinates DCAA's Response to a FOIA Request?

After a response has been received from each of the offices to which a FOIA request was sent, the FOIA Coordinator will prepare a coordinated Agency response to the request. If the request involves a significant number of records, or if the responses from some offices are delayed, the FOIA Coordinator will prepare a partial response, or a series of partial responses, depending upon the situation. Each record released or denied is identified on an appendix to the response. (In cases involving an on-going investigation, records are identified as a group rather than specifically identified in order not to disclose the focus of the investigation or allow those being investigated to hide or destroy potential evidence).

If records are denied, the applicable FOIA exemption(s) for the denial are specified. The response also names the denying official who is the head of the particular office involved (e.g., Regional Director). The letter also informs the requester that any denial may be appealed within 60 calendar days to the Assistant Director, Resources, Headquarters, DCAA. Any records denied by DCAA must, under DCAA's Files Maintenance and Disposition Manual (DCAAM 5015.1), be retained for a period of six years after denial of the initial request or, if there was an appeal, six years after denial of the appeal (See DCAAM 5015.1, series 502.5 and 502.6).

Should Contractor Names be Exempt from "FOIA Material" Considered Releasable?

Contractor names are considered exempt information per Exemption 6.

When Part of the Record to be Released Originates Outside of DCAA, Should the Requester be Routinely Advised to Contact the Originator to Obtain that Portion of the Record?

The requester should not be "referred" to another agency for material which is considered part of a DCAA record (e.g., enclosure to an MRD) and the information is clearly releasable. If a release determination cannot be established during review by the action office, the record may be referred to the originator for processing, after coordination with the originator.

Essentially, when DCAA locates records responsive to a request which were generated by another Federal agency, the standard procedure has been to "automatically" refer either the record or the requester to the originating agency for processing. The FOIA, however, not only gives agencies the authority to make a release determination on any record in the possession and control of the Agency, but compels them to do so. In this light, DCAA offices should consider externally generated records. (Note: Control of the record means that the materials came into DCAA's possession in the legitimate conduct of its official duties).

What is the Procedure for Handling Audit Reports Subject to the FOIA?

The purpose of this section is to standardize Agency processing procedures for handling audit reports, solicited under the Freedom of Information Act, whose release is dependent upon the consent of the receiving DoD contracting officer to whom the report was furnished.

The compelling reason for formalizing procedures for processing requests of this type is the literal dependency the disposition of the audit report has on the related working papers maintained by the Agency. Further, given that no DCAA decision on the working papers may be consummated until the releasability of the audit report is formally determined, the management of the affected referral is often significantly impaired as to delay processing for an indefinite period of time. Therefore, since the Act mandates that requests submitted under the FOIA be processed in a timely fashion, it is necessary that we take a proactive position in dealing with the respective contracting officers.

The intent of the following practice or technique is to ensure that this Agency is in full control of the request during the life cycle of the FOIA request. It further provides methods that

facilitate the "consultative process" with the contracting officer by offering specific criteria which delineate responsibilities and identify DCAA actions related to the case.

The typical scenario described is one that finds the requester seeking both the audit report and working papers where the releasability of the audit report is not yet known. In accordance with the provisions of section C1.5.9.3, DoD 5400.7-R, DoD Freedom of Information Act Program, it has been determined that "the advisory report (audit report) should be referred to the appropriate DoD contracting officer."

The specific efforts necessary to process the FOIA are as follows:

Refer the Audit Report and FOIA request to the contracting officer's FOIA Coordinator. It is important to note that any other destination may remove the request from FOIA channels and be perceived as a routine administrative action by those not versed in the FOIA.

How are Requests for Audit Reports without Working Papers Processed?

This section provides procedural guidance on the processing of requests submitted to the Agency for copies of audit reports without concurrent demand for related working papers. The prime motive in formulating standard processing procedures is to ensure that Agency resources are not spent in the production of records when cognizant release authority rests with another component.

Qualifying requests are those that seek "e.g., all audit reports from 198X to present related to XYZ company" and/or specifically identify the audit report(s) by number that are perceived to be on file with the Agency.

In cases where only the company name is known, FOIA Coordinators should refer to the Contractor Alpha Listing for the identification of the "R/ORG" code of the DCAA office responsible for that contractor. The first four digits of the audit report number also identifies the "R/ORG" code. The R/ORG code assigned to the DCAA activity may be verified by referring to DCAAP 5100.1, Directory of DCAA Offices.

FOIA Coordinators should then refer the request directly to the Contracting Officer's FOIA Coordinator and inform the requester accordingly. Requesters should be provided with a brief explanation of DCAA's role in the audit report and its intended purpose. They should also be advised that section 1-508d of DoD 5400.7-R, DoD Freedom of Information Act Program (32 CFR 286.7(i)(4)) requires that these advisory reports (audit reports) be referred to the appropriate contracting office for release determination.

Requests for audit reports generated for non-DoD agencies should be treated as requests for DCAA records since the DoD FOIA regulation does not address them. Moreover, the theory underlying referral to another component, i.e., DoD is one agency and can determine which of its activities will respond to a FOIA request, is not applicable to this case. However, this does not preclude the coordination of such actions with the non-DoD agency.

How are Requests for Audit Reports and Working Papers Processed that are Predecisional and Deliberative?

This provides procedural guidance concerning the processing of requests for audit reports and their related working papers where the contracting officer has determined the report to be "predecisional and deliberative" and thereby subject to the deliberative process privilege of Exemption 5 of the Freedom of Information Act.

Should We Verify Representation Claimed by Law Firms on Behalf of Their Clients Seeking Copies of Records Under the Freedom of Information Act?

It has become common practice for law firms representing DoD contractors to file FOIA requests on behalf of their clients. These requests usually contain either a statement indicating that fact or a signed notice from their client authorizing the release of their records directly to the requesting law firm. This condition often raises questions pertaining to the authenticity of such claims from Agency personnel tasked to respond to these FOIA requests. These concerns surface as a result of our Agency's innate interest in protecting the commercial and financial position of DoD contractors subject to DCAA review.

As a matter of practice, verification of representation is not required and may be taken at face value. Severe penalties would be imposed on any attorney fraudulently seeking copies of confidential commercial or financial information on a DoD contractor. As a result, risk of wrongful disclosure is considered minimal.

This standard, however, does not necessarily apply to other requesters outside of the legal community. Each case must be reviewed on a case-by-case basis for application of the requirement to verify or validate the interests of the requester.

Who is Responsible for Processing FOIA Requests Applicable to More Than One Region and/or the Headquarters?

The handling process depends primarily on the type of action required to satisfy the request. After review of the request by the FOIA Coordinator, the request may be centrally processed or responses may be decentralized based on the criteria stated below.

A decentralized method of processing is utilized where each FOIA Coordinator reacts only to those records under his/her cognizance. Typically, this is done when a single requester is seeking records related to a specified subject which may be available at given locations within the Agency. This type of record is not normally connected to those records located elsewhere in the Agency. Usually, processing is limited to determining the availability and releasability of the responsive records. An example of a typical request of this type would be one that seeks copies of audit reports on XYZ Company at location East coast and location West coast. On requests received directly by the Headquarters, the Information and Privacy Advisor will review the content of the request and will resolve outstanding issues (when ascertainable and within the Headquarters control, e.g., problems related to the requester's description of the requested

records; adequacy of the fee declaration; scope of the request; etc.), prior to referring the request to the region(s) for processing.

A centralized method of processing is desirable when a requester is seeking records which are highly complex, broad in scope but reasonably described, and due to the nature and sensitivity of the action, require a consolidated Agency response. Unlike decentralized requests which are not interdependent, consistency of interpretation is significant to the Agency's position on the releasability of the records. In cases of this type, the Headquarters would serve as the central processing activity.

When the Agency Refers Documents to Another Agency, Does This Release DCAA from Further Obligation Pertaining to the Case?

Technically, the Agency has a continuing obligation to the requester with regard to the referred documents. In fact, since DCAA has possession and control of the requested records, the responsibility to process the request remains with DCAA. However, the common practice and generally the accepted one, is to close out the case upon referral of documents to the originating or cognizant agency. The obvious benefit of this practice is the elimination of a series of processing tasks associated with coordinating determinations between several agencies and the inherent demand on internal resources. Further, this back and forth exercise is not normally very efficient for the requester as the process consumes much more time than a direct referral.

As a method of monitoring the activities related to the processing of documents provided to another agency as part of a referred case, the referral letter should include a request for a copy of the final response to the requester, citing our control number.

Which Region Should Process a FOIA Request for an Assist Audit Report and Work Papers When an FAO from One Region Conducted the Assist Audit for an FAO in Another Region?

This issue depends on who receives the FOIA request, who has the audit report and working papers, and who reacts to the request. If the region that receives the request has the work papers and audit report, it should refer the audit report to the DoD contracting officer for a release determination and process the portion pertaining to the work papers in accordance with our established procedures for such records. If, however, the receiving region does not have the requested documents, it has no records to respond to the request. As such, it should treat the request as misdirected correspondence and forward the request to the region that has the requested documents.

How Do We Assist a Requester Who is Seeking Extremely Broad Information?

Occasionally FOIA requesters come to the Defense Contract Audit Agency for contract information based solely on our name. Most of these requests are very general and often state that they are looking for any information on XYZ Company. Obviously we can help to some degree, but when the request is general we can probably assist the requester more by advising them of the existence of the Federal Procurement Data Center (FPDC).

The FPDC carries all kinds of information on contracts let by the Federal government. The information is detailed and can be tailored to the requester's specific needs. This little known element of the General Services Administration can provide most of the information a requester is seeking. Based on the information obtained from the FPDC, the requester can more effectively draft requests which can easily be identified and processed without undue demand on DCAA's valuable resources.

The Federal Procurement Data Center may be contacted by calling (202) 401-1529 or by writing to the U.S. General Services Administration, Federal Procurement Data Center, 7th and D Streets, SW, Room 5652, Washington, DC 20407.

How Do We Handle Requests for Contractor Records?

Contractor records are often the subject of Freedom of Information Act requests submitted to various levels within DCAA. Although the handling of such requests is usually fairly routine, Regional FOIA Coordinators should consult with the Investigations Support Division (RSI) to determine if the named contractor is currently under investigation prior to assigning the request to an FAO for processing. If RSI responds in the affirmative, Regional FOIA Coordinators should refer the request to the investigative agency for processing. However, if RSI indicates that the contractor is unaware of the investigation and that contractor knowledge of the investigation would harm the investigative process, Regional FOIA Coordinators will respond to the requester using a glomar approach (i.e., neither confirm or deny the existence of responsive records).

This guidance does not apply to the referral of records pertaining to contractors from investigative agencies. In this instance, the investigative agency is simply returning Agency records to DCAA for release determination and direct response to the requester. The investigative position of these records is no longer an issue.

CHAPTER 4 - HOW DO AGENCIES HANDLE APPEALS TO FOIA REQUESTS

Highlights

If DCAA initially denies a request for records, the requestor has the right to appeal that decision to DCAA and, if denied on appeal, to seek a judicial review of the denial in a Federal District Court.

When an appeal is received, the Agency must reconsider its decision to assure that the records denied are still legally withholdable and should continue to be withheld. At this time, new exemptions may be cited or previous ones disregarded.

Normally, DCAA must respond to a FOIA appeal within 20 working days.

How Long Do Requesters Have to Appeal a Denial?

A requester has the right to appeal the denial of records, or the denial of a request for waiver of fees, within 60 calendar days of receiving DCAA's denial. All appeals are forwarded to the Assistant Director, Resources, Headquarters, DCAA, as the central DCAA control point, where they are assigned a sequential number for processing.

Can a Requestor Appeal a Delay in the Initial Request?

A requester may appeal DCAA's lack of a timely response to an initial request. In that case, the initial request and the appeal are processed concurrently. If any records are denied, the requester is given new appeal rights.

How are Appeals Processed?

The following procedures apply to the processing of appeals when DCAA denies records in response to an initial FOIA request.

The appeal is sent to the Assistant Director, Resources where the Information and Privacy Advisor date marks the appeal letter and assigns it a sequential appeal number (e.g., A-12-001-H, the first position letter "A", designating appeal, in place of the original symbol "I" which represents initial requests).

The Information and Privacy Advisor will review the records denied and consider any new information presented in the appeal, and make a recommendation as to whether the records, in whole or part, should continue to be withheld from public disclosure. This reviewing official will consider arguments presented in the appeal letter, changes in circumstances because of the passage of time, and whether releasable information is scrupulously segregated from information that is not releasable.

The Information and Privacy Advisor will submit determinations along with a copy of the records to the Office of General Counsel, which will review the recommendation to assure its adequacy and identify any issues they should address.

The Office of General Counsel will review the information denied if applicable to assure that the denial is legally correct. If the appeal is denied, the response will include specific information regarding the basis for the denial and will advise the requester of his/her right to seek judicial review under 5 U.S.C. § 552(a)(4)(B) and 32 CFR 290.7.

How Long Does DCAA Have to Respond to an Appeal?

All issues on appeals should be resolved by the 15th working day after the appeal is received unless it is necessary to consult with another agency or to obtain a company's review of proprietary information. Thereafter, the appellate authority will prepare DCAA's approval or denial of the appeal for the signature of the Assistant Director, Resources. If the request is denied, the requester will be informed that a judicial review of the denial is available in the Federal district court in which the requester resides, has his or her principal place of business, where the agency records are located, or in the District of Columbia.

Unless there are extenuating circumstances, DCAA's response should be signed and mailed by the 20th working day after the appeal was received.

Under DCAA's records disposal schedule, FOIA appeals and records denied under any appeals are to be maintained by the Agency for six years from the date of the response.

Can a Requester Appeal a "No Record" Determination or Fee Waiver Denial?

The requester must be given the opportunity to challenge the adequacy of the Agency's search under the appellate process. All "no record" responses shall provide an adequate statement offering appeal rights in accordance with established administrative appeal procedures. An example of a suitable response is as follows:

After a thorough search of Agency records, we have determined that we have no records responsive to your request. Should you disagree with the finding cited above, you may appeal in writing within 60 calendar days from the date of this letter to Mr. J. Philip Anderson, Assistant Director, Resources, 8725 John J. Kingman Road, Fort Belvoir, Virginia 22060-6219.

In the event of a denial of a fee waiver request, the requester must be advised of appeal rights available as outlined above.

CHAPTER 5 - CAN REQUESTERS APPEAL AGENCY DENIALS IN THE COURTS?

Highlights

An individual may sue an agency under the FOIA in a U.S. District Court if the agency:

withholds requested records or portions thereof, denies a request for waiver of fees, or fails to respond within the statutory time limits.

FOIA litigation is handled by the Office of General Counsel (DL), working with the Department of Justice.

In defending against FOIA suits, Agency staff involved in searching for and reviewing documents may be requested to prepare, under oath, detailed affidavits regarding their actions in processing a request or why they believe specific documents are exempt from public disclosure.

Agency staff may also be subject to written interrogatories or oral depositions, which may subsequently be used during the course of legal proceedings.

A Vaughn Index, which is an itemized description of each document withheld, the applicable FOIA exemption, and the basis for asserting the exemption, must normally be prepared by the staff in each FOIA case.

Courts may examine agency documents in camera, meaning in private, to verify agency claims that the records are being validly withheld.

If the plaintiff (requester) "substantially prevails" in a FOIA suit against the Agency, the U.S. Government may be required to pay reasonable attorney fees and costs for the plaintiff.

A court has the authority under the FOIA to refer matters for disciplinary action to the Special Counsel of the Merit Systems Protection Board if it finds that "Agency personnel acted arbitrarily or capriciously with respect to the withholding."

When May a Requester Sue an Agency?

The FOIA, 5 U.S.C. § 552 provides that if a FOIA request is denied on appeal, the requester may seek review in a U.S. District Court in which the requester resides, or has his principal place of business, or the records are situated, or in the District of Columbia.

Normally, before going to court, persons must exhaust their administrative remedies; that is, there must be a final decision denying the documents by the Agency. However, the FOIA provides that if the Agency does not respond to a FOIA request within the statutory time limits (normally 20 working days for an initial request and 20 working days for an appeal), the requester may treat such delay as a denial of the request and may immediately file suit in a district court. In practice, persons who file FOIA requests with DCAA seldom go directly to

court even if the Agency is tardy in responding to the request. There are reasons for this. First, DCAA keeps the requester informed periodically regarding the status of the request. Second, it is unlikely that anything would be gained by filing suit early. In *Open America v. Watergate Special Prosecution Force*, the court held that an agency is deemed to be in compliance with the FOIA if it is exercising good faith and "due diligence" by processing requests in the order in which they are received, absent a demonstration of "exceptional need or urgency" by the requester. Under this commonly accepted approach, the courts get involved immediately only in cases in which an agency is not exercising "due diligence" with respect to an individual request, or is "lax overall in meeting its obligations under the Act with all available resources," or when the requester can show a genuine need for having the request processed out of turn.

How Does a FOIA Suit Begin?

A FOIA suit against an agency begins with the filing of a Summons and Complaint, usually by the requester's attorney, in a U.S. District Court. It sets forth the parties involved, the nature of the action, the basis for the court's jurisdiction, the factual basis of the suit, including the records requested, correspondence between the parties, and the records denied by the agency. It also alleges that such withholding by the agency is contrary to law and requests that the court order the agency to make the records immediately available. Frequently, the complaint will also request that the court award the plaintiff reasonable attorney's fees against the Government.

After receiving a copy of the Summons and Complaint, the agency has 30 days to respond. The response sets forth in broad terms the agency's reaction to the complaint, and attempts to narrow those items at issue in the suit.

DCAA's responsibility for action on a FOIA suit is handled by an attorney in the Office of General Counsel. The attorney forwards copies of the summons and complaint to the Information and Privacy Advisor, obtains a copy of the file on the processing of the request, including copies of any withheld documents, and consults with the staff of those offices responsible for the documents withheld in preparing an answer to the complaint. The answer to the complaint is signed by an attorney in the Department of Justice, which acts as the Government's lawyers.

What is a Vaughn Index?

The FOIA establishes a presumption that all agency records should be made available to the public, and the burden is upon the agency to overcome this presumption and sustain its decision to withhold records. To meet this burden of proof for information withheld, agencies must prepare a Vaughn Index, which is an itemized list describing each document or portion of a document withheld, and asserting the basis for the exception. The Vaughn Index is based on a case in the D.C. Circuit of the same name. The preparation of Vaughn Indexes and supporting affidavits are difficult, time consuming, and require the close collaboration of the technical staff most familiar with the records and the attorneys handling the case. Where large numbers of records are involved, it may be possible to prepare a Vaughn Index on only a representative sample of records rather than all records withheld. In any case, this process requires that every

record withheld be reviewed to assure that it is legally withholdable and it is in the public interest to continue to withhold the document.

Is the Agency Required to Produce a Vaughn Index at the Administrative Level?

The Vaughn Index was fashioned only in connection with the adjudication of a defendant agency's motion for summary judgment in litigation and does not apply to the administrative process. There is no requirement that administrative responses to FOIA requests contain the same documents necessary in litigation. In fact, no court has held that a requester may compel production of such an index at the administrative level.

