Description of document:	National Archives and Records Administration (NARA) Office of Inspector General (OIG) Office of Audits (OA) Policy Manual, September 2016
Requested date:	06-January-2017
Released date:	19-January-2017
Posted date:	30-January-2017
Source of document:	FOIA Request National Archives and Records Administration Office of the Inspector General FOIA Request 8601 Adelphi Road, Room 1300 College Park, MD 20740 Fax: 301-837-3197

NATIONAL ARCHIVES

OFFICE *of*
INSPECTOR GENERAL

January 19. 2017

Via email

Re: Request for NARA OIG Audit Manual and Investigation Manual (NARA OIG FOIA 17-10)

This letter is in response to your letter, received January 6, 2017 requesting "the NARA OIG Audit Manual and … the NARA OIG Investigation Manual." The National Archives and Records Administration (NARA) Office of Inspector General (OIG) does have an "OIG Investigation Manual" but instead has a Special Agent Handbook released to you under NARA OIG FOIA 17-09. The NARA OIG does have an Office of Audits Policy Manual which appears to be responsive to your request for an Audit Manual. It is attached.

If you have a dispute with this response, you may contact the OIG's FOIA Public Liaison, James Springs, for assistance at:

National Archives and Records Administration
Office of Inspector General
8601 Adelphi Road, Room 1300
College Park, MD 20740-6001
 (301) 837-3018
james.springs@nara.gov

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

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road–OGIS
College Park, MD 20740-6001
ogis@nara.gov
ogis.archives.gov
202-741-5770 or 1-877-684-6448

Finally, in accordance with Department of Justice guidance, I would also like to notify you that Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. *See* 5 U.S.C. 552(c) (2006 & Supp. IV 2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification given to all our requesters and should not be taken as an indication excluded records do, or do not, exist.

If you have any questions, you may contact me at 301-837-1966 or john.simms@nara.gov. Thank you for contacting the NARA OIG.

Sincerely,

John Simms
Counsel to the Inspector General
Office of Inspector General
National Archives and Records Administration

OFFICE of
INSPECTOR GENERAL
NATIONAL ARCHIVES

OFFICE OF AUDITS
POLICY MANUAL
SEPTEMBER 2016

TABLE OF CONTENTS

September 2016

Contents

CHAPTER 1 – OIG PLANNING PROCESS

1. POLICY

The planning process is considered an essential part of the Office of Inspector General (OIG) management process. OIG policy is to provide adequate coverage of NARA programs and operations through a systematic planning process.

Quality Standards for Federal Offices of Inspector General, published by the President's Council on Integrity and Efficiency (PCIE) in October 2003, requires each OIG to maintain a planning system for assessing the nature, scope, trends, vulnerabilities, special problems, and inherent risks of agency programs and operations and for establishing the goals, objectives, and tasks to be accomplished by the OIG within a specific time period.

2. UNIVERSE OF NARA PROGRAMS AND OPERATIONS

The OIG maintains an up-to-date universe of NARA programs and operations subject to review. Using NARA's Strategic Plan as a guide, the OIG develops the universe of programs and operations, based on the Strategic Plan's goals and objectives, the strategies to be pursued for achieving the agency's goals and objectives, and the targets for determining how well the agency is achieving its goals and objectives. In addition, to help update the universe, other documentation such as the NARA budget, mission and function statements, vulnerability assessments, organization charts, etc., may be reviewed. The next step in the process is to assign review priorities. When completed, the results of this exercise will be used to update the OIG's Strategic Plan and to prepare the annual OIG Work Plan. Coverage of NARA programs and operations will be based on priorities and available OIG resources.

Annually, the first step in the OIG planning process is to update the universe of NARA programs and operations, if needed, reflecting any changes to the agency's Strategic Plan.

3. ANNUAL WORK PLAN

An annual OIG Work Plan will be prepared which identifies the audits, attestation engagements, nonaudit services, and fraud prevention activities planned for NARA's programs and operations.