By definition, the decision in *Vaughn v. Rosen* requires agencies to prepare an itemized index, correlating each withheld document (or portion) with a specific FOIA exemption and the relevant part of the agency's nondisclosure justification. The primary purpose of the index is to allow a clear explanation of why each document or portion of a document withheld is claimed to be exempt from disclosure.

The statutory language of the FOIA requires only that an agency inform the requester of the reasons for the denial of an initial request, of the name and title of each person responsible for the denial, and the right to administrative appeal. See 5 U.S.C. § 552(a)(6)(i), (6)(C).

Will the Courts Allow Discovery?

Discovery, available in U.S. District Courts under the Federal Rules of Civil Procedures, is only allowed with the permission of the court, and may be either oral or written. Essentially, it is a process by which one party to a proceeding uncovers information known exclusively to or in the possession of the other party to the proceeding, and which the party requesting discovery believes are necessary in order to obtain a fair resolution of the case.

Normally in FOIA cases, the court relies on the Vaughn Index and affidavits submitted by the parties, and will not permit discovery. An agency is required by affidavits to show how the FOIA request was processed; it must identify its records management policies, procedures, and practices as it relates to the requested records and the possible locations of such records. It must identify specifically what offices and staff were contacted, and what files were searched for records subject to the request. The agency officials responsible for the search must also certify that to the best of their knowledge all records subject to the request were identified.

If legitimate questions are raised concerning the thoroughness of the search, the court can permit interrogatories or depositions of the staff. Depositions are taken under oath and in the presence of a court reporter. Opposing counsel may try to elicit information which would not otherwise be available under the FOIA. Statements made during FOIA discovery are admissible in these proceedings and may be used to challenge or discredit the testimony of DCAA staff witnesses.

Will the Courts Examine Agency Records in Detail?

The FOIA provides that a court "may examine the contents of ... agency records in camera to determine whether such records or any part thereof shall be withheld ..." In camera, meaning in private, refers to the review by a judge of records in the judge's chambers. Opposing counsel and the public are not permitted to see in camera filings.

In camera inspection is discretionary with the court, and generally is the exception rather than the rule since courts do not have the time to conduct detailed reviews of voluminous documents. It may, however, be used to test the agency's claims of exceptions where the Vaughn Index is too vague or the agency's claims of withholding are too sweeping.

In cases involving classified information, national security interests, or law enforcement investigations; where it is not possible for the court to make a decision based upon the information presented in the public record; the court may also allow the Government to file an ex parte in camera affidavit which is not made available to opposing counsel. This process is extremely rare, and is allowed only when the Government can demonstrate that the interests of the adversary process are outweighed by other crucial national security or law enforcement interests.

How Does a Court Make its Decision?

In virtually all FOIA cases, the court makes its decision based upon the written records (pleadings, depositions, interrogatories, and affidavits) filed in the case. The method normally used for doing this is review by the judge of these written records submitted by the agency. The average FOIA case in the D.C. Circuit Court takes between one and one-half to two years from start to finish.

Can a Court Decision be Appealed?

The losing party in the District Court may appeal to the Court of Appeals (or appellate court). In reviewing FOIA decisions, the appellate court determines, as a matter of law, whether the District Court had an adequate factual basis for its determination, and assuming an adequate factual basis, whether the court's determination was clearly erroneous. If there was not an adequate factual basis, the appellate court normally remands the case back to the District Court with instructions to make additional findings.

Exemptions which were not raised by the Government in the District Court are normally considered waived and cannot be raised for the first time in the appellate court. If the Government loses in the District Court, it can obtain a stay of the court's order to disclose records since disclosure of the records at that time would in essence comply with the request and make the case unnecessary.

Can an Appeal be Made to the Supreme Court?

The losing party at the appellate level may appeal to the Supreme Court of the United States. Unlike the appellate court, the Supreme Court does not have to take the case, and will do so only if the case presents an important Constitutional issue or if there is a split in decisions among the various Circuit Courts of Appeals. If the Supreme Court does not take the case, the decision of the Court of Appeals stands as the final decision on the matter.

How do the Courts Award Attorney Fees?

Under the FOIA, a court may assess against the Government "reasonable attorney fees and other litigation costs reasonably incurred in a case...in which the complainant has substantially prevailed" at both the District Court and appellate court level. In *Cuneo v. Rumsfeld*, the court said:

"Congress realized that too often the insurmountable barriers presented by court costs and attorney fees to the average person requesting information under the FOIA enabled the Government to escape compliance with the law."

In order to "substantially prevail" and receive attorney fees and costs, the plaintiff must show that initiating and prosecuting the litigation was in process. It is not enough to show the mere fact that documents were released after the filing of the suit.

Assuming the plaintiff has substantially prevailed, the court still has discretion to decide whether fees should be awarded and, if so, the amount of the award. In making its determination, the court is generally guided by four criteria:

- (1) the public benefit derived from the case,
- (2) the commercial benefit to the complainant,
- (3) the nature of the complainant's interest in the records sought, and
- (4) whether the Government's withholding had a reasonable basis in law.

If a court decides to award attorney fees, the amount of the award is dependent upon the number of hours reasonably expended on this type of case multiplied by the attorney's reasonable hourly rate. Fees for paralegals working on the case are also covered. However, work done by an attorney at the administrative stage (making the initial FOIA request and handling any appeal within the agency) is not covered. In addition, attorney fees for an individual suing on his or her own behalf are not normally recoverable, except in the D.C. Circuit Court. Litigation costs (the cost of filing, depositions, reproduction, mailing, etc.) are recoverable in either case. Also, although the FOIA provides that courts may only award costs "against the United States," at least one court (the D.C. Circuit) has used Rule 39(a) of the Federal Rules of Appellate Procedures to award costs to the Government when it was successful in defending a FOIA appeal.

As a case in point, the adequacy of search conducted by the Agency in response to a FOIA request can be challenged. If the Agency claims that no further records exist, and, for example, additional documents are located during the discovery process, the Courts will be highly likely to rule in favor of the requester and allow attorney's fees and litigation costs. As such, searches for responsive records must be processed with due diligence and thoroughness to ensure that all records sought by the requester are identified.

Attorney fees and litigation costs in FOIA cases can be substantial and are paid by the Agency out of appropriated funds.

Can the Courts Discipline an Agency Employee?

Section 552(a)(4)(F) of the FOIA provides that "whenever the court orders the production of any agency records improperly withheld from the complainant and assesses against the United States reasonable attorney's fees and other litigation costs, and the court additionally issues a written finding that the circumstances surrounding the withholding raise questions with respect to the withholdings, the Special Counsel shall promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding ..."

The sanctions provision of the FOIA was made as part of the 1974 amendment to the Act. In 1976, a D.C. Court in *Holly v. Acree* made a finding that agency officials may have acted arbitrarily or capriciously. However, after its investigation, the Civil Service Commission, which at the time was responsible for investigating court referrals, declined to take any disciplinary action. There have been no reported cases since.

CHAPTER 6 - WHAT RECORDS ARE EXEMPT FROM FOIA DISCLOSURE?

Highlights

The FOIA requires that any reasonably segregable portion of a record be made available upon request after deletion of the exempt portions of the record.

Except for drafts and certain legal records, all records must be reviewed on a line-by-line basis to segregate exempt from non-exempt information records.

If, after deletion of the exempt information, the remainder is essentially unintelligible, in most cases, the entire record may be withheld from disclosure to the requester.

Commercial use requesters may be charged for the staff time spent reviewing records for exempt information and for making the actual deletions. No other requesters can be charged for such activities for reviewing records for releasability.

Section 552(b) of the FOIA requires that:

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection meaning the nine exemptions of the FOIA.

How is Exempt Segregated from Nonexempt Information?

This chapter discusses each of the nine exemptions to the FOIA, its applicability to DCAA, and the Agency's duty to segregate exempt information from nonexempt information. The nine exemptions to the FOIA which permit an agency to withhold records are listed below.

1. Classified Information
2. Internal Rules and Practices
3. Information Exempted by Statute
4. Proprietary Information
5. Predecisional Information
6. Personal Privacy Information
7. Law Enforcement Records
8. Records of Financial Institutions
9. Oil and Gas Well Data

What Have the Courts Said about Segregating Information?

In applying the segregation requirement of determining what is "reasonably segregable," courts in the past have evaluated a combination of what is intelligible and the extent of the burden upon an agency in segregating material. Courts also have the discretion to review the records in camera to determine if the extent of an agency's deletions is reasonable. If the exempt

and nonexempt portions of a record, particularly a predecisional record, are so "inextricably intertwined," that release of segregable portions would reveal the deliberative process itself, then the entire record may be withheld.

What is the Best Technique for Reviewing Records?

To the extent possible, a records reviewer should go through all the records at one sitting rather than spreading the review out over several days. If it is not possible to review everything at one time, the reviewer should at least scan all the records at one time after completing the review to assure that the information deleted is consistent.

Records must be reviewed on a line-by-line basis. Entire pages or paragraphs cannot be withheld if only a sentence or a few words are exempt.

Material to be deleted should be bracketed in red pencil and the applicable FOIA exemption should be noted in the margin. A red pen, or any pen for that matter, should not be used to mark material to be deleted since ink cannot be readily whited out or erased if changes are made.

After the staff reviewer has completed marking the records, the Designated Senior Official for the office reviews all withheld records and material to be deleted on substantive grounds.

Offices must forward copies of all records proposed for withholding, in whole or in part, to the FOIA Coordinator. A memorandum accompanying the records should state the rationale for withholding, and contain separate appendices listings, in date order, all records withheld in whole or in part and identifying the exemptions involved for the denials.

The FOIA Coordinator will review the records, or portions thereof, recommended for withholding with respect to compliance with past practice and procedures, applicability of the claimed exemption to the records, and the internal consistency of the information deleted within the records.

Because of staff constraints, the FOIA Coordinator does not review records proposed for release. Consequently, each office must ensure that a record to be released contains no information that should be withheld, such as classified, proprietary, or personal information, or information that is contained in another record which is being withheld.

When is a Discretionary Release Appropriate?

It is DCAA policy to make records publicly available, unless they qualify for exemption under one or more of the nine exemptions. DCAA organizational elements may elect to make a discretionary release, however, a discretionary release is generally not appropriate for records under exemptions 1, 3, 4, 6 and 7(c). Exemptions 4, 6, and 7(c) cannot be claimed when the requester is the submitter of the information.

A discretionary release to one requester may preclude the withholding of the same record under a FOIA exemption if the record is subsequently requested by someone else. In applying exemptions, the identity of the requester and the purpose for which the record is sought are irrelevant with the exception that an exemption may not be invoked where the particular interest to be protected is the requester's interest.

The following is an explanation of and the uses of the nine FOIA exemptions from DoD 5400.7-R, DoD Freedom of Information Act Program. These rules of usage should be followed by the Agency personnel when processing FOIA requests.

Exemption 1 - Classified Information

Those properly and currently classified in the interest of national defense or foreign policy, as specifically authorized under the criteria established by Executive Order and implemented by regulations. Although material is not classified at the time of the FOIA request, a classification review may be undertaken to determine whether the information should be classified. If the information qualifies as Exemption 1 information, there is **no discretion** regarding its release. In addition, this exemption shall be invoked when the following situations are apparent:

The fact of the existence or nonexistence of a record would itself reveal classified information. In this situation, Components shall neither confirm nor deny the existence or nonexistence of the record being requested. A "refusal to confirm or deny" response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no record" response when a record does not exist, and a "refusal to confirm or deny" when a record does exist will itself disclose national security information.

Compilations of items of information that are individually unclassified may be classified if the compiled information reveals additional association or relationship that meets the standard for classification under an existing executive order for classification and is not otherwise revealed in the individual items of information.

Exemption 2 - Internal Rules and Practices

Those related solely to the internal personnel rules and practices of the Department of Defense or any of its Components. This exemption is **entirely discretionary**. This exemption has two profiles, **high (b)(2) and low (b)(2)**. When only a minimum Government interest would be affected (administrative burden), there is a great potential for discretionary disclosure of the information. Consequently, DoD Components **shall not invoke** the low (b)(2) profile.

Records qualifying under high (b)(2) are those containing or constituting statutes, rules, regulations, orders, manuals, directives, instructions, and security classification guides, the release of which would allow circumvention of these records thereby substantially hindering the effective performance of a significant function of the Department of Defense. Examples include:

Those operating rules, guidelines, and manuals for DoD investigators, inspectors, auditors, or examiners that must remain privileged in order for the DoD Component to fulfill a legal requirement.

Personnel and other administrative matters, such as examination questions and answers used in training courses or in the determination of the qualifications of candidates for employment, entrance on duty, advancement, or promotion.

Computer software, the release of which would allow circumvention of a statute or DoD rules, Regulations, orders, Manuals, Directives, or Instructions. In this situation, the **use** of the software must be closely examined to ensure a circumvention possibility exists.

Records qualifying under the low (b)(2) profile are those that are trivial and housekeeping in nature for which there is no legitimate public interest or benefit to be gained by release, and it would constitute an administrative burden to process the request in order to disclose the records. Examples include rules of personnel's use of parking facilities or regulation of lunch hours, statements of policy as to sick leave, and administrative data such as file numbers, mail routing stamps, initials, data processing notations, brief references to previous communications, and other like administrative markings. **DoD Components shall not invoke the low (b)(2) profile.**

Exemption 3 - Information Exempted by Statute

Those concerning matters that a statute specifically exempts from disclosure by terms that permit **no discretion** on the issue, or in accordance with criteria established by that statute for withholding or referring to particular types of matters to be withheld. The Directorate for Freedom of Information and Security Review maintains a list of (b)(3) statutes used within the Department of Defense, and provides updated lists of these statutes to DoD Components on a periodic basis.

Exemption 4 - Proprietary Information

Those containing trade secrets or commercial or financial information that a DoD Component receives from a person or organization outside the Government with the understanding that the information or record will be retained on a privileged or confidential basis in accordance with the customary handling of such records. Records within the exemption must contain trade secrets, or commercial or financial records, the disclosure of which is likely to cause substantial harm to the competitive position of the source providing the information; impair the Government's ability to obtain necessary information in the future; or impair some other legitimate Government interest. Commercial or financial information submitted on a voluntary basis, absent any exercised authority prescribing criteria for submission is protected without any

requirement to show competitive harm. If the information qualifies as Exemption 4 information, there is **no discretion** in its release. Examples include:

Commercial or financial information received in confidence in connection with loans, bids, contracts, or proposals set forth in or incorporated by reference in a contract entered into between the DoD Component and the offeror that submitted the proposal, as well as other information received in confidence or privileged, such as trade secrets, inventions, discoveries, or other proprietary data.

Statistical data and commercial or financial information concerning contract performance, income, profits, losses, and expenditures, if offered and received in confidence from a contractor or potential contractor.

Personal statements given in the course of inspections, investigations, or audits, when such statements are received in confidence from the individual and retained in confidence because they reveal trade secrets or commercial or financial information normally considered confidential or privileged.

Financial data provided in confidence by private employers in connection with locality wage surveys that are used to fix and adjust pay schedules applicable to the prevailing wage rate of employees within the Department of Defense.

Scientific and manufacturing processes or developments concerning technical or scientific data or other information submitted with an application for a research grant, or with a report while research is in progress.

Technical or scientific data developed by a contractor or subcontractor exclusively at private expense, and technical or scientific data developed in part with Federal funds and in part at private expense, wherein the contractor or subcontractor has retained legitimate proprietary interests in such data in accordance with 10 U.S.C. 2320-2321 and DoD Federal Acquisition Regulation Supplement (DFARS), Chapter 2 of 48 C.F.R., Subpart 227.71-227.72

Computer software which is copyrighted under the Copyright Act of 1976 (17 U.S.C. 106), the disclosure of which would have an adverse impact on the potential market value of a copyrighted work.

Proprietary information submitted strictly on a **voluntary** basis, absent any exercised authority prescribing criteria for submission. Examples of exercised authorities prescribing criteria for submission are statutes, Executive Orders, regulations, invitations for bids, requests for proposals, and contracts. Submission of information under these authorities **is not voluntary**.

Exemption 5 - Predecisional Information

Those containing information considered privileged in litigation, primarily under the deliberative process privilege. Internal advice, recommendations, and subjective evaluations, as contrasted with factual matters, that are reflected in deliberative records pertaining to the

decision-making process of an Agency, whether within or among Agencies (as defined in 5 U.S.C. 552(e) (reference (a))), or within or among DoD Components. In order to meet the test of this exemption, the record must be both deliberative in nature, as well as part of a decision-making process. Merely being an internal record is insufficient basis for withholding under this exemption. Also potentially exempted are records pertaining to the attorney-client privilege and the attorney work-product privilege. This exemption is **entirely discretionary**.

Examples of the deliberative process include:

The non-factual portions of staff papers, to include after-action reports, lessons learned, and situation reports containing staff evaluations, advice, opinions, or suggestions.

Advice, suggestions, or evaluations prepared on behalf of the Department of Defense by individual consultants or by boards, committees, councils, groups, panels, conferences, commissions, task forces, or other similar groups that are formed for the purpose of obtaining advice and recommendations.

Those non-factual portions of evaluations by DoD Component personnel of contractors and their products.

Information of a speculative, tentative, or evaluative nature or such matters as proposed plans to procure, lease or otherwise acquire and dispose of materials, real estate, facilities or functions, when such information would provide undue or unfair competitive advantage to private personal interests or would impede legitimate Government functions.

Trade secret or other confidential research development, or commercial information owned by the Government, where premature release is likely to affect the Government's negotiating position or other commercial interest.

Those portions of official reports of inspection, reports of the Inspector Generals, audits, investigations, or surveys pertaining to safety, security, or the internal management, administration, or operation of one or more DoD Components, when these records have traditionally been treated by the courts as privileged against disclosure in litigation.

Planning, programming, and budgetary information that is involved in the defense planning and resource allocation process.

If any such intra- or inter-agency record or reasonably segregable portion of such record hypothetically would be made available routinely through the discovery process in the course of litigation with the Agency, then it should not be withheld under the FOIA. If, however, the information hypothetically would not be released at all, or would only be released in a particular case during civil discovery where a party's particularized showing of need might override a privilege, then the record may be withheld. Discovery is the formal process by which litigants obtain information from each other for use in the litigation. Consult with legal counsel to determine whether Exemption 5 material would be routinely made available through the discovery process.

Intra- or inter-agency memoranda or letters that are factual, or those reasonably segregable portions that are factual, are routinely made available through discovery, and shall be made available to a requester, unless the factual material is otherwise exempt from release, inextricably intertwined with the exempt information, so fragmented as to be uninformative, or so redundant of information already available to the requester as to provide no new substantive information.

A direction or order from a superior to a subordinate, though contained in an internal communication, generally cannot be withheld from a requester if it constitutes policy guidance or a decision, as distinguished from a discussion of preliminary matters or a request for information or advice that would compromise the decision-making process.

An internal communication concerning a decision that subsequently has been made a matter of public record must be made available to a requester when the rationale for the decision is expressly adopted or incorporated by reference in the record containing the decision.

Exemption 6 - Personal Privacy Information

Information in personnel and medical files, as well as similar personal information in other files, that, if disclosed to a requester, other than the person about whom the information is about, would result in a clearly unwarranted invasion of personal privacy. Release of information about an individual contained in a Privacy Act System of records that would constitute a clearly unwarranted invasion of privacy is prohibited, and could subject the releaser to civil and criminal penalties. If the information qualifies as Exemption 6 information, there is **no discretion** in its release.

Examples of other files containing personal information similar to that contained in personnel and medical files include:

Those compiled to evaluate or adjudicate the suitability of candidates for civilian employment or membership in the Armed Forces, and the eligibility of individuals (civilian, military, or contractor employees) for security clearances, or for access to particularly sensitive classified information.

Files containing reports, records, and other material pertaining to personnel matters in which administrative action, including disciplinary action, may be taken.

Home addresses, *including private e-mail addresses*, are normally not releasable without the consent of the individuals concerned. This includes lists of home addressees and military quarters' addressees without the occupant's name. *Additionally, the names and duty addresses (postal and/or e-mail) of DoD military and civilian personnel who are assigned to units that are sensitive, routinely deployable, or stationed in foreign territories can constitute a clearly unwarranted invasion of personal privacy.*

Privacy Interest. A privacy interest may exist in personal information even though the information has been disclosed at some place and time. If personal information is not freely available from sources other than the Federal Government, a privacy interest exists in its nondisclosure. The fact that the Federal Government expended funds to prepare, index and maintain records on personal information, and the fact that a requester invokes FOIA to obtain these records indicates the information is not freely available.

Names and duty addresses (*postal and/or e-mail*) published in telephone directories, organizational charts, rosters and similar materials for personnel assigned to units that are sensitive, routinely deployable, or stationed in foreign territories are withholdable under this exemption.

This exemption shall not be used in an attempt to protect the privacy of a deceased person, but it may be used to protect the privacy of the deceased person's family if disclosure would rekindle grief, anguish, pain, embarrassment, or even disruption of peace of mind of surviving family members. In such situations, balance the surviving family members' privacy against the public's right to know to determine if disclosure is in the public interest. Additionally, the deceased's social security number should be withheld since it is used by the next of kin to receive benefits. Disclosures may be made to the immediate next of kin.

A clearly unwarranted invasion of the privacy of third parties identified in a personnel, medical or similar record constitutes a basis for deleting those reasonably segregable portions of that record. When withholding third party personal information from the subject of the record and the record is contained in a Privacy Act system of records, consult with legal counsel.

This exemption also applies when the fact of the existence or nonexistence of a responsive record would itself reveal personally private information, and the public interest in disclosure is not sufficient to outweigh the privacy interest. In this situation, DoD Components shall neither confirm nor deny the existence or nonexistence of the record being requested. This is a Glomar response, and Exemption 6 must be cited in the response. Additionally, in order to insure personal privacy is not violated during referrals, DoD Components shall coordinate with other DoD Components or Federal Agencies **before** referring a record that is exempt under the Glomar concept.

A "refusal to confirm or deny" response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no records" response when a record does not exist and a "refusal to confirm or deny" when a record does exist will itself disclose personally private information.

Refusal to confirm or deny should not be used when (a) the person whose personal privacy is in jeopardy has provided the requester a waiver of his or her privacy rights; (b) the person initiated or directly participated in an investigation that lead to the creation of an Agency record seeks access to that record; or (c) the person whose personal privacy is in jeopardy is deceased, the Agency is aware of that fact, and disclosure would not invade the privacy of the deceased's family.

Exemption 7 - Investigatory Records

Records or information compiled for law enforcement purposes; i.e., civil, criminal, or military law, including the implementation of Executive Orders or regulations issued pursuant to law. This exemption may be invoked to prevent disclosure of documents not originally created for, but later gathered for law enforcement purposes. **With the exception of parts (C) and (F) of this exemption, this exemption is discretionary.** If information qualifies as exemption (7)(C) or (7)(F) information, there is **no discretion** in its release.

This exemption applies, however, only to the extent that production of such law enforcement records or information could result in the following:

Could reasonably be expected to interfere with enforcement proceedings (5 U.S.C. 552(b)(7)(A)).

Would deprive a person of the right to a fair trial or to an impartial adjudication (5 U.S.C. 552(b)(7)(B)).

Could reasonably be expected to constitute an unwarranted invasion of personal privacy of a living person, including surviving family members of an individual identified in such a record (5 U.S.C. 552(b)(7)(C)).

This exemption also applies when the fact of the existence or nonexistence of a responsive record would itself reveal personally private information, and the public interest in disclosure is not sufficient to outweigh the privacy interest. In this situation, Components shall neither confirm nor deny the existence or nonexistence of the record being requested. This is a Glomar response, and Exemption (7)(C) must be cited in the response. Additionally, in order to insure personal privacy is not violated during referrals, DoD Components shall coordinate with other DoD Components or Federal Agencies **before** referring a record that is exempt under the Glomar concept.

A "refusal to confirm or deny" response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no records" response when a record does not exist and a "refusal to confirm or deny" when a record does exist will itself disclose personally private information.

Refusal to confirm or deny should not be used when 1) the person whose personal privacy is in jeopardy has provided the requester with a waiver of his or her privacy rights; or 2) the person whose personal privacy is in jeopardy is deceased, and the Agency is aware of that fact.

Could reasonably be expected to disclose the identity of a confidential source, including a source within the Department of Defense; a State, local, or foreign agency or authority; or any private institution that furnishes the information on a confidential basis; and could disclose information furnished from a confidential source and obtained by a criminal law enforcement

authority in a criminal investigation or by an Agency conducting a lawful national security intelligence investigation (5 U.S.C. 552(b)(7)(D)).

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 (5 U.S.C. 552(b)(7)(E)).

Could reasonably be expected to endanger the life or physical safety of any individual (5 U.S.C. 552(b)(7)(F)).

Some examples of Exemption 7 are:

Statements of witnesses and other material developed during the course of the investigation and all materials prepared in connection with related Government litigation or adjudicative proceedings.

The identity of firms or individuals being investigated for alleged irregularities involving contracting with the Department of Defense when no indictment has been obtained nor any civil action filed against them by the United States.

Information obtained in confidence, expressed or implied, in the course of a criminal investigation by a criminal law enforcement Agency or office within a DoD Component, or a lawful national security intelligence investigation conducted by an authorized Agency or office within a DoD Component. National security intelligence investigations include background security investigations and those investigations conducted for the purpose of obtaining affirmative or counterintelligence information.

The right of individual litigants to investigative records currently available by law is not diminished.

Exclusions. Excluded from the above exemption are the below two situations applicable to the Department of Defense.

Whenever a request is made that involves access to records or information compiled for law enforcement purposes, and the investigation or proceeding involves a possible violation of criminal law where there is reason to believe that the subject of the investigation or proceeding is unaware of its pendency, and the disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, Components may, during only such times as that circumstance continues, treat the records or information as not subject to the FOIA. In such situation, the response to the requester will state that no records were found.

Whenever informant records maintained by a criminal law enforcement organization within a DoD Component under the informant's name or personal identifier are requested by a third party using the informant's name or personal identifier, the Component may treat the records as not subject to the FOIA, unless the informant's status as an informant has been

officially confirmed. If it is determined that the records are not subject to 5 U.S.C. 552(b)(7), the response to the requester will state that no records were found.

Exemption 8 - Records of Financial Institutions Highlights

Those contained in or related to examination, operation or condition reports prepared by, on behalf of, or for the use of any Agency responsible for the regulation or supervision of financial institutions.

Exemption 9 - Oil and Gas Well Data

Those containing geological and geophysical information and data (including maps) concerning wells.

CHAPTER 7 - HOW ARE FEES ASSESSED FOR FOIA SEARCHES?

The following is an explanation of FOIA fees, waivers and requester classification from DoD 5400.7-R, DoD Freedom of Information Act Program. These rules of usage should be followed by the Agency personnel when determining FOIA requester classification and the application of possible FOIA fees.

Collection of fees will be made at the time of providing the documents to the requester or recipient when the requester specifically states that the costs involved shall be acceptable or acceptable up to a specified limit that covers the anticipated costs. Collection of fees may not be made in advance unless the requester has failed to pay previously assessed fees within 30 calendar days from the date of the billing by DCAA, or the Agency has determined that the fee will be in excess of \$250.

Search Time.

Manual Search.

Type Grade Hourly Rate (\$)
Clerical E9/GS8 and below 20
Professional O1-O6/GS9-GS15 44
Executive O7/GS16/ES1 and above 75

Computer Search. Fee assessments for computer search consists of two parts; individual time (hereafter referred to as human time), and machine time.

Human time. Human time is all the time spent by humans performing the necessary tasks to prepare the job for a machine to execute the run command. If execution of a run requires monitoring by a human, that human time may be also assessed as computer search. The terms “programmer/operator” shall not be limited to the traditional programmers or operators. Rather, the terms shall be interpreted in their broadest sense to incorporate any human involved in performing the computer job (e.g. technician, administrative support, operator, programmer, database administrator, or action officer).

Machine time. Machine time involves only direct costs of the Central Processing Unit (CPU), input/output devices, and memory capacity used in the actual computer configuration. Only this CPU rate shall be charged. No other machine related costs shall be charged. In situations where the capability does not exist to calculate CPU time, no machine costs can be passed on to the requester. When CPU calculations are not available, only human time costs shall be assessed to requesters.

Duplication.

Type Cost per Page (cents)
Pre-Printed material 02

Office copy 15
Computer copies (tapes,
discs or printouts)
Actual cost of duplicating the tape, disc or printout
(includes operator's time and cost of the medium)

Review Time (in the case of commercial requesters).

Type Grade Hourly Rate (\$)
Clerical E9/GS8 and below 20
Professional O1-O6/GS9-GS15 44
Executive O7/GS16/ES1 and above 75

Audiovisual Documentary Materials. Search costs are computed as for any other record. Duplication cost is the actual direct cost of reproducing the material, including the wage of the person doing the work. Audiovisual materials provided to a requester need not be in reproducible format or quality.

Other Records. Direct search and duplication cost for any record not described in this section shall be computed in the manner described for audiovisual documentary material.

FEE WAIVERS

Documents shall be furnished without charge, or at a charge reduced below fees assessed to the categories of requesters, when the Agency determines that waiver or reduction of the fees is in the public interest because furnishing the information is likely to contribute significantly to public understanding of the operations or activities of DCAA and is not primarily in the commercial interest of the requester.

When assessable costs for a FOIA request total \$15.00 or less, fees shall be waived automatically for all requesters, regardless of category.

Decisions to waive or reduce fees that exceed the automatic waiver threshold shall be made on a case-by-case basis, consistent with the following factors:

Disclosure of the information "is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the Government."

The subject of the request. The Agency should analyze whether the subject matter of the request involves issues that will significantly contribute to the public understanding of the operations or activities of the DCAA. Requests for records in the possession of the DCAA which were originated by non-government organizations and are sought for their intrinsic content, rather than informative value, will likely not contribute to public understanding of the operations or activities of the DCAA. An example of such records might be press clippings, magazine articles, or records forwarding a particular opinion or concern from a member of the

public regarding a DCAA activity. Similarly, disclosures of records of considerable age may or may not bear directly on the current activities of the DCAA; however, the age of a particular record shall not be the sole criteria for denying relative significance under this factor. It is possible to envisage an informative issue concerning the current activities of the Agency, based upon historical documentation. Requests of this nature must be closely reviewed consistent with the requester's stated purpose for desiring the records and the potential for public understanding of the operations and activities of the DCAA.

The informative value of the information to be disclosed. This factor requires a close analysis of the substantive contents of a record, or portion of the record, to determine whether disclosure is meaningful, and shall inform the public on the operations or activities of the Agency. While the subject of a request may contain information that concerns operations or activities of the Agency, it may not always hold great potential for contributing to a meaningful understanding of these operations or activities. An example of such would be a previously released record that has been heavily redacted, the balance of which may contain only random words, fragmented sentences, or paragraph headings. A determination as to whether a record in this situation will contribute to the public understanding of the operations or activities of the Agency must be approached with caution, and carefully weighed against the arguments offered by the requester. Another example is information already known to be in the public domain. Disclosure of duplicative, or nearly identical information already existing in the public domain may add no meaningful new information concerning the operations and activities of the Agency.

The contribution to an understanding of the subject by the general public likely to result from disclosure. The key element in determining the applicability of this factor is whether disclosure will inform, or have the potential to inform the public, rather than simply the individual requester or small segment of interested persons. The identity of the requester is essential in this situation in order to determine whether such requester has the capability and intention to disseminate the information to the public. Mere assertions of plans to author a book, researching a particular subject, doing doctoral dissertation work, or indigence are insufficient without demonstrating the capacity to further disclose the information in a manner that will be informative to the general public. Requesters should be asked to describe their qualifications, the nature of their research, the purpose of the requested information, and their intended means of dissemination to the public.

The significance of the contribution to public understanding. In applying this factor, the Agency must differentiate the relative significance or impact of the disclosure against the current level of public knowledge, or understanding which exists before the disclosure. In other words, will disclosure on a current subject of wide public interest be unique in contributing previously unknown facts, thereby enhancing public knowledge, or will it basically duplicate what is already known by the general public? A decision regarding significance requires objective judgment, rather than subjective determination, and must be applied carefully to determine whether disclosure will likely lead to a significant public understanding of the issue. The Agency shall not make value judgments as to whether the information is important enough to be made public.

Disclosure of the information "is not primarily in the commercial interest of the requester."

The existence and magnitude of a commercial interest. If the request is determined to be of a commercial interest, the Agency should address the magnitude of that interest to determine if the requester's commercial interest is primary, as opposed to any secondary personal or non-commercial interest. In addition to profit-making organizations, individual persons or other organizations may have a commercial interest in obtaining certain records. Where it is difficult to determine whether the requester is of a commercial nature, the Agency may draw inference from the requester's identity and circumstances of the request. The Agency is reminded that in order to apply the commercial standards of the FOIA, the requester's commercial benefit must clearly override any personal or non-profit interest.

The primary interest in disclosure. Once a requester's commercial interest has been determined, the Agency should then determine if this disclosure would be primarily in that interest. This requires a balancing test between the commercial interest of the request against any public benefit to be derived as a result of that disclosure. Where the public interest is served above and beyond that of the requester's commercial interest, a waiver or reduction of fees would be appropriate. Conversely, even if a significant public interest exists, and the relative commercial interest of the requester is determined to be greater than the public interest, then a waiver or reduction of fees would be inappropriate. As examples, news media organizations have a commercial interest as business organizations; however, their inherent role of disseminating news to the general public can ordinarily be presumed to be of a primary interest. Therefore, any commercial interest becomes secondary to the primary interest in serving the public. Similarly, scholars writing books or engaged in other forms of academic research, may recognize a commercial benefit, either directly, or indirectly (through the institution they represent); however, normally such pursuits are primarily undertaken for educational purposes, and the application of a fee charge would be inappropriate. Conversely, data brokers or others who merely compile Government information for marketing can normally be presumed to have an interest primarily of a commercial nature. The Agency is reminded that the factors and examples used are not all inclusive. Each fee decision must be considered on a case-by-case basis and upon the merits of the information provided in each request. When the element of doubt as to whether to charge or waive the fee cannot be clearly resolved, the Agency should rule in favor of the requester.

In addition, the following additional circumstances describe situations where waiver or reduction of fees are most likely to be warranted:

A record is voluntarily created to prevent an otherwise burdensome effort to provide voluminous amounts of available records, including additional information not requested.

A previous denial of records is reversed in total, or in part, and the assessable costs are not substantial (e.g. \$15.00 - \$30.00).

FEE ASSESSMENT

Fees may not be used to discourage requesters, and to this end, FOIA fees are limited to standard charges for direct document search, review (in the case of commercial requesters) and duplication.

In order to be as responsive as possible to FOIA requests while minimizing unwarranted costs to the taxpayer, the Agency shall adhere to the following procedures:

Analyze each request to determine the category of the requester. If the Agency determination regarding the category of the requester is different than that claimed by the requester, the Agency shall:

Notify the requester to provide additional justification to warrant the category claimed, and that a search for responsive records will not be initiated until agreement has been attained relative to the category of the requester. Absent further category justification from the requester, and within a reasonable period of time (i.e., 30 calendar days), the Agency shall render a final category determination, and notify the requester of such determination, to include normal administrative appeal rights of the determination.

Advise the requester that, notwithstanding any appeal, a search for responsive records will not be initiated until the requester indicates a willingness to pay assessable costs appropriate for the category determined by the Agency.

Requesters should submit a fee declaration appropriate for the below categories.

Commercial. Requesters should indicate a willingness to pay all search, review and duplication costs.

Educational or Noncommercial Scientific Institution or News Media. Requesters should indicate a willingness to pay duplication charges in excess of 100 pages if more than 100 pages of records are desired.

Requesters should indicate a willingness to pay assessable search and duplication costs if more than two hours of search effort or 100 pages of records are desired.

If the above conditions are not met, then the request need not be processed and the requester shall be so informed.

The Agency must be prepared to provide an estimate of assessable fees if desired by the requester. While it is recognized that search situations will vary, and that an estimate is often difficult to obtain prior to an actual search, requesters who desire estimates are entitled to such before committing to a willingness to pay. Should DCAA's actual costs exceed the amount of the estimate or the amount agreed to by the requester, the amount in excess of the estimate or the requester's agreed amount shall not be charged without the requester's agreement.

No DoD Component may require advance payment of any fee; i.e., payment before work is commenced or continued on a request, unless the requester has previously failed to pay fees in a timely fashion, or the Agency has determined that the fee will exceed \$250.00. As used in this sense, a timely fashion is 30 calendar days from the date of billing (the fees have been assessed in writing) by the Agency.

Whereas the Agency estimates or determines that allowable charges that a requester may be required to pay are likely to exceed \$250.00, the Agency shall notify the requester of the likely cost and obtain satisfactory assurance of full payment where the requester has a history of prompt payments, or require an advance payment of an amount up to the full estimated charges in the case of requesters with no history of payment.

Where a requester has previously failed to pay a fee charged in a timely fashion (i.e., within 30 calendar days from the date of the billing), the Agency may require the requester to pay the full amount owed, plus any applicable interest, or demonstrate that he or she has paid the fee, and to make an advance payment of the full amount of the estimated fee before the Agency begins to process a new or pending request from the requester. Interest will be at the rate prescribed in 31 U.S.C. 3717, and confirmed with respective Finance and Accounting Offices.

After all work is completed on a request, and the documents are ready for release, the Agency may request payment before forwarding the documents, particularly for those requesters who have no payment history, or for those requesters who have failed previously to pay a fee in a timely fashion (i.e., within 30 calendar days from the date of the billing).

The administrative time limits of the FOIA will begin only after the Agency has received a willingness to pay fees and satisfaction as to category determination, or fee payments (if appropriate).