1. Financial Audits. The OIG utilizes financial audits for independent assessments of and reasonable assurance about whether an entity's reported financial condition, results, and use of resources are presented fairly in accordance with recognized criteria. Reporting on financial audits performed in accordance with generally accepted government auditing standards (GAGAS) also includes reports on internal control, compliance with laws and regulations, and provisions of contracts and grant agreements as they relate to financial transactions, systems, and processes. Financial audits performed under GAGAS include financial statement audits and other related financial audits.

   a. Financial Statement Audits. The primary purpose of a financial statement audit is to provide reasonable through an opinion (or disclaim an opinion) about whether an entity's financial statements are presented fairly in all material respects in conformity with generally accepted accounting principles (GAAP), or with a comprehensive basis of accounting other than GAAP.

   b. Other Types of Financial Audits. These audits provide for different levels of assurance and entail various scopes of work, including: (a) providing special reports, such as for specified elements, accounts, or items of a financial statement; (b) reviewing interim financial information; (c) issuing letters for underwriters and certain other requesting parties; (d) reporting on the controls over processing of transactions by service organizations; and (e) auditing compliance with regulations relating to federal award expenditures and other governmental financial assistance in conjunction with, or as a by-product of, a financial statement audit.

2. <u>Performance Audits</u>. Performance audits are engagements that provide assurance or conclusions based on an evaluation of sufficient, appropriate evidence against stated criteria, such as specific requirements, measures, or defined business practices. Performance audits provide objective analysis so that management and those charged with governance and oversight can use the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability. Performance audit objectives may vary widely and include assessments of program effectiveness, economy, and efficiency; internal control; compliance; and prospective analyses.

3. <u>Attestation Engagements</u>. Attestation engagements can cover a broad range of financial or nonfinancial objectives and may provide different levels of assurance about the subject matter or assertion depending on the users' needs. Attestation engagements result in an examination, a review, or an agreed-upon procedures report on a subject matter or on an assertion about a subject matter that is the responsibility of another party. There are three types of attestation engagements.

   a. <u>Examination</u>. Consists of obtaining sufficient, appropriate evidence to express an opinion on whether the subject matter is based on, or in conformity with, the criteria in all material respects or the assertion is presented, or fairly stated, in all material respects, based on the criteria.

   b. <u>Review</u>. Consists of sufficient testing to express a conclusion about whether any information came to the auditors' attention on the basis of the work performed that indicates the subject matter is not based on (or not in conformity with) the criteria or the assertion is not presented (or not fairly stated) in all material respects based on the criteria.

   c. <u>Agreed-Upon Procedures</u>. Consists of specific procedures performed on a subject matter.

4. <u>Nonaudit Services</u>. Nonaudit services are professional services that are not performed in accordance with GAGAS. These services are often performed

in response to a statutory requirement, at the discretion of the authority of the audit organization, or for a legislative oversight body or an independent external organization and do not impair auditor independence. These services include: (1) providing information or data to a requesting party without auditor evaluation or verification of the information or data; (2) developing standards, methodologies, audit guides, audit programs, or criteria for use throughout the government or for use in certain specified situations; (3) collaborating with other professional organizations to advance auditing or government entities and programs; (4) developing question and answer documents to promote understanding of technical issues or standards; (5) providing assistance and technical expertise to legislative bodies or independent external organizations and assisting legislative bodies by developing questions for use at a hearing; (6) providing training, speeches, and technical presentations; (7) developing surveys, collecting responses on behalf of others, and reporting results as "an independent third party"; (8) providing oversight assistance in reviewing budget submissions; (9) contracting for audit services on behalf of an audited entity and overseeing the audit contract, as long as the overarching principles are not violated and the auditor under contract reports to the audit organization and not to management; (10) identifying good business practices for users in evaluating program management system approaches, including financial and information management systems; and (11) providing audit, investigative, and oversight-related services that do not involve a GAGAS audit