The Agency may charge for time spent searching for records, even if that search fails to locate records responsive to the request. The Agency may also charge search and review (in the case of commercial requesters) time if records located are determined to be exempt from disclosure. In practice, if the Agency estimates that search charges are likely to exceed \$25.00, we shall notify the requester of the estimated amount of fees, unless the requester has indicated in advance his or her willingness to pay fees as high as those anticipated. Such a notice shall offer the requester the opportunity to confer with Agency personnel with the object of reformulating the request to meet his or her needs at a lower cost.

Commercial Requesters. Fees shall be limited to reasonable standard charges for document search, review and duplication when records are requested for commercial use. Requesters must reasonably describe the records sought.

The term "commercial use" request refers to a request from, or on behalf of one who seeks information for a use or purpose that furthers the commercial, trade, or profit interest of the requester or the person on whose behalf the request is made. In determining whether a requester properly belongs in this category, the Agency must determine the use to which a requester will put the documents requested. Moreover, when the Agency has reasonable cause to doubt the use

to which a requester will put the records sought, or where that use is not clear from the request itself, the Agency should seek additional clarification before assigning the request to a specific category.

When the Agency receives a request for documents for commercial use, we should assess charges which shall recover the full direct costs of searching for, reviewing for release, and duplicating the records sought. Commercial requesters (unlike other requesters) are not entitled to two hours of free search time, nor 100 free pages of reproduction of documents. Moreover, commercial requesters are not normally entitled to a waiver or reduction of fees based upon an assertion that disclosure would be in the public interest. However, because use is the exclusive determining criteria, it is possible to envision a commercial enterprise making a request that is not for commercial use. It is also possible that a non-profit organization could make a request that is for commercial use. Such situations must be addressed on a case-by-case basis.

Educational Institution Requesters. Fees shall be limited to only reasonable standard charges for document duplication (excluding charges for the first 100 pages) when the request is made by an educational institution whose purpose is scholarly research. Requesters must reasonably describe the records sought. The term "educational institution" refers to a pre-school, a public or private elementary or secondary school, an institution of graduate high education, an institution of undergraduate higher education, an institution of professional education, and an institution of vocational education, which operates a program or programs of scholarly research. Fees shall be waived or reduced in the public interest if the criteria have been met.

Non-Commercial Scientific Institution Requesters. Fees shall be limited to only reasonable standard charges for document duplication (excluding charges for the first 100 pages) when the request is made by a non-commercial scientific institution whose purpose is scientific research. Requesters must reasonably describe the records sought. The term "non-commercial scientific institution" refers to an institution that is not operated on a "commercial" basis, and that is operated solely for the purpose of conducting scientific research, the results of which are not intended to promote any particular product or industry. Fees shall be waived or reduced in the public interest if the criteria, have been met.

DCAA shall provide documents to these requesters for the cost of duplication alone, excluding charges for the first 100 pages. To be eligible for inclusion in these categories, requesters must show that the request is being made under the auspices of a qualifying institution and that the records are not sought for commercial use, but in furtherance of scholarly (from an educational institution) or scientific (from a non-commercial scientific institution) research.

Representatives of the news media. Fees shall be limited to only reasonable standard charges for document duplication (excluding charges for the first 100 pages) when the request is made by a representative of the news media. Requesters must reasonably describe the records sought. Fees shall be waived or reduced if the criteria has been met.

The term "representative of the news media" refers to any person actively gathering news for an entity that is organized and operated to publish or broadcast news to the public. The term "news" means information that is about current events or that would be of current interest to the

public. Examples of news media entities include television or radio stations broadcasting to the public at large, and publishers of periodicals (but only in those instances when they can qualify as disseminators of "news") who make their products available for purchase or subscription by the general public. These examples are not meant to be all-inclusive. Moreover, as traditional methods of news delivery evolve (e.g., electronic dissemination of newspapers through telecommunications services), such alternative media would be included in this category. In the case of "freelance" journalists, they may be regarded as working for a news organization if they can demonstrate a solid basis for expecting publication through that organization, even though not actually employed by it. A publication contract would be the clearest proof, but the Agency may also look to the past publication record of a requester in making this determination.

To be eligible for inclusion in this category, a requester must meet the criteria listed above, and his or her request must not be made for commercial use. A request for records supporting the news dissemination function of the requester shall not be considered to be a request that is for a commercial use. For example, a document request by a newspaper for records relating to the investigation of a defendant in a current criminal trial of public interest could be presumed to be a request from an entity eligible for inclusion in this category, and entitled to records at the cost of reproduction alone (excluding charges for the first 100 pages).

"Representative of the news media" does not include private libraries, private repositories of Government records, information vendors, data brokers *or similar marketers of information whether to industries and businesses, or other entities.*

All Other Requesters. The Agency shall charge requesters who do not fit into any of the categories described above, fees which recover the full direct cost of searching for and duplicating records, except that the first two hours of search time and the first 100 pages of duplication shall be furnished without charge. Requesters must reasonably describe the records sought. Requests from subjects about themselves will continue to be treated under the fee provisions of the Privacy Act of 1974, which permit fees only for duplication.

Aggregating Requests. Except for requests that are for a commercial use, the Agency may not charge for the first two hours of search time or for the first 100 pages of reproduction. However, a requester may not file multiple requests at the same time, each seeking portions of a document or documents, solely in order to avoid payment of fees. If DCAA reasonably believes that a requester or, on rare occasions, a group of requesters acting in concert, is attempting to break a request down into a series of requests for the purpose of avoiding the assessment of fees, the Agency may aggregate any such requests and charge accordingly. One element to be considered in determining whether a belief would be reasonable is the time period in which the requests have occurred. For example, it would be reasonable to presume that multiple requests of this type made within a 30 day period had been made to avoid fees. For requests made over a longer period however, such a presumption becomes harder to sustain and the Agency should have a solid basis for determining that aggregation is warranted in such cases. The Agency is cautioned that before aggregating requests from more than one requester, we must have a concrete basis on

which to conclude that the requesters are acting in concert and are acting specifically to avoid payment of fees. In no case may the Agency aggregate multiple requests on unrelated subjects from one requester.

CHAPTER 8 – THE PRIVACY ACT AND FOIA

The Privacy Act of 1974

Highlights

The FOIA applies to all Agency records. The Privacy Act applies only to records about individuals maintained in Privacy Act systems of records.

A person may request records about himself or herself under either the FOIA or Privacy Act, or both. DCAA will normally give the person as much information as would be available under either Act.

DCAA has systems of records, such as personnel records, security files, which contain personal information.

DCAA is required by the Privacy Act to maintain only such information about employees as is necessary and relevant for an Agency purpose. It is also required to assure that its records about individuals are as accurate, relevant, timely, and complete as necessary to assure fairness.

How Do the FOIA and Privacy Acts Differ?

Under FOIA, a person may obtain access to any Government record, including records about himself or herself, unless the records fall within one of the nine exemptions to the Act. The Privacy Act, on the other hand, is limited only to records about individuals which are maintained in a "system of records" from which information is retrieved by his or her name or other personal identifier. If the records are not maintained by the Agency in a "system of records," the Privacy Act does not apply, and the person would have to seek access to the information under the provisions of the FOIA.

A difficult question arises when access to information in one person's file would affect the personal privacy of another person. For example, one court refused to give the address of minor children to an unmarried father who was paying child support, but who did not have visitation rights, even though the addresses were listed in the father's social security account. Similarly, it is doubtful if DCAA would make available to an employee derogatory information about his or her spouse that is contained in the employee's security file. Courts reason, in these cases, that the information does not pertain to the individual. Of course, if information is misfiled or placed in a person's file by accident, it may clearly be withheld.

What is a System of Records?

A system of records is a group of records under the control of an Agency from which information is retrieved by the name of the individual or by some other identifying particular assigned to the individual, such as a social security number, badge number, fingerprint, or voice print. To be considered a system of records, it is not enough that the records are retrievable by reference to an individual's name if the records are not normally accessed in that manner. Thus,

a reading file, chronological file, or any other grouping of records that is not normally accessed by a person's name, even if it is possible to locate a record about an individual by manually searching the file, is not a system of records under the Privacy Act.

Each agency is required to identify and publish its systems of records in the Federal Register, and no new system of records may be established without the Agency first notifying Congress and OMB, and announcing the system in the Federal Register.

How Does the Privacy Act Control Access to Agency Records?

Like the FOIA, the Privacy Act has certain exemptions to its access provisions. Section 552a(k) of the Act provides that the Agency may promulgate rules exempting any system of records from the access and certain other provisions of the Act if the records are:

1. Classified
2. Investigatory material compiled for law enforcement purposes
3. Maintained in connection with providing protective services to the President
4. Required by statute to be maintained and used solely as statistical records
5. Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information,
6. Testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal service, the disclosure of which would compromise the objectivity or fairness of the testing or examination process, or
7. Evaluation material used to determine potential for promotion in the armed services.

Are Personal Records under the FOIA and the Privacy Act the Same?

With regard to the distinction under the FOIA between "agency records" which are subject to the FOIA and "personal records" which are not subject to the FOIA, it should be noted that personal records under the Privacy Act have the same meaning as under the FOIA (see discussion in Chapter 2). Thus, personal records would not normally be available if requested under the Privacy Act.

"Personal Records" [are], uncirculated personal notes, papers and records which are retained or discarded at the author's sole discretion and over which the DCAA exercises no control or dominion. However, if a "personal record" is shown or transmitted to any other individual, it becomes an Agency record subject to the requirements of the Privacy Act. Furthermore, if "personal records" are maintained in the same file as, or

commingled with Agency records, there is a presumption that they are Agency records also.

(Note: In a 1986 case, the court held that memos which were kept in a supervisor's desk along with official personnel records and which were left behind when the supervisor was assigned to another base were agency records and not personal records).

How Much Information about Individuals can Agencies Collect?

Agencies are required to maintain only such information about employees as is relevant and necessary to accomplish an Agency purpose. To the extent possible, agencies are also required to collect information directly from the individuals involved and, if an Agency form is used to solicit personal information, to provide a Privacy Act Statement. A Privacy Act Statement informs the individual furnishing the information as to the reasons for requesting the information, the authority which authorizes the solicitation of the information, whether disclosure is mandatory or voluntary, how it will be used, and what the consequences are, if any, of not providing the information.

Agencies are also required to maintain their records concerning any individual with such accuracy, relevance, timeliness and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, opportunities, or benefits due to the individual.

When can Agencies Permit Access to Personal Information?

The general rule in the Privacy Act is that no Agency shall disclose any record which is contained in a system of records to any person except in response to a written request by, or with the prior written consent of, the individual to whom the record pertains. The Act has 12 exceptions, the first three of which are utilized most frequently by agencies. Records may be disclosed:

to those officers and employees of the agency who have a need for the records in the performance of their official duties,
if required pursuant to the FOIA and,

for any "routine use."

A "routine use" is defined as "any use of a record which is compatible with the purpose for which the record was collected."

CHAPTER 9 – THE FOIA AND CONGRESSIONAL REQUESTS

Freedom of Information Act Prohibition on Withholding Information from Congress - Transmittal of Sensitive Documents to Congress

Highlights

The FOIA specifically provides that the Act may not be used to withhold information from Congress.

Where records requested by Congress are exempt under the FOIA, Congress is notified of that fact and requested to maintain the records in confidence.

All Congressional requests for records should be referred to the Headquarters, Policy and Plans Directorate, Auditing Standards Division (PAS).

DCAA provides documents to Congress not available to the general public only when requested by a committee or subcommittee chairman or ranking minority member which has jurisdiction over DCAA. The Agency is not required to provide documents to committees or subcommittees who do not have jurisdiction over DCAA.

Can the FOIA be Used to Withhold Information from Congress?

Section 552(d) of the FOIA specifically provides that "this section is not an authority to withhold information from Congress." The only way information can be formally withheld from Congress is through a claim of Executive Privilege.

Members of Congress, Members of Congressional Committees, and their staffs often request copies of classified and unclassified sensitive documents. Procedures have been established by the PAS to assure that these Congressional requests are treated uniformly and responded to promptly.

Appendix A - The Freedom of Information Act, 5 U.S.C. § 552 and Code of Federal Regulations, 32 CFR Part 290

1. The Freedom of Information Act, 5 U.S.C. § 552 is available from the Department of Justice's web site at <http://www.justice.gov/oip/amended-foia-relinded-2010.pdf>
2. The DCAA Freedom of Information Act Program regulation has been published in the Federal Register as 32 CFR Part 290. It may be accessed through the Agency web site http://www.dcaa.mil/FOIA/FOIA_Reading_Room.html

Appendix B - The Privacy Act of 1974, 5 U.S.C. §552a

The Privacy Act of 1974, 5 U.S.C. §552a, is available from the Defense Privacy and Civil Liberties Office's web site at <http://dpclo.defense.gov/privacy/documents/pa1974.pdf>.

Appendix C - Reference Material

Government Publications

Regulatory Issuances

Title 5, United States Code, 552, The Freedom of Information Act

Title 5, United States Code, 552a, The Privacy Act of 1974

Department of Defense

DoD Directive 5105.36, Defense Contract Audit Agency

DoD Directive 5400.7, DoD Freedom of Information Act Program

DoD Directive 5400.11, Department of Defense Privacy Program

DoD 5400.7-R, DoD Freedom of Information Act Program

DoD 5400.11-R, Department of Defense Privacy Program

DoD FAR Supplement, Appendix G Activity Address Numbers

DoD Handbook 4105.59-H, DoD Directory of Contract Administration Services Components

DCAA Instruction 5410.8, DCAA Freedom of Information Act Program

DCAA Instruction 5410.10, DCAA Privacy Act Program

DCAA Instruction 5025.2, Index of DCAA Numbered Publications

DCAA Instruction 5025.13, Index of DCAA Memorandums for Regional Directors

DCAA Instruction 7230.3, User Charges

DCAA Pamphlet 5100.1, Directory of DCAA Offices

Other Federal Agencies

OMB Circular A-130, Management of Federal Information Resources (50 FR 52730)

OMB FOIA Reform Act of 1986; Uniform FOIA Fee Schedule and Guidelines (52 FR 10012)

OMB Privacy Act Implementation (40 FR 28948)

Appendix D - Pro Forma Paragraphs

Exemptions

b(2) (b)(2), as it applies to operating rules and guidelines that must remain privileged in order for this Agency to adequately fulfill its mission.

b(4) (b)(4), the disclosure of trade secrets, commercial and financial data could cause substantial harm to the competitive position of the entity from which the information was obtained, could impair the ability of the Government to obtain such information in the future or could impair some other legitimate Government interest.

b(5) (b)(5), information is predecisional inter/intra agency data that is part of a decision-making process containing opinions and recommendations.

b(6) (b)(6), the disclosure of information would constitute a clearly unwarranted invasion of personal privacy of individuals.

b(7)(A) (b)(7)(A), the disclosure of any portion of the investigation at this time could reasonably be expected to interfere with law enforcement proceedings. We do not have a timeframe for the completion of this investigation.

Fee Waiver Request

With respect to the portion of your letter seeking a waiver of the customary fees, we will be in a position to make a decision on that request once our records search is completed.

Appeal Rights

The following statement must be made on each response containing denials:

Should you disagree with the finding cited above, you may appeal in writing within 60 calendar days from the date of this letter to Mr. J. Philip Anderson, Assistant Director, Resources, at the above address. If you have further questions, please contact the DCAA Information and Privacy Adviser at 703-767-1022.

Mission Statement

Our mission is to produce audit reports for contracting offices; these audit reports are the property of DoD contracting offices and their release is at the sole discretion of those offices. Therefore, we recommend that you send any requests for audit reports to the contracting officer's FOIA office.

Appendix E – Agency Freedom of Information and Privacy Act Coordinators

Headquarters, DCAA

Defense Contract Audit Agency
8725 John J. Kingman Road, Suite 2135
Fort Belvoir, VA 22060-6219
(TEL) (703) 767-1022

Central Region

Defense Contract Audit Agency
6321 Campus Circle Drive
Irving, Texas 75063-2742
(TEL) (972) 753-2535

Eastern Region

Defense Contract Audit Agency
2400 Lake Park Drive, Suite 300
Smyrna, GA 30080-7644
(TEL) (770) 319-4510

Mid-Atlantic Region

Defense Contract Audit Agency
615 Chestnut Street, Suite 1000
Philadelphia, PA 19106-4498
(TEL) (215) 597-5403

Northeastern Region

Defense Contract Audit Agency
59 Lowes Way, Suite 300
Lowell, MA 01851-5150
(TEL) (978) 551-9831

Western Region

Defense Contract Audit Agency
16700 Valley View Avenue, Suite 300
La Mirada, CA 90638-5833
(TEL) (714) 228-7033

Appendix F – Boilerplate Letters and Memorandums

ACKNOWLEDGEMENT LETTER

CM 502.4
I-12-058-H

Address

Dear Sir:

This letter is in response to your amended Freedom of Information Act (FOIA) request dated July 6, 2012, and received in this office on July 9, 2012. You are requesting:

We are processing FOIA requests that were received prior to yours. In an attempt to afford each requester equal and impartial treatment, we have adopted a general practice of assigning requests in the order of receipt. Your FOIA request has been assigned case number I-12-058-H. Please mention this number in any future correspondence to this agency regarding this matter.

We will notify you of the decision on your FOIA request as soon as possible. The necessity of this delay is regretted and your continuing courtesy is appreciated. Should you have any questions regarding this matter, please contact Mr. Keith Mastromichalis, the DCAA Information and Privacy Adviser at 703-767-1022.

Sincerely,

Duane R. Adens
Chief
Information and Records Management Branch

FOIA SEARCH TASKER MEMORANDUM

CM 503.2
I-12-058-H

TO: O

FROM: CM

SUBJECT: Freedom of Information Request

The enclosed Freedom of Information Act (FOIA) request from: is forwarded to your office for review and action. (Requester) is requesting:

Please review the request and provide this office with copies of any responsive documents along with your assessment as to their releasability under the Freedom of Information Act. Any recommendations for withholding information should be conveyed as bracketed text, in red pencil, on the copies you provide. In addition, any recommendations for withholding information should include a detailed narrative supporting the reasons(s) for withholding and stating the specific "harm" which would be realized if released.

Provide your response to this office no later than TEN BUSINESS DAYS. If you have any questions, please contact Mr. Keith Mastromichalis, Information and Privacy Adviser, at (703) 767-1022.

Duane R. Adens
Chief
Information and Records Management Branch

Enclosure:

1. FOIA Case I-12-058-H Request Letter

ACKNOWLEDGEMENT REFERRAL LETTER

CM 502.4
I-12-042-W

Address

Dear Sir:

This is an interim response to your Freedom of Information Act request dated April 24, 2012, and received in this office on April 25, 2012. You are requesting:

Our Western Region operates its own FOIA Office and would have cognizance over the records you have requested. They have been sent a copy of your request and will respond directly to you concerning the availability of the records you requested.

Should you disagree with the denial of your expedited processing, you may appeal in writing within 60 calendar days from the date of this letter to Mr. J. Philip Anderson, Assistant Director, Resources, at the above address. If you have further questions, please contact the DCAA Information and Privacy Adviser at 703-767-1022.

Sincerely,

Duane R. Adens
Chief
Information Management and Records Branch

REGIONAL REFERRAL MEMORANDUM

CM 502.4
I-12-047-W

MEMORANDUM FOR REGIONAL DIRECTOR, WESTERN REGION

ATTENTION: Ms. Michele Fratus
Freedom of Information Act Officer

SUBJECT: Freedom of Information Act Request

The enclosed Freedom of Information Act request from (Requester) is forwarded to you for a release determination and direct response to the requester in the enclosed action (Enclosure 1).

A copy of our letter to the requester is provided at Enclosure 2. Should you have any questions, please contact the DCAA Information and Privacy Adviser, Mr. Keith Mastromichalis at 703-767-1022.

Sincerely,

Duane R. Adens
Chief
Information Management and Records Branch

Enclosures: 2

1. FOIA Request
2. HQ, DCAA Response

RELEASE IN FULL FINAL RESPONSE LETTER

CM 502.4
I-12-020-H

Address

Dear Sir:

This letter is a final response to your Freedom of Information Act (FOIA) request dated January 20, 2012 (DCAA FOIA Case Number I-12-020-H). You are requesting:

Enclosed is a copy of the DCAA Memorandum for Regional Directors, Audit Guidance/Management Memorandum No. 99-PFC-084(R), July 26, 1999. This Memorandum for Regional Directors that originated with the Defense Contract Audit Agency may be released to you without redactions.

For your information, the correct number for this DCAA Memorandum of Regional Directors is 99-PFC-084(R).

Should you have any questions regarding this matter, please contact Mr. Keith Mastromichalis, the DCAA Information and Privacy Adviser at 703-767-1022.

Sincerely,

Duane R. Adens
Chief
Information and Records Management Branch

Enclosure:
DCAA MRD 99-PFC-084(R)

NO RECORDS FINAL RESPONSE LETTER

CM 502.4
I-12-031-H

Address

Dear Sirs:

This responds to your March 22, 2012, Freedom of Information Act (FOIA) request (DCAA FOIA Case Number I-12-031-H) for:

We have reviewed your request in an effort to assist you. Based on the information you provided, we must conclude that we have no records responsive to your request.

DCAA's mission is to produce audit reports for contracting offices; these audit reports are the property of DoD contracting offices and their release is at the sole discretion of those offices. Therefore, we recommend that you send any requests for audit reports to the contracting officer's FOIA office.

Should you disagree with the finding cited above, you may appeal in writing within 60 calendar days from the date of this letter to Mr. J. Philip Anderson, Assistant Director, Resources, at the above address. If you have further questions, please contact the DCAA Information and Privacy Adviser at 703-767-1022.

Sincerely,

Duane R. Adens
Chief
Information and Records Management Branch

NO RECORDS CONTRACT INFORMATION FINAL RESPONSE LETTER

CM 502.4
I-12-029-H

Address

Dear Sirs:

This responds to your March 24, 2012, Freedom of Information Act (FOIA) request (DCAA FOIA Case Number I-12-029-H) for:

We have reviewed your request in an effort to assist you. Based on the information you provided, we must conclude that we have no records responsive to your request.

The documents you are requesting would be associated with contracts. This Agency does not produce contracts. Our mission is to produce audit reports for contracting offices; these audit reports are the property of DoD contracting offices and their release is at the sole discretion of those offices. Therefore, we recommend that you send any requests for audit reports to the contracting officer's FOIA office.

You may find some information pertaining to contracts issued by the Federal government by contacting the Federal Procurement Data Center, 1800 F Street, NW, Washington, DC 20405-0002, (202) 219-3416 (<https://www.fpds.gov>).

Should you disagree with the finding cited above, you may appeal in writing within 60 calendar days from the date of this letter to Mr. J. Philip Anderson, Assistant Director, Resources, at the above address. If you have further questions, please contact the DCAA Information and Privacy Adviser at 703-767-1022.

Sincerely,

Duane R. Adens
Chief
Information and Records Management Branch

SUBMITTERS NOTICE LETTER

CM 502.4
I-10-030-H

Address

Dear Sirs:

This is in reference to an August 26, 2009, Freedom of Information Act request from for the following information:

Under the provisions of the Federal of Information Act, we must determine whether these documents, or any part of them, contain confidential business information that is proprietary to your company and that should be withheld, therefore, from public disclosure under 5 U.S.C. § 552(b)(4). If the documents contain no propriety information, we will release the documents with redactions for personal privacy. If we determine that some materials in the documents are proprietary, the Freedom of Information Act requires us to segregate and withhold the proprietary portion and to release the rest to the requester.

Please review the enclosed documents. If you believe that any portion of the material in them is exempt from release, answer the following questions in sufficient detail to demonstrate, as to each portion, that the material should be withheld.

1. Was the information transmitted to, and received by DCAA in confidence? Please give detail.
2. To the best of your knowledge, is the information currently available in public sources?
3. Does your company customarily treat this information, or this type of information, as confidential? Please explain why.
4. Would public disclosure of this information be likely to cause substantial harm to the competitive position of your company? If so, how?

Please provide your response to the above questions to this office no later than TEN BUSINESS DAYS. If your response has not been received by this date, the requested materials will be process by this agency.

Should you have any questions regarding this matter, please contact Mr. Keith Mastromichalis, the DCAA Information and Privacy Adviser at 703-767-1022.

Sincerely,
Supervisor

REFERRAL TO ANOTHER AGENCY MEMORANDUM

CM 502.4
I-11-074-H

MEMORANDUM FOR DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
ROOM 10139
451 7TH STREET, N.W.
WASHINGTON, DC 20410

SUBJECT: Freedom of Information Act Request Referral
REQUESTER
FOIA Case Number I-11-074-H

This memorandum refers to the attached subject request. While processing this request, we identified your information consisting of five pages in our files. This attached information is referred for your review, release determination and direct response to (Requester). A copy of our response to the requester is attached. Please furnish this office with a copy of your final response to the requester.

This office has redacted information on the attached document that originated with this agency, we request the information to be withheld in accordance with the FOIA under exemption (b)(6), the disclosure of information would constitute a clearly unwarranted invasion of personal privacy of individuals. If you determine the attached document that is redacted should be released, please provide the following appeal information to the requester: Your appeal should be in writing to the Appellate Authority, Defense Contract Audit Agency: Mr. J. Philip Anderson, Assistant Director, Resources, Defense Contract Audit Agency, 8725 John J. Kingman Road, Suite 2135, Fort Belvoir, VA 22060-6219

Should you have any questions regarding this matter, please contact Mr. Keith Mastromichalis, the DCAA Information and Privacy Adviser at 703-767-1022.

Sincerely,

Duane R. Adens
Chief
Information and Records Management Branch

Attachments:

1. DCAA I-11-074-H Request Letter
2. DCAA Referred Document

FINAL RESPONSE LETTER

CM 502.4
I-12-038-H

Address

Dear Sirs:

This letter is a final response to your Freedom of Information Act (FOIA) request dated April 11, 2012 (DCAA FOIA Case Number I-12-038-H). You are requesting:

USE PRO FORMA EXEMPTION PARAGRAPH(S)

Should you disagree with the finding cited above, you may appeal in writing within 60 calendar days from the date of this letter to Mr. J. Philip Anderson, Assistant Director, Resources, at the above address. If you have further questions, please contact the DCAA Information and Privacy Adviser at 703-767-1022.

Sincerely,

Duane R. Adens
Chief
Information and Records Management Branch

APPEAL ACKNOWLEDGEMENT LETTER

CM 502.4
A-12-002-H

Address

Dear Sirs:

This is to acknowledge receipt of your May 22, 2012, letter in which you are appealing the no records responsive to your April 4, 2012, Freedom of Information Act request (DCAA FOIA Case Number I-12-036-H). Once our new search for responsive records in DCAA's Headquarters' Operations component is completed, we will offer you our final decision on the matter.

Should you have any questions related to the processing of your appeal, please contact Mr. Keith Mastromichalis at (703) 767-1022.

Sincerely,

J. Philip Anderson
Assistant Director, Resources

APPEAL FINAL RESPONSE LETTER

CM 502.4
A-12-002-H

Address

Dear Sirs

This is in response to your May 22, 2012, Freedom of Information Act (FOIA) appeal letter in which you are appealing the no records denial to your April 4, 2012, Freedom of Information Act request (DCAA FOIA Case Number I-12-036-H).

Based upon the results of a new search for responsive records in our DCAA Livelink records management system and DCAA Headquarters Operations component, we have concluded that DCAA has no records responsive to your request.


This determination is the final decision of this Agency on your appeal. If you disagree with this decision, you may seek judicial review in the United States District Courts in the district where you are located, where the requested information is located, or in the U.S. District Court of the District of Columbia.

Should you have any further questions, please contact Mr. Keith Mastromichalis, Information and Privacy Adviser at (703) 767-1022.

Sincerely,

J. Philip Anderson
Assistant Director, Resources

Appendix G – FOIA Forms

FOIA
FREEDOM OF INFORMATION ACT

ACTION
<p><u>NOTE:</u> RESPONSE TO REQUESTER MUST BE ACCOMPLISHED WITHIN 10 WORKING DAYS AFTER RECEIPT. (PUBLIC LAW 93-502)</p> <p>DCAAR 5410.8 32 CFR PART 290</p>

DCAA Label 1
December 2007

HANDCARRY

**FREEDOM
OF
INFORMATION
ACT**

**REQUEST
HANDCARRY**

DCAA Label 2
December 2007

FREEDOM OF INFORMATION ACT

32 CFR Part 290



**DOCUMENT(S) PROVIDED
IN RESPONSE TO YOUR REQUEST**

FREEDOM OF INFORMATION CASE SUMMARY					
1. REQUEST NUMBER:		2. TYPE OF REQUEST: <input type="checkbox"/> INITIAL <input type="checkbox"/> APPEAL		3. TYPE OF REQUESTER: <input type="checkbox"/> COMMERCIAL <input type="checkbox"/> NEWS MEDIA <input type="checkbox"/> OTHER <input type="checkbox"/> SCIENTIFIC/EDUCATIONAL INSTITUTION	
4. ACTIONS TAKEN: <input type="checkbox"/> GRANTED IN FULL <input type="checkbox"/> GRANTED IN PART <input type="checkbox"/> DENIED <input type="checkbox"/> LACK OF RECORDS <input type="checkbox"/> NOT AN AGENCY RECORD <input type="checkbox"/> RECORDS NOT DESCRIBED <input type="checkbox"/> REQUESTER NON COMPLIANCE <input type="checkbox"/> REQUEST WITHDRAWN <input type="checkbox"/> TRANSFERRED TO: _____					
5. EXEMPTIONS INVOKED: <input type="checkbox"/> B1 <input type="checkbox"/> B2 <input type="checkbox"/> B3 AND STATUTE <input type="checkbox"/> B4 <input type="checkbox"/> B5 <input type="checkbox"/> B6 <input type="checkbox"/> B7 <input type="checkbox"/> B8 <input type="checkbox"/> B9 IDA _____					
6. EXTENTIONS: <input type="checkbox"/> LOCATION <input type="checkbox"/> VOLUME <input type="checkbox"/> CONSULTATION <input type="checkbox"/> COURT INVOLVEMENT					
*Chargeable to the requester **Chargeable to commercial requesters					
7. PROCESSING COST					
Grade levels for each type of direct cost listed below will be as follows: Clerical (GS-8 and below), Professional (GS-9 - GS-15) and Executives (GS-16 and above).					
TYPE OF PROCESS (A)	TYPE OF DIRECT COST (B)	HOURLY RATE (C)	NUMBER OF HOURS (D)	COST (C X D) (E)	TOTAL COST (ADD FIGURES IN COLUMN E FOR EACH (F))
Search	Clerical	\$20.00		\$ 0.00	*
	Professional	\$44.00		\$ 0.00	\$ 0.00
Review/Redaction	Clerical	\$20.00		\$ 0.00	**
	Professional	\$44.00		\$ 0.00	
	Executive	\$75.00		\$ 0.00	\$ 0.00
Coordination/ Approval/ Denial	Professional	\$44.00		\$ 0.00	
	Executive	\$75.00		\$ 0.00	\$ 0.00
Correspondence Preparation	Clerical	\$20.00		\$ 0.00	\$ 0.00
Computer Search	Machine			\$ 0.00	\$ 0.00*
Other Activity	Clerical	\$20.00		\$ 0.00	
	Professional	\$44.00		\$ 0.00	\$ 0.00
8. OTHER CASE COSTS					
TYPE OF PROCESS (A)	COST PER COPY (B)	TOTAL PAGES (C)	TOTAL COST (B X C) (D)		
Office Copy Reproduction	\$0.15		\$ 0.00 *		
CD	\$1.50		\$ 0.00 *		
9. REMARKS:					
10. FOR FOI OFFICE USE ONLY					
TOTAL COLLECTABLE COSTS:	TOTAL PROCESSING COSTS:	TOTAL CHARGED:	FEES WAIVED/REDUCED:		
\$0.00	\$0.00		<input type="checkbox"/> TWO FREE HOURS OF SEARCH TIME <input type="checkbox"/> 100 FREE PAGES OF REPRODUCTION <input type="checkbox"/> PUBLIC/GOVERNMENT INTEREST <input type="checkbox"/> LESS THAN \$15.00 THRESHOLD <input type="checkbox"/> OTHER: _____		
SEARCH FEES PAID:	REVIEW FEES PAID:	COPY FEES PAID:			

INSTRUCTIONS FOR COMPLETING THE FOIA CASE SUMMARY	
1.	REQUEST NUMBER - First two digits will express Fiscal Year followed by dash (-) and activity request number. i.e., I-89-001-H.
2.	TYPE OF REQUEST - Mark the appropriate block to indicate initial request or appeal of a denial.
3.	TYPE OF REQUESTER - Mark the appropriate block to indicate category of requester.
4.	ACTIONS TAKEN - Mark the block(s) which summarizes actions taken on the request. If the action was transferred, enter the name(s) of the other DoD Component or Federal Agency to which it was sent. Referrals to other DCAA activities should not be counted for reporting purposes. See DCAAR 5410.5 for more information on each action taken.
5.	EXEMPTIONS INVOKED - Mark the appropriate exemption(s) invoked to withhold records from the public. In the case of exemption (b) (3), the actual statute should also be entered (e.g., 5 USC 1917).
6.	EXTENSIONS - Mark the appropriate block to indicate the reason for invoking a 10 day extension.
7.	<p>PROCESSING COST - For each applicable activity category, enter time expended to the nearest 15 minutes in the number of hours column (D).</p> <p>SEARCH - Time spent locating from the files the requested information.</p> <p>REVIEW / EXCISING - Time spent reviewing the document content and determining if the entire document must retain its classification or segments could be excised thereby permitting the remainder of the document to be declassified.</p> <p>In reviewing for other than classification, FOI exemptions 2 through 9 should be considered.</p> <p>COORDINATION / APPROVAL / DENIAL - Time spent coordinating the staff action with interested offices or agencies and obtaining the approval for the release or denial of the requested information.</p> <p>CORRESPONDENCE PREPARATION - Time spent in preparing the necessary correspondence and forms to answer the request.</p> <p>COMPUTER SEARCH - Enter exact computer processing value in the total hours column. The salary scale for the programmer/operator executing the search will be recorded as part of the computer search cost.</p> <p>Multiply total hours by the computer hourly rate and enter the cost figures. Computer search will be based on direct cost only of the Central Processing Unit, input/output devices, and memory capacity of the actual computer and configuration used.</p> <p>OTHER ACTIVITY - Time spent in activity other than above, such as, duplicating documents, hand carrying documents to other locations, restoring files, etc.</p>
8.	<p>OTHER CASE COSTS</p> <p>OFFICE COPY REPRODUCTION - Enter the number of pages reproduced.</p> <ul style="list-style-type: none"> - Multiply by the rate per copy and enter cost figures. - CD - Enter number of disks being sent to the requester.
9.	REMARKS - Self explanatory.
10.	<p>FOR FOI OFFICE ONLY</p> <p>TOTAL COLLECTABLE COSTS - Add the blocks in the total cost column marked with an asterisk and enter total in the total collectable cost block.</p> <p>TOTAL PROCESSING COSTS - Add all blocks in the total cost column and enter total in the total processing cost block. The total processing cost in most cases will exceed the total collectable cost.</p> <p>TOTAL CHARGED - Enter the total amount that the requester was charged, taking into account the fee waiver threshold and fee waiver policy.</p> <p>SEARCH FEES PAID - Enter total clerical and professional search and/or computer search fees paid by the requester.</p> <p>REVIEW FEES PAID - Enter total review fees paid by the requester.</p> <p>COPY FEES PAID - Enter total amount paid by the requester for office copy reproduction.</p> <p>FEES WAIVED / REDUCED - Mark the appropriate block as applicable. Enter reason for the fee waiver reduction (e.g., public interest).</p>

FOIA CONTROL RECORD

1. REQUEST NUMBER: 2. DATE OF REQUEST: 3. DATE RECEIVED: 4. REQUESTOR: 5. ORGANIZATION:

6. DESCRIPTION OF RECORDS REQUESTED:

a. Name (s) and Date (s) of Parties:	b. Description of Discussion/Action:
--------------------------------------	--------------------------------------

[illegible]

DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

DL

DCAA REGULATION
NO. 5500.4

July 20, 2006

**COORDINATION OF SIGNIFICANT LITIGATION AND OTHER MATTERS INVOLVING
THE DEPARTMENT OF JUSTICE**

Reference: DoD Instruction 5030.7, Coordination of Significant Litigation and Other Matters Involving the Department of Justice, dated 22 August 1988

1. REISSUANCE AND PURPOSE. This regulation implements DoD Instruction 5030.7 and establishes procedures for coordination of requests to the Department of Justice for formal opinions and for coordinating DCAA actions that are being litigated or that may be litigated by the Department of Justice.

2. CANCELLATION. DCAA Regulation 5500.4, Coordination of Significant Litigation and Other Matters Involving the Department of Justice, dated April 20, 2002, is canceled.

3. APPLICABILITY AND SCOPE. This regulation applies to all DCAA organizational elements.

4. POLICY. DCAA will coordinate with other DoD Components all requests to the Department of Justice for formal opinions and all civil and criminal actions significantly affecting the Department of Defense but under the purview of the Department of Justice.

5. RESPONSIBILITIES.

5.1. Heads of Principal Staff Elements and Regional Directors are responsible for notifying the Director and General Counsel, DCAA, as soon as practicable, of any matters which require external coordination under this regulation. Initial telephonic notification is encouraged.

5.2. The General Counsel, DCAA, is responsible for:

5.2.1. Ensuring that the Director, DCAA is kept apprised of significant litigation and other matters involving the Department of Justice that have an impact on DCAA operations or activities and require coordination with the General Counsel, DoD.

5.2.2. Coordinating with other DoD Components and the General Counsel, DoD, all requests to the Department of Justice for formal opinions.

5.2.3. Maintaining liaison with other DoD Components and the General Counsel, DoD, concerning all significant court actions conducted by the Department of Justice at the trial or appellate stage that may affect materially the administration of another DoD Component or the

legal basis of an activity of the Department of Defense. This includes coordination with the General Counsel, DoD, and other affected DoD components on recommendations for seeking *certiorari* for cases before the Supreme Court.

5.2.4. Ensuring that the General Counsel, DoD, is kept advised of significant developments pertaining to those actions in which the Secretary of Defense is a party, in his or her personal capacity, and for which the primary responsibility for supporting the Department of Justice is being discharged by DCAA.

5.2.5. Submitting and updating case reports on significant actions which are either defended by the Department of Justice or have been referred to the Department of Justice for possible court action and for which DCAA is the cognizant component.

5.2.6. Submitting reports on all new significant legal issues that may affect materially the administration of another DoD activity or that may attract widespread publicity.

6. EFFECTIVE DATE. This regulation is effective immediately.

/s/

William H. Reed
Director



DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

DL

February 13, 2008

DCAA INSTRUCTION
NO. 5500.8

ALLEGATIONS AGAINST SENIOR OFFICIALS OF DOD

- References:
- (a) DoD Directive 5505.6, Investigations of Allegations Against Senior Officials of the Department of Defense, April 10, 2006,
<http://www.dtic.mil/whs/directives>
 - (b) DoD 5500.7-R, Joint Ethics Regulation (JER), August 30, 1993,
<http://www.dtic.mil/whs/directives>
 - (c) Uniform Code of Military Justice, 10 U.S.C. § 801 et seq.
http://www.access.gpo.gov/uscode/title10/subtitlea_partii_chapter47_.html

1. REISSUANCE AND PURPOSE. This instruction implements reference (a) and establishes policy, assigns responsibilities, and prescribes procedures for reporting to the Inspector General, Department of Defense (DoDIG) allegations of serious misconduct against senior officials of the Department of Defense.

2. CANCELLATION. This cancels DCAA Instruction 5500.8, Allegations Against Senior Officials of DoD, dated August 25, 2000.

3. APPLICABILITY AND SCOPE. This instruction applies to all organizational components of DCAA, and governs the responsibilities for reporting and investigating allegations of misconduct by senior officials of the Department of Defense (DoD).

4. DEFINITIONS.

4.1. Allegations of Misconduct. A credible allegation that, if proven, would constitute:

4.1.1. A violation of criminal law, including for military officers, a violation of the Uniform Code of Military Justice (reference (c)).

4.1.2. A violation of the DoD Standards of Conduct as identified in the Joint Ethics Regulation, DoD 5500.7-R (reference (b)).

4.1.3. A matter not included in paragraphs 4.1.1 and 4.1.2 that, nevertheless, involves other misconduct of concern to the leadership of the DoD or could reasonably be expected to be of significance to the Secretary of Defense, especially when there is an element of unauthorized personal benefit to the senior official, a family member, or an associate.

4.2. Senior Official. Active duty, retired, Reserve, or National Guard military officers in or selected for promotion to grades O-7 and above; current and former members of the Senior Executive Service; other current and former DoD civilian employees whose positions are deemed equivalent to that of a member of the Senior Executive Service (e.g., Defense Intelligence Senior Executive Service employees, senior level employees, and non-appropriated fund senior executives); and current and former Presidential appointees.

5. POLICY.

5.1. It is DCAA policy to assure that allegations of serious misconduct against senior DoD officials are promptly reported to the DoDIG.

5.2. Allegations of misconduct against senior officials shall be vigorously investigated by appropriate investigative organizations pursuant to the procedures established in DoD Directive 5505.6 (reference (a)).

6. RESPONSIBILITIES. The General Counsel, DCAA shall serve as the component designated official (CDO) who is the point of contact with the DoDIG for the exchange of information required by paragraph 5.2.1 of DoD Directive 5505.6 (reference (a)).

7. PROCEDURES.

7.1. The General Counsel, DCAA, shall:

7.1.1. Report to the DoDIG, within 5 workdays of receipt, allegations of serious misconduct made against senior officials of DCAA or other DoD components. The notification shall be made in writing and shall include the following information:

7.1.1.1. Name of senior official(s) involved.

7.1.1.2. Rank and/or grade and duty position of senior official.

7.1.1.3. Organization and location of senior official.

7.1.1.4. Synopsis of the allegation(s) and date received by the CDO.

7.1.1.5. Name and duty position of the CDO.

7.1.2. If the senior official involved is an employee of DCAA, and unless notified that the DoDIG assumes investigative responsibility for a particular matter, initiate or cause to be initiated an investigation of the issues raised in the allegation(s).

7.1.3. Upon request from the DoDIG, provide the status, scope, findings to date, and expected completion date of the investigation.

7.1.4. Provide a copy of the report of investigations to the DoDIG within 5 work days of completion of the investigation.

7.1.5. Upon request from the DoDIG, provide a written report of any disciplinary and/or administrative action and the nature thereof taken against a senior official.

7.1.6. Ensure that allegations of criminal misconduct are referred to the appropriate criminal investigative organization.

7.2. The Assistant Director, Policy and Plans; the Assistant Director, Resources; and the Assistant Director, Operations shall assure that all allegations of serious misconduct against senior DCAA officials that are directed to them for action are promptly forwarded to the General Counsel for reporting to the DoDIG.

7.3. All DCAA employees shall report all instances of serious misconduct involving senior DoD officials directly to the General Counsel. Reports of allegations of serious misconduct involving the General Counsel, DCAA, shall be reported directly to the General Counsel, DoD. Notwithstanding any other regulation or CAM provisions, such allegations shall be reported only in accordance with this instruction.

8. EFFECTIVE DATE. This instruction is effective immediately.

/s/
John M. Farenish
General Counsel



DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

Q

June 17, 2010

DCAA INSTRUCTION
NO. 7050.1

**ACCESS TO DEFENSE CONTRACT AUDIT AGENCY RECORDS AND INFORMATION
BY THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE**

Reference: DoD Instruction 7050.3, "Access to Records and Information by the Inspector General, Department of Defense", dated April 24, 2000, and available at <http://www.dtic.mil/whs/directives>

1. REISSUANCE AND PURPOSE. This instruction implements the referenced DoD instruction and assigns responsibilities for expediting access to data required by members of the Department of Defense Inspector General (DoDIG), in the performance of their official duties.

2. CANCELLATION. DCAAI 7050.1, Access to Defense Contract Audit Agency Records and Information by the Inspector General, Department of Defense, dated August 22, 2003, is hereby canceled.

3. APPLICABILITY AND SCOPE. This instruction applies to all organizational elements of DCAA.

4. POLICY.

4.1. Timely access to DCAA personnel and documents needed for the performance of announced DoDIG reviews shall be granted subject to the limitations in 4.2. below.

4.2. Access to Privacy Act data, sensitive documents, and data not required as part of announced DoDIG reviews shall be granted in accordance with the provisions in 5. below.

5. RESPONSIBILITIES.

5.1. The Assistant Director, Integrity and Quality Assurance Directorate (Q), shall serve as the designated focal point for arranging access to sensitive DCAA documents, such as executive conference minutes, Quality Assurance Program documents, etc.

5.2. Heads of Principal Staff Elements, Regional Directors, and Director, Field Detachment shall provide timely and appropriate access to Headquarters and regional personnel, documents, and files, other than sensitive or Privacy Act data, needed for the performance of announced DoDIG reviews. A proper security clearance will be required from those DoDIG officials

requesting access to classified data. DoDIG requests for data not associated with announced reviews will be referred promptly to Headquarters, DCAA, Attention: Q.

5.3. DCAA system managers or other designated officials shall provide Privacy Act data in response to written DoDIG requests made in connection with announced reviews.

5.4. The Assistant Director, Integrity and Quality Assurance is designated as the focal point to:

5.4.1. Respond to written DoDIG requests for data not required in connection with announced reviews.

5.4.2. Respond to written DoDIG requests for special DCAA Management Information System (DMIS) output reports, where existing DMIS reports cannot be used.

5.4.3. Resolve any access to records problems that cannot be resolved by the region. It is important that problems be referred in a timely manner since any objection to granting access must be submitted to the DoDIG by the Director, no later than 15 days from the date of the DoDIG's request.

6. EFFECTIVE DATE. This instruction is effective immediately.

FOR THE DIRECTOR:

/s/

Donald J. McKenzie
Assistant Director
Integrity and Quality Assurance



DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

PQA

August 28, 2003

DCAA Instruction

7050.2

RESPONDING TO OVERSIGHT REVIEWS

References:

- (a) DoD Directive 5106.1, *Inspector General of the Department of Defense*, dated January 4, 2001 and available at <http://dtic.mil/whs/directives>
- (b) DoD Directive 7650.1, *General Accounting Office Access to Records*, dated September 11, 1997 and available at <http://dtic.mil/whs/directives>
- (c) DoD Instruction 7650.4, *Procedures for Responding to General Accounting Office and Comptroller General Requests for Access to Records*, dated September 9, 1997 and available at <http://dtic.mil/whs/directives>

1. Reissuance and Purpose. This instruction provides procedures for responding to visits and inquiries taking place under oversight reviews covered by the referenced DoD Directives and Instruction.

2. Cancellation. DCAA Instruction No. 7050.2 dated August 22, 2000 is canceled.

3. Applicability and Scope. This instruction is applicable to all DCAA organizational levels.

4. Policy.

4.1. To ensure accuracy and completeness of Agency responses to oversight reviews, it is DCAA policy that Regional Directors will respond directly to oversight reviewer visits or inquiries regarding matters which pertain exclusively to actions occurring within their regions.

4.2. To ensure timeliness of Agency responses, it is DCAA policy that no more than three levels of review will be interposed between the originating office and transmission of the written response to the oversight reviewer.

4.3. Regional Directors may submit inquiries to Headquarters covering specific issues for which expertise is not available at the regional level. Such situations include, but are not limited to, questions regarding policy issues, operations, resources, or emerging technical areas not covered

by written Agency guidance. Headquarters responses on these issues will be incorporated into the written response by the Regional Director.

5. *Responsibilities.*

5.1. Assistant Directors, Headquarters will:

5.1.1. Coordinate oversight reviews affecting their areas of responsibility in accordance with Enclosure 1 by:

5.1.1.1. Reviewing the DoDIG annual program plan.

5.1.1.2. Reviewing the DoDIG or GAO announcement letter for a specific review.

5.1.1.3. Attending the oversight reviewers' entrance conference to become familiar with the review locations and objectives.

5.1.1.4. Notifying Regional Directors of the impending review.

5.1.1.5. Maintaining coordination with the reviewers, including attendance at field review sites as necessary.

5.1.2. Review inquiries appropriately forwarded by Regional Directors, coordinate Headquarters responses from other Directorates if necessary, and provide responses to regions for timely inclusion in the written response.

5.1.3. Coordinate preparation of the Agency response to the oversight reviewers' draft and final reports.

5.1.4. Coordinate ongoing activities as outlined in Enclosure 1.

5.1.5. Assist in maintaining a Policy and Plans database which incorporates summary data on the status of all oversight reviews, and a Tracking System which monitors the status of oversight report recommendations.

5.2. Regional Directors and the Director, Field Detachment will:

5.2.1. Assure that the audit staff is adequately trained and aware of their responsibilities.

5.2.2. Assure that notice of impending reviews and their objectives is distributed to sites to be visited within the region within two working days of receipt at the regional office.

5.2.3. Notify Headquarters, PQA, of any oversight reviewer contacts with FAOs for which the region does not have notice of official coordination.

5.2.4. Designate no more than three levels of regional review for responses from the region. This may be done via Regional Instruction applicable to every review or on a case-by-case basis.

5.2.5. Assure that submitted written responses are accurate, complete, timely, and in accordance with Enclosure 2 guidelines.

5.2.6. Request information on reviewer questions concerning unique issues of Agency policy, operations, or resource management from the Headquarters staff element monitoring the review only when necessary to assure a complete and accurate response.

5.2.6.1. Identify the question for which Headquarters input is requested.

5.2.6.2. Assess the reason(s) expertise is not available at the regional level.

5.2.6.3. Incorporate information furnished by Headquarters into the written response.

5.2.7. If the reviewer does not require a written response, forward the exit conference notes and related materials furnished by the FAO (see 5.3.9.) to Headquarters, attention: PQA, within five working days of receipt at the regional office.

5.2.8. If the reviewer requires a written response (see 5.3.10.), forward the original copy of the written response to the oversight reviewer, with a concurrent copy to Headquarters, attention: PQA, within the timeframe specified by the reviewer.

5.3. FAO Managers will:

5.3.1. Assure that the oversight review has been fully coordinated by:

5.3.1.1. Obtaining the control number (assignment number, reference number) and title of the review at the time of the initial contact.

5.3.1.2. Notifying the Regional Quality Assurance Division (RQA) (or other designated regional office element) of the contact (see 5.1.1.4.). Should an oversight reviewer request a field visit prior to official coordination, RQA (or other designated regional office element) should immediately inform Headquarters, PQA (see 5.2.3.) and scheduling of the oversight review should be deferred until specific instructions have been received.

5.3.1.3. Advising RQA (or other designated regional office element) and Headquarters, PQA of the date scheduled for the oversight visit.

5.3.2. Provide the oversight reviewer with access to records needed to perform the specific oversight review, including auditor assistance in understanding the circumstances under which the records were prepared. Records related to active contract audits will not be provided without the prior approval of RQA (or other designated regional office element).

5.3.3. Provide administrative field support to the oversight reviewer as requested, including office space and use of standard office equipment. If the FAO manager believes excessive audit support, e.g., reformatting of workpaper data, has been requested, RQA (or other designated regional office element) should be notified.

5.3.4. Provide answers to questions concerning factual issues raised by the reviewer during the course of the review. This improves the reporting of factual information in the government internal audit organization's written observations and comments, and helps to resolve potential issues before they become incorporated in the reviewer's findings.

5.3.5. Preliminary discussions with the oversight reviewer regarding significant issues should take place during the review. If possible, the FAO should obtain the reviewers' written comments and develop the FAO's preliminary position on significant issues prior to the exit conference.

5.3.6. Promptly notify Headquarters, PQA if no exit conference is provided.

5.3.7. If the reviewer provides written notes, request that the representative's written observations and comments be transferred to an electronic file. This will help speed the FAO manager's reporting of the results to the region and Headquarters.

5.3.8. Attend the exit conference.

5.3.9. Prepare and forward to RQA (or other designated regional office element) within ten working days:

5.3.9.1. A memorandum detailing discussions at the exit conference which identifies the organization's control number (assignment number; reference number) and contains all pertinent information, including (i) the purpose of the visit; (ii) the government internal audit organization's observations; (iii) DCAA responses to specific comments or observations; (iv) references to or actual copies of data provided; (v) the representative's reaction after discussions were completed (if known); (vi) any additional comments regarding the representative's reaction; and (vii) any actions that will be taken as a result of the specific findings of the oversight reviewer.

5.3.9.2. If necessary, a memorandum detailing any other matters deemed relevant in understanding the questions to be answered in the written response.

5.3.9.3. Any supplemental documentation requested by the reviewer but not available at the FAO during the review.

5.3.10. If the reviewer's comments are provided in writing, concurrently prepare and forward to RQA (or other designated regional office element) a draft written response to the oversight reviewer's written comments (see Enclosure 2). The response should identify the organization's control number (assignment number; reference number) and contain all pertinent information.

6. *Effective Date and Implementation.* This instruction is effective upon receipt.

For The Director:

Robert DiMucci

Enclosures -- 2

1. Overview of the Oversight Review Process
2. Responding to Inquiries and Field Visit Write-ups

Enclosure 1

Overview of the Oversight Review Process

E1.1. DoDIG Annual Program Plan announcement notifies DCAA of potential reviews.

E1.2. DoDIG or GAO issues an announcement letter for a specific review.

E1.3. Entrance conference is held, usually at DCAA Headquarters, and arrangements are made for field visits.

E1.4. Headquarters appropriately announces the review, identifies the FAOs to be visited and keeps the impacted regions/FAOs apprised of the review status.

E1.5. GAO or DoDIG field visits:

E1.5.1. Oversight reviewer's field visit.

E1.5.2. Oversight reviewer provides region/FAO with results of field visit.

E1.5.3. FAO exit conference memorandum and draft response to reviewer's write-up forwarded to region.

E1.5.4. Region issues response to reviewer with a copy to Headquarters; sends copy of exit conference memorandum to Headquarters.

E1.6. The cognizant Headquarters element will make interim briefings/reports to management as needed.

E1.7. (DoDIG reviews only:) Upon receipt of the DoDIG's discussion draft report by cognizant Headquarters staff element:

E1.7.1. Follow the *Processing Responses to External Oversight Reports* procedure contained in the Attachment.

E1.7.2. Expand the scope of effort to include:

E1.7.2.1. Review of the DoDIG wording for a more favorable tone.

E1.7.2.2. Consider revising and consolidating DoDIG recommendations to correspond to the DCAA position.

E1.7.2.3. Verify DoDIG “facts” to our summaries and evaluate the validity of the DoDIG illustrations.

E1.7.2.4. Arrange for the exit conference date and participants.

E1.7.2.5. Attend the exit conference.

E1.7.2.6. After the exit conference, coordinate results of exit conference with DoDIG reviewer.

E1.8. Receipt of the DoDIG or GAO draft report by cognizant Headquarters staff element:

E1.8.1. Follow the Processing Responses to External Oversight Reports procedure.

E1.8.2. After the draft report response is issued:

E1.8.2.1. Coordinate the results of the response with the oversight reviewer.

E1.8.2.2. Update Tracking System for all concurred recommendations. This includes assigning divisions to perform agreed-to actions.

E1.9. Receipt of the DoDIG or GAO final report by cognizant Headquarters staff element:

E1.9.1. After the final report response is issued, coordinate the results of the response with the oversight reviewer.

E1.9.2. Follow the Processing Responses to External Oversight Reports procedure.

E1.9.3. If all recommendations have been resolved, issue an MRD with the final report and final report response.

E1.9.4. Update the oversight report data base.

E1.9.5. Provide a copy of the report to PQA for update of the Tracking System, and filing of report and response in the Policy and Plans library.

E1.10. Receipt by cognizant Headquarters staff element of DoDIG notification of follow-up review on recommendations forwarded for resolution (DoDIG reviews only):

E1.10.1. Follow the Processing Responses to External Oversight Reports procedure.

E1.10.2. Attend resolution meeting and draft MFR documenting the meeting.

E1.10.3. Issue MRD with the final report, final report response, and the resolution agreement.

E1.10.4. Update the oversight report data base.

E1.10.5. Provide a copy of the report response, and resolution agreement to PQA for update of the Tracking System and filing of report response, and resolution agreement in the Policy and Plans library.

Attachment 1 to Enclosure 1

Processing Responses to External Oversight Reports

A1.E1.1. Headquarters Principal Staff Elements (HPSEs) are responsible for monitoring external oversight (DoDIG/GAO) reviews and Agency responses to the resulting reports. Often these responses require a short turnaround time. The five-step process below should ensure complete and timely response.

A1.E1.1.1. Upon receipt of the reviewer's report, the responsible HPSE will review the draft/final oversight report and refer it to the cognizant staff element (usually a Headquarters division) to identify the sensitive issues requiring DCAA management attention. The cognizant division will determine if the report findings and recommendations are supported by the DoDIG/GAO exit notes and associated FAO comments. Additionally, the division will prepare a timetable for developing the response and attending any scheduled exit conferences. This analysis and timetable will be provided to each affected HPSE.

A1.E1.1.2. The cognizant division will gather needed information and attend any scheduled exit conferences. Any information needed from field offices will be obtained through the cognizant regional offices. Regions may also be requested to provide opinions on issues of policy.

A1.E1.1.3. If no additional information is needed, the Agency response will be developed by the cognizant division. If further information is necessary, the cognizant division may need to arrange a meeting with the responsible HPSE(s) after the appropriate information has been gathered to develop a proposed Agency response. Depending upon the sensitivity, the HPSE will discuss the proposed Agency response with the Director and Deputy Director.

A1.E1.1.4. The cognizant division, with assistance from PQA if necessary, will draft the official Agency response and coordinate it with the affected regional offices and the appropriate Headquarters elements, including D and DD. Because the responsible HPSEs are involved in the development of the response, this coordination will be limited to editorial changes; changes to the Agency's position are not expected.

A1.E1.1.5. The HPSE will transmit the Agency response to the oversight organization and provide copies to the appropriate Headquarters and regional staff elements. The cognizant division will update the Tracking System to reflect completed actions.

Enclosure 2

Responding to Oversight Reviewer Inquiries and Findings Communicated to Field Audit Offices

E2.1. The FAO should include in the draft written response (1) the reviewer's exit notes, if provided; (2) the FAO's comments; and (3) the names, organizations, office telephone numbers and other communications information (fax numbers, e-mail addresses) of the exit conference attendees.

E2.2. The FAO should prepare and forward to the Regional Quality Assurance Division (or other designated regional office element) a summarized listing of the major areas of importance and significant issues raised. Enclosures to the transmittal memorandum should include any other data or information requested by the reviewer.

E2.3. The written response to a specific reviewer comment and/or highlighted and underlined statements should begin by stating the Agency position (Agree, Partially Agree, Disagree, or No Comment):

E2.3.1. If the FAO agrees or partially agrees with the statement, the draft written response should say so. If any action needs to be taken as a result of the reviewer's comments, it should explain what will be done and by when. If the FAO only partially agrees, it should explain the specific area of disagreement.

E2.3.2. If the FAO disagrees with the statement, the draft written response should fully explain why the FAO disagrees. The FAO should provide any working papers, correspondence, or other documentation that supports its position.

E2.3.3. If the FAO has responded to a previous statement on the same matter, no comment, with a reference to the previous response will be the appropriate response. Draft responses to reviewer statements regarding overall Agency policy, operations, or resources should be prepared when answers can be found in written Agency guidance, and the source of the response should be referenced or incorporated. Some statements, such as background information or concluding remarks, do not require a comment.

E2.3.4. Specific reviewer questions should be answered completely and factually. If the reviewer has identified an error or omission, the response should specifically acknowledge the accuracy of the tentative finding. If working papers or other documentation support the written response, provide a copy with the response. Comments on current or significant issues may also be incorporated.

E2.4. An example of each of these types of responses follows:

E2.4.1. Agree:

E2.4.1.1. Reviewer Comment: W/P F-6 summarizes the review of the procedure to correct labor distribution errors. The conclusion paragraph states that a sample of six employees who had labor errors on the November report were taken. There was no documentation of how the month (November) or how the six employees were selected.

E2.4.1.2. DCAA Response: Agree. The auditor should have documented that the sample selection was judgmental. We will issue a memorandum to the audit staff within the next two weeks explaining the importance of properly documenting audit working papers in accordance with CAM 4-400, Audit Working Papers.

E2.4.2. Partially agree:

E2.4.2.1. Reviewer Comment: The auditor should mark superseded working papers as such if he does not intend to rely on the work.

E2.4.2.2. DCAA Response: Partially Agree. Superseded working papers should be marked when superseded. However, working paper A, summarizing the results of audit, was not superseded. A preliminary conclusion reflects agreement between the auditor and supervisory auditor that significant defective pricing did not exist. This is an appropriate documentation of a change in decision and should not be a superseded working paper.

E2.4.3. Disagree:

E2.4.3.1. Reviewer Comment: Most of the standard audit program steps are either lined out or deleted. The audit program appears inadequate in its present condition.

E2.4.3.2. DCAA Response: Disagree. The audit program is budgeted for 80 hours, reflects actual hours for a total of 74 hours, and contains referencing for actual work performed. Steps lined out or deleted did not apply to this procurement. The supervisory auditor signed and dated the audit program. A copy of the audit program is enclosed.

E2.4.4. No comment:

E2.4.4.1. Reviewer Comment: Policy No. 44 states that the contractor will ensure all unallowable costs have been removed from final indirect cost proposals at the time of the certification of the indirect cost rates.

E2.4.4.2. DCAA Response: No comment. (This is a statement of fact. No response is necessary.)

E2.4.5. Question asked:

E2.4.5.1. Reviewer Comment: Did you select another contract to replace the canceled defective pricing assignment? The matrix selection indicated you were to perform a specific number, however, if you did not replace this selection, you would not be performing the required number of defective pricing reviews specified by the matrix?

E2.4.5.2. DCAA Response: We replaced this selection with a contract from XYZ Corporation in the same dollar strata as the canceled assignment. The replacement was contract number F42600-03-C-0001 and audit assignment number 2003A42000031.

E2.4.6. Significant Issue: The reviewer requested that we identify instances in which D/P findings were not sustained by the cognizant Procuring Office. We provided DMIS data. The reviewer selectively reviewed D/P files for which recommended findings were not sustained by (name of procuring office). The DoDIG's exit conference notes do not contain any reference to the reviewer's conclusions, if any, arising from review of the D/P findings presented in the selected files.



DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

Q

June 16, 2011

DCAA INSTRUCTION
NO. 7640.12

**FOLLOW-UP ON OVERSIGHT REPORTS AND MEMORANDA CONCERNING
DEFENSE CONTRACT AUDIT AGENCY OPERATIONS**

- References:
- (a) DoD Instruction 7650.01, *Government Accountability Office (GAO) and Comptroller General Requests for Access to Records*, dated January 27, 2009 and available at <http://www.dtic.mil/whs/directives/>
 - (b) DoD Instruction 7650.02, *Government Accountability Office (GAO) Reviews and Reports*, dated November 20, 2006 and available at <http://www.dtic.mil/whs/directives/>
 - (c) DoD Directive 7650.3, *Follow-up on General Accounting Office (GAO), DoD Inspector General (DoD IG), and Internal Audit Reports*, dated June 3, 2004 and available at: <http://www.dtic.mil/whs/directives>
 - (d) DCAA Instruction No. 7050.2, *Responding to Oversight Reviews*,

1. PURPOSE.

a. This instruction implements policy, assigns responsibilities, and prescribes procedures for DCAA follow-up on findings and recommendations of the Government Accountability Office (GAO) and the Department of Defense Inspector General (DoDIG) which concern DCAA operations as covered by the referenced DoD Instructions and Directive.

b. DCAA Regulation No. 7640.12, dated March 30, 2001, is canceled.

2. APPLICABILITY. This instruction applies to all organizational elements of DCAA.

3. POLICY.

a. DCAA will recognize, support, and use GAO and DoD internal audit recommendations concerning its operations as important elements of its overall management and internal control systems.

b. Prompt and responsive management action will be accorded all GAO and DoDIG findings and recommendations applicable to DCAA operations.

(1) Comments on the findings and recommendations of GAO draft reports should be provided by the requested due date as instructed by the DoDIG, or a written request should be provided outlining the reason for requesting an extension.

(2) Comments on the findings, recommendations, and any proposed corrective action contained in GAO and DoDIG final reports and memoranda will be furnished within 60 days or the requested response date, whichever is earlier. Comments on disagreements will clearly delineate the rationale for the disagreement. Where appropriate, responses will identify corrective action taken or planned to be taken, along with the estimated savings or other anticipated benefits, and the completion dates.

(3) Comments on the findings and recommendations of oversight visits and interviews other than final reports, will be provided in accordance with reference (d).

(4) Where corrective action is considered appropriate, the affected DCAA management level will institute such action and report the completion of corrective measures to the designated DCAA official.

4. RESPONSIBILITIES.

a. The Executive Officer will designate a focal point for GAO and DoDIG announced reviews affecting DCAA operations.

b. The designated focal point will:

(1) Serve as the initial point of contact for GAO and DoDIG reviewers.

(2) Notify the cognizant DCAA organizational element of the impending DoDIG or GAO review by providing the cognizant element a copy of the review announcement, and any other information relevant to establishing a working interface with the reviewer.

(3) Maintain an Agency copy of relevant final GAO and DoDIG reports and memoranda.

(4) Establish and maintain a record of proposed and initiated management actions and time schedules for responding to and acting on findings and recommendations until final disposition has been made.

(5) Prepare periodic reports for DCAA executive management and the DoDIG on the status of implementing agreed-upon GAO and DoDIG recommendations.

c. The Heads of Principal Staff Elements, Regional Directors, and the Director, Field Detachment, will:

(1) Receive, control, and coordinate responses to GAO and DoDIG reports and memoranda, ensuring that appropriate action is taken within the time limits specified by 3.b.(1) and 3.b.(2). above.

(2) Follow-up on GAO and DoDIG reports and memoranda.

(3) Maintain a record of actions taken and time schedules for responding to and acting on findings and recommendations until final disposition has been made of agreed to recommendations.

5. PROCEDURES.

a. Specific procedures for responding to oversight reviews are provided in reference (d).

b. Copies of GAO and DoDIG final reports and memoranda and DCAA's official written response will be provided to the DCAA focal point.

6. RELEASABILITY. UNLIMITED. This Issuance is approved for public release and is available on the Intranet website.

7. EFFECTIVE DATE. This instruction is effective upon receipt.

/s/

Patrick J. Fitzgerald
Director

DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

OTS

June 30, 2006

DCAA REGULATION
No. 7640.15

**MANAGEMENT AND MONITORING OF SUSPECTED CONTRACTOR
FRAUD AND OTHER CONTRACTOR IRREGULARITIES PROGRAM**

- References:
- (a) DoD Directive 7600.2, Audit Policies, March 20, 2004
 - (b) DoD Instruction 7640.4, DoD Contract Auditing Standards, September 4, 1986
 - (c) Memorandum, Deputy Inspector General, Subject: Contract Audit, Internal Audit and Criminal Investigations Joint Policy Memorandum No.2, Coordination by Audit and Investigative Organizations in Cases Involving Allegations of Fraud, April 24, 1987
 - (d) DoD Instruction 5240.4, Reporting of Counterintelligence and Criminal Violations, September 22, 1992
 - (e) DoD Instruction 5505.2, Criminal Investigations of Fraud Offenses, February 6, 2003
 - (f) GAO Yellow Book, Government Auditing Standards, 2003 revision.
 - (g) DoD Directive 7050.5, Coordination of Remedies for Fraud and Corruption Related to Procurement Activities, June 7, 1989
 - (h) DCAA Instruction 7640.16, Reporting Suspected Contractor Fraud and Other Irregularities, February 9, 2006

1. REISSUANCE AND PURPOSE. This regulation assigns responsibilities and provides procedures for monitoring suspected instances of contract fraud, anti-competitive practices, illegal political contributions, violation of the Foreign Corrupt Practices Act, and corruption of Government officials.
2. CANCELLATION. DCAA Regulation 7640.15 dated March 10, 2002 is cancelled.
3. APPLICABILITY AND SCOPE. This regulation applies to all DCAA organizational levels. This regulation covers only contractor fraud or misconduct. Misconduct on the

part of DCAA employees is handled in accordance with DoD Directive 5500.7, Standards of Conduct, incorporating change 1 November 2, 1994 or DoD Instruction 5505.6, Investigations of Allegations Against Senior Officials of the Department of Defense, July 12, 1991.

4. POLICY.

4.1. It is DCAA policy to comply with the fraud detection provisions of DoD and GAO Auditing Standards references (b) and (f) by designing audits which require assessment of compliance with laws or regulations, and which provide reasonable assurance of detecting abuse or illegal acts that could have a material effect on the audit objectives, the financial statements, or results of financial related audits.

4.2. It is DCAA policy to comply with Joint Policy Memorandum Number 2, reference (c) by promptly reporting suspected contractor fraud or other irregularities.

4.3. Audit support to DoD investigative organizations is authorized by DoD Directive 7600.2, reference (a), Joint Policy Memorandum Number 2, reference (c), governs relations with investigative agencies; DCAA also extends its provisions to Department of Justice entities conducting investigations of contract-related irregularities. Requests for audit assistance to such investigations are to be treated as demand assignments. All DCAA employees will cooperate fully with investigators by making relevant information and documents contained in Agency files available to the investigators upon request.

5. RESPONSIBILITIES.

5.1. The Assistant Director, Operations will:

5.1.1. Provide overall coordination of the Agency's efforts to prevent and detect contractor fraud and related irregularities.

5.1.2. Inform the Director and Deputy Director of all significant cases that warrant their attention and apprise them of significant developments as they occur.

5.1.3. Prepare and forward to the DoD Inspector General reports on contract fraud and related matters that are deemed significant as defined in reference (d).

5.1.4. As the Agency fraud monitor, track and monitor the status of all contract fraud cases reported by DCAA through liaison with the cognizant investigative organizations.

5.1.5. Maintain a database of numbered DCAA referrals, including a brief synopsis of each. As requested, provide information, including statistical data, on suspected contract fraud and other cases.

5.1.6. Review matters reported to DCAA through the Defense Hotline, and when there are reasonable grounds to believe a civil or criminal violation may have occurred, assure that such allegations are promptly referred to the appropriate investigative activity for appropriate action.

5.1.7. Monitor cases of particular significance to the Agency for their impact on operations. Based on lessons learned, develop improved audit techniques that will help to disclose similar situations in the future. Identify subjects needing audit policy coverage and communicate the need for appropriate guidance to the Assistant Director, Policy and Plans.

5.1.8. Using the guidance in reference (c), resolve any disputes that may arise between DCAA regions and investigative organizations regarding the assigning of personnel to support investigations or tasks to be performed.

5.1.9. Assure that training materials are developed on fraud and corruption in the procurement process, and that all procurement and procurement-related training includes a period of such instruction when appropriate.

5.2. The Assistant Director, Policy and Plans will:

5.2.1. Issue appropriate guidance regarding those subjects that need audit policy coverage.

5.2.2. Assure that audit policy and procedures do not impede, compromise, or otherwise prejudice pending civil or criminal investigation or litigation.

5.3. Regional Directors and the Director, Field Detachment will:

5.3.1. Implement a continuing training program to maintain auditor awareness of their responsibilities.

5.3.2. Decide, for a contractor with multiple segments, if a suspected fraudulent condition indicates systemic problems that may impact other segments. Assure coordination with other DCAA offices potentially affected giving due consideration to careful handling of sensitive information.

5.3.3. Assure that annual audit plans provide sufficient flexibility for (1) the proper reporting and follow-up of suspected fraud and/or (2) providing support to investigators as required by reference (a).

5.3.4. Provide auditor support to investigators in accordance with reference (c).

5.3.5. Establish procedures, documented by regional instruction, that provide for regional oversight of the timeliness and quality of audit support to investigators.

5.4. FAO Managers and Supervisory Auditors will:

5.4.1. Assure that all auditors are knowledgeable of their responsibilities for detecting and promptly reporting suspected irregularities and prosecution of fraud and that they properly carry out such responsibilities.

5.4.2. Plan and conduct audits in accordance with references (b) and (f).

6. PROCEDURES.

6.1. Reporting Allegations of Fraud Affecting DoD Components. In accordance with the procedures established in reference (h), suspected contractor irregularities shall be reported to the cognizant investigative organization(s).

6.2. Reporting Allegations of Fraud Affecting Non-DoD Organizations.

6.2.1. Suspected fraud or other irregularities affecting a contract awarded by an agency, administration, or department having an Inspector General will be reported to that Inspector General using the procedures in reference (h).

6.2.2. Suspected fraud or other irregularities affecting a contract awarded by an agency, administration, or department that does not have an Inspector General will be reported to the head of the affected agency, administration, department, or designee through Headquarters, (OTS).

7. MARKING DOCUMENTS. Information and documents generated as a result of the activities prescribed above will be marked "FOR OFFICIAL USE ONLY" unless the information warrants a security classification in which case the appropriate security markings will be affixed to the documents.

8. EFFECTIVE DATE. This regulation is effective immediately. Provide copies of any instructions implementing this regulation to Headquarters, Attention: OTS, upon promulgation.

/s/

William H. Reed
Director

DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

OTS

December 23, 2010

DCAA INSTRUCTION
No. 7640.16

**REPORTING SUSPECTED CONTRACTOR FRAUD
AND OTHER CONTRACTOR IRREGULARITIES**

- References:
- (a) DCAAR 7640.15, Detecting, Reporting, and Monitoring Suspected Contractor Fraud and Other Contractor Irregularities
 - (b) DCAA CAM 4-700, Responsibilities for Detection and Reporting of Suspected Irregularities
 - (c) DoD Instruction 5505.15, DoD Contractor Disclosure Program, June 16, 2010
 - (d) U.S. Government Accountability Office Government Auditing Standards (The Yellow Book)

1. **REISSUANCE AND PURPOSE.** This instruction provides procedures for reporting and referring suspected instances of contractor fraud and other contractor irregularities, including labor mischarging, submitting false claims, repeated significant overbilling, falsifying labor charges, improper transfers of costs between contracts, and bribes/kick-backs. It assigns responsibility to (1) auditors for the initiation of reports on suspected contractor fraud and other contractor irregularities; (2) supervisors and Field Audit Office (FAO) managers for the review of such reports, when requested by the auditor; (3) FAO managers for the distribution of such reports, when requested by the auditor; and (4) Headquarters for the review and formal referral of these reports.

2. **CANCELLATION.** DCAA Instruction 7640.16, Reporting Suspected Contractor Fraud and Other Contractor Irregularities, dated February 9, 2006, is cancelled.

3. **APPLICATION AND SCOPE.** This instruction applies to all DCAA organizational levels.

4. POLICY.

4.1. It is DCAA policy that suspected irregularities, whether discovered through audit steps and procedures or by an auditor inadvertently, as in an overheard conversation or disclosed to an auditor either in person or through an anonymous tip, shall be recorded in the audit workpapers and promptly reported to FAO management.

4.1.1. Referrals may be made using the DCAA Suspected Irregularity Referral Form (DCAA Form 2000)(CAM Figure 4-7-2) or the DoD Hotline. The DoD Hotline toll free telephone number is (800-424-9098) and e-mail address is: hotline@dodig.mil. Mailed correspondence to the DoD Hotline should be addressed to the Defense Hotline, The Pentagon, Washington, DC 20301-1900.

4.1.2. When the referral comes from an audit finding or when the auditor has information to supplement that obtained from an external source, the DCAA Form 2000 is preferred because it specifies information needed by investigators and provides for appropriate consideration of the audit impact.

4.2. The following should not be reported using this instruction:

4.2.1. Leads reported by other agencies to investigators and submitted to the auditor for follow-up, including Qui Tam complaints and DoD Hotline referrals (CAM 4-709 and CAM 4-710).

4.2.2. Contractor disclosures made in accordance with the Contractor Disclosure Program (Reference (c)). However, when evaluating the contractor disclosure, if it is determined that the contractor failed to accurately report the disclosed incident, the matter should be reported on the DCAA Form 2000.

4.2.3. Matters reportable under CAM 4-800 – Special Reporting of Unsatisfactory Conditions.

5. RESPONSIBILITIES.

5.1. The Assistant Director, Operations will:

5.1.1. Review each submitted DCAA Form 2000 for completeness and clarity related to the established criteria for irregular activities. Coordinate with Headquarters General Counsel (DL) on all referrals that report suspected corruption of Government officials. Consult with the FAO and DL as necessary to confirm factual or procedural matters.

5.1.2. Assign a case number to each approved DCAA Form 2000 and transmit it with any clarifying analysis to the appropriate recipients. Notify the appropriate regional director, regional investigative support division chief, and FAO manager when a report of fraud or other suspected irregularity is transmitted for investigation and keep the aforementioned recipients advised of significant developments.

5.1.3. Notify the preparer (e.g., auditor) of the DCAA Form 2000 in writing of the reason(s) for a decision to reject a submitted DCAA Form 2000, and advise the preparer of the availability of the DoD Hotline to report the condition if in disagreement with the Headquarters decision.

5.1.4. Notify the investigative organization(s) that received the “early alert” of the decision not to submit a formal Agency referral.

5.2. FAO Managers will:

5.2.1. When requested by the preparer (e.g., auditor) of the DCAA Form 2000, promptly review materials submitted in support of allegations of unlawful activity to ensure clarity and discuss with the auditor and supervisor, if necessary to fully understand the basis of the allegation. No attempt should be made to dissuade an auditor from completing and submitting a DCAA Form 2000.

5.2.2. Expedite the accumulation of any additional information.

5.2.3. Notify DCAA regional representatives of fraud suspicions as required by regional instructions.

5.2.4. Notify the Regional Director if a multiple segment contractor is suspected of having systemic fraudulent conditions that might impact other segments.

5.2.5. When requested by the preparer (e.g., auditor) of the DCAA Form 2000, distribute the DCAA Form 2000 to the Justice Liaison Auditor and the “early alert” to the local unit of the appropriate investigative organization as required in Sections 6.1.2. and 6.1.4. of this instruction.

5.2.6. Notify the Justice Liaison Auditor of significant events regarding outstanding referrals, for example, indictment, conviction, etc.

5.2.7. Notify the Administrative Contracting Officer (ACO) of Headquarters decisions against issuing formal referrals.

5.3. The Supervisory Auditor will:

5.3.1. When requested by the preparer (e.g., auditor) of the DCAA Form 2000, review each DCAA Form 2000 submitted by an assigned auditor for clarity and to determine that it is complete, it has been followed-up through audit to the extent possible, and it is not a matter already known to the Government. No attempt should be made to dissuade an auditor from completing and submitting a DCAA Form 2000.

5.3.2. Promptly obtain any additional information needed to satisfactorily complete the DCAA Form 2000.

5.4. Auditors encountering or receiving information that raises a reasonable suspicion of fraud or other unlawful activity:

5.4.1. May discuss the apparent unlawful activity with the supervisor, FAO manager and the Regional Investigative Support Division to determine whether a DCAA Form 2000 should be prepared. Such discussions, however, should not in any way impede the auditor from forwarding a potential unlawful activity referral.

5.4.2. Prepare a DCAA Form 2000 when the situation meets the criteria for a fraud referral (i.e., contains information which suggests a reasonable basis for suspicion of fraud, corruption, or unlawful activity affecting Government contracts). It is recommended that the DCAA Form 2000 be submitted to FAO management to review for clarity and to determine that it is complete.

5.4.3. Adequately describe the unlawful activity, keeping in mind the need for conciseness, including appropriate references to procurement regulations or statutes, if any, which the auditor believes may have been violated. General reference is sufficient (i.e., the auditor is not expected to conduct legal research to identify citations). Report any contractor efforts to hinder or obstruct audit work that uncovered the suspected unlawful activity (see CAM 4-708).

5.4.4. Continue with assigned duties and pursue development of factual information as appropriate/required by reference (b) above. Any continuing review must be coordinated with the supervisor or the FAO manager.

5.4.5. Prepare a DCAA Form 2000 when warranted by disclosures arising from additional audit effort.

6. PROCEDURES:

6.1. Submission of a DCAA Form 2000 from an acceptable referral as follows:

6.1.1. Use Enclosure 1 to determine the appropriate DoD investigative organization to send the "early alert." If uncertain where to send the "early alert," contact the Justice Liaison Auditor

for guidance. Field Detachment “early alerts” should be coordinated with the Field Detachment Investigative Support Division.

6.1.2. For unclassified referrals - Encrypt an e-mail, attaching the dated and signed DCAA Form 2000 in an Adobe Acrobat “pdf” file (no Word or Excel files) and send to Headquarters, Justice Liaison Auditor, at the following address: “DCAA HQ JLA” or mail to Headquarters, Attention: Justice Liaison Auditor, using regular first-class mail.

6.1.3. For Field Detachment referrals – Encrypt an e-mail, attaching the dated and signed DCAA Form 2000 in an Adobe Acrobat “pdf” file (no Word or Excel files) and send to Field Detachment, Investigative Support Division at the following address: “FD ISD”. The Field Detachment Investigative Support Division will distribute the DCAA Form 2000 to the appropriate investigative organization.

6.1.4. Mark an additional copy of the DCAA Form 2000 “early alert” and promptly send it using registered mail, return receipt requested, to the local unit of the appropriate investigative organization. The transmittal memorandum, signed by the FAO manager, should state that unless advised to the contrary within five days of receipt, a copy of the DCAA Form 2000 will be furnished to the ACO or Procuring Contracting Officer for defective pricing issues. (See Enclosure 2). Do not give contracting representatives suspected of involvement in the unlawful activity a copy of the DCAA Form 2000. In this case, contact the Justice Liaison Auditor for guidance.

6.2. MARKING OF DOCUMENTS. Information and documents generated as a result of the activities prescribed above will be marked “FOR OFFICIAL USE ONLY” unless the information warrants a security classification, in which case the appropriate security markings will be affixed to the documents.

7. EFFECTIVE DATE. This instruction is effective immediately. Copies of any instructions implementing this instruction shall be provided to Headquarters, Attention: Justice Liaison Auditor upon promulgation.

FOR THE DIRECTOR:

/s/
Nina I. S. Kissinger
Deputy Assistant Director
Operations

Enclosures:

Investigative Responsibility for Allegations of Fraud
Pro Forma Early Alert Memorandum

ENCLOSURE 1

Investigative Responsibility for Allegations of Fraud

Early alerts should be sent to investigators as follows:

Contracts

<u>Awarded By</u>	<u>Administered By</u>	<u>Investigative Responsibility</u>
Military Departments	DCMA	Joint DCIS and MCIO
Defense Logistics Agency	DCMA	DCIS
Military Departments	Military Departments	MCIO

Exceptions to Basic Referral Policy: If any of the following organizations are involved in the contracts to which the allegations of fraud are related, contact the DCAA Justice Liaison Auditor prior to issuing any early alert:

1. Defense Agencies other than DLA
2. Defense Fuel Supply
3. Defense Reutilization and Marketing Service
4. Department of Defense Dependent Schools
5. Joint Chiefs of Staff
6. Naval Facilities Engineering Command
7. Non-DoD Government Departments and Agencies
8. North Atlantic Treaty Organization (NATO)
9. Office of the Secretary of Defense
10. Special Operations Forces Low Intensity Conflicts (SOFLIC)
11. Strategic Defense Initiative Organization (SDIO)
12. U.S. Army Corps of Engineers (USACE)

Acronyms:

DCMA	Defense Contract Management Agency
DCIS	Defense Criminal Investigative Service
MCIO	Military Criminal Investigative Organization (i.e., Army Criminal Investigative Command, Naval Investigative Service, Air Force Office of Special Investigations)

ENCLOSURE 2

Pro Forma Early Alert Memorandum

MEMORANDUM FOR (Name and address of appropriate investigative organization)

SUBJECT: Early Alert of a Suspected Irregularity Referral Relating to (state the subject of the referral, for example, Possible Labor Mischarging at ABC Company)

The attached Suspected Irregularity Referral Form (DCAA Form 2000) provides information that suggests a reasonable basis for suspicion of fraud, corruption, or other unlawful activity affecting Government contracts. (Add any additional comments as appropriate.) Unless you advise us to the contrary within five days of your receipt of this notice, we will furnish a copy of the attached DCAA Form 2000 to the cognizant (Select either: i) administrative contracting officer or ii) procuring contracting officer for defective pricing issues). We are available to discuss this matter at your earliest convenience and we can be reached at (telephone number).

(Signature)

Branch Manager/Resident Auditor

FOR OFFICIAL USE ONLY



DEFENSE CONTRACT AUDIT AGENCY
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

PAS

December 19, 2008

DCAA INSTRUCTION
NO. 7640.17

**FORMAL REPORTING PROCEDURES FOR
DENIAL OF ACCESS TO CONTRACTOR'S RECORDS
(RCS: PAS AR/SA - 188)**

References: (a) DCAA Regulation 5500.5, Subpoenas of Defense Contractor Records (Available on DCAA's Intranet Site)
(b) CAM 1-504, Access to Records of Contractor (Available on DCAA's Intranet Site)

1. REISSUANCE AND PURPOSE. To establish the procedure for formal reporting to Headquarters, Policy and Plans, of contractor denial of access to records. This reporting procedure precedes the subpoena procedures that are cited in DCAA Regulation 5500.5, referenced above and supplements the referenced CAM guidance.
2. CANCELLATION. DCAAI 7640.17, "Formal Reporting Procedures for Denial of Access to Contractor's Records," dated February 10, 2006 is cancelled.
3. APPLICABILITY AND SCOPE. This instruction applies to all DCAA organizational elements.
4. POLICY.
 - 4.1. DCAA auditors must adhere to generally accepted government auditing standards in determining what comprises competent, relevant, and sufficient evidential matter to form and express an audit opinion on a contractor's proposed or incurred costs. A contractor's refusal to provide all records required to audit in accordance with these standards will formally be reported as a denial of access to records.
 - 4.2. This instruction provides the procedure for formally reporting denials of access to records.
5. RESPONSIBILITIES.
 - 5.1. The Assistant Director, Policy and Plans, is responsible for:

5.1.1. Monitoring formal denial of access to records issues received from the regional offices, and taking appropriate follow-up action to ensure timely pursuit of access.

5.1.2. Providing guidance to the field as required to resolve denial of access to records.

5.1.3. Providing semiannual status reports to the Director on access to records activity reported by the regions.

5.1.4. Processing subpoena requests in accordance with DCAA Regulation 5500.5.

5.2. Regional Directors are responsible for:

5.2.1. Making every possible effort to resolve denial of access to records issues with contractors' top management, concurrently with efforts taken by the FAO, RAM, RSPM, ACO/PCO, and CAC.

5.2.2. Monitoring FAO reported denials of access to contractor records (Enclosure 1).

5.2.3. Submitting semiannual reports (Enclosure 2) to Headquarters that summarize denials of access to records reported to the region by FAOs. The reports are due on the 15th of April and October each year. This reporting requirement is assigned reports control symbol RCS: PAS AR/SA - 188.

5.2.4. Coordinating, processing, and forwarding FAOs' subpoena requests to Headquarters, Policy and Plans (Attn: PAS) in accordance with DCAA Regulation 5500.5.

5.2.5. Withdrawing requests for subpoenas when records are received or no longer required.

5.3. FAO Managers and Supervisory Auditors are responsible for:

5.3.1. Assuring that auditors are knowledgeable of their rights and responsibilities concerning access to contractor records.

5.3.2. Maintaining close coordination with the contractor, ACO, PCO, and CAC, and keeping the regional office currently informed on the status of reported denial of access to records.

5.3.3. Submitting to the regional office the initial and, thereafter as applicable, calendar quarterly reports (Enclosure 1) that summarize the status of reported denials of access to contractor records.

5.4. CAC/CHOA Auditor. If the contractor's denial of access to records is based on corporate policy, the CAC or CHOA should take action to resolve the issue. The results of these efforts must be submitted to each affected FAO, with copies to the appropriate regional offices.

6. PROCEDURES.

6.1. When an auditor requests supporting data/documentation from a contractor (either verbally or informally in writing), the request should clearly state what support is needed and when it should be provided. The contractor should be provided a reasonable time period to provide the data given the specific circumstances. Generally, data/documentation supporting the contractor's assertion should be readily available. Therefore, unless the request requires analysis by the contractor, or there are extenuating circumstances (e.g., the request is for a voluminous amount of data or for data stored at an off-site location), the contractor should provide the data upon request. If the request does require analysis or if extenuating circumstances exist, auditors should allow the contractor additional time deemed necessary to provide the requested documentation.

6.2. If the contractor does not provide the requested information by the requested due date, and the contractor has not provided an appropriate explanation for the delay, the FAO should prepare a formal written request to the contractor stating that the information must be provided by a specific date (not to exceed one week). This written request should be initiated as soon as the due date is missed, and no later than five days after the due date. (See 6.7 for accelerated procedures for price proposal reviews.)

6.3. Written requests should be addressed to the appropriate high-level contractor management (i.e., at a level no lower than the business segment vice president or chief financial officer) with a copy to the contracting officer.

6.4. When the auditor is convinced that the requested data will not be provided based on (1) a categorical denial reply from the contractor (oral or written), or (2) the contractor's failure to provide the data or an appropriate explanation within the one-week period specified in paragraph 6.2. above, the following steps should be taken simultaneously:

6.4.1. Notify the contractor (via a letter signed by the FAO manager) that a formal denial to records exists and is being reported to appropriate government personnel.

6.4.2. Write to the ACO and CAC to request their assistance in resolving the access problem. The request should include a description of the denied data, why the data are needed, the cost impact related to the denial of access, if known, and the actions taken by DCAA to gain access. A copy of the notification to the contractor should be attached.

6.4.3. Prepare and forward to the regional office a Denial of Access to Contractor Records (see Enclosure 1). At the completion of the regional review, the form should be forwarded to DCAA, Headquarters ATTN: PAS. This submission is controlled as RCS:PAS AR/SA - 188.

6.4.4. Thoroughly document the file. Documentation may consist of a contractor letter to the auditor or a copy of a letter from the auditor to the contractor. Although a statement signed by the authorized contractor official is preferable, this must not impede the other needed actions. Therefore, the auditor may document the contractor's position in a letter to the contractor.

6.5. If the efforts of the FAO, ACO, CAC and regional office prove unsuccessful, the Regional Director should review the matter to determine if a subpoena should be requested. This review may include informal consultations with the Assistant Director, Policy and Plans, and the General Counsel, DCAA.. If it is resolved in these discussions that a subpoena is the appropriate means to comply with the Agency policy cited in paragraph 4. above, then the FAO should prepare and submit to the regional office a request for a subpoena of the required records in accordance with DCAA Regulation 5500.5. If the documents necessary for audit cannot be obtained using DCAA's subpoena authority (10 U.S.C. 2313(b)), DCAA should work with the DoDIG to issue an IG subpoena using their broad subpoena authority.

6.6. If the auditor either obtains access to the records in question or determines that further action is not warranted, he or she must advise all officials previously contacted in the preceding steps.

6.7. Accelerated Procedures in Price Proposal Reviews:

6.7.1. The most effective means of obtaining access to records needed for the review of price proposals is to promptly refer the matter to the PCO for action as stipulated by FAR 15.404-2 (d).

6.7.2. Frequently, when auditing a price proposal, time does not permit accomplishing all the steps exactly as set forth above. In these cases the formal request may only provide the contractor 1 to 3 days to respond and the other parties affected can be contacted by telephone or e-mail.

6.7.3. If the accelerated procedures are unsuccessful, the matter may be referred to the regional director by telephone or e-mail. Similarly, the regional director's efforts, including notification of Headquarters, may be accomplished by telephone or e-mail.

6.7.4. All actions accomplished by telephone should be confirmed in writing.

6.7.5. Forward pricing audit reports issued prior to satisfactory resolution of a denial of access to records should follow CAM 10-304.4 guidance.

7. EFFECTIVE DATE. This instruction is effective immediately.

FOR THE DIRECTOR:

/Signed/
Kenneth J. Saccoccia
Assistant Director
Policy and Plans

Enclosures - 2

1. Denial of Access to Contractor Records (Data Sheet)
2. Denial of Access to Records Status Report

DENIAL OF ACCESS TO CONTRACTOR RECORDS
(DATA SHEET)
RCS: PAS AR/SA - 188

TO: Regional Office, ATTN: Special Programs

FAO: _____

RORG CODE: _____

CONTRACTOR: _____

_____ INITIAL REPORT _____ INTERIM REPORT _____ DISPOSITION REPORT

DATE OF DENIAL: _____

DISPOSITION DATE: _____

AUDIT BEING PERFORMED/ASSN NO: _____

RECORD SOUGHT: _____

AUDITOR RATIONALE FOR REQUESTING ACCESS: _____

CONTRACTOR RATIONALE FOR DENIAL: _____

FAO MANAGER _____ DATE: _____

ATTACHMENTS:

- _____ Original written request
- _____ Contractor's written denial
- _____ Letter to ACO, PCO
- _____ CAC correspondence
- _____ Correspondence with contractor
- _____ Other - Identify

DISTRIBUTION:

- Original - Regional Office, SP
- Copy 1 - RAM
- Copy 2 - W/P File
- Copy 3 - CAC (if necessary)

DENIAL OF ACCESS TO RECORDS STATUS REPORT

AS OF _____

RCS: PAS AR/SA - 188

TO: HEADQUARTERS, PAS

FROM: _____ REGION

FAO & RORG CODE: _____

CHECK STATUS: NEW (), UPDATE (), RESOLVED (A ^{1/}____, C ____, DATE _____)

AUDIT ASSN. NO. AND DESCRIPTION: _____

RECORD SOUGHT: _____

DATE OF DENIAL: _____

CONTRACTOR & CONTRACTOR ID: _____

CONTRACTOR LOCATIONS INVOLVED: _____

AUDITOR RATIONALE FOR REQUESTING ACCESS: _____

CONTRACTOR RATIONALE FOR DENIAL: _____

CHRONOLOGY OF DATES AND EVENTS: ^{2/}_____

^{1/} A-Accessed, C-Resolved w/o access

^{2/} Synopsise all communication between the contractor and
Government representatives, and the status for resolution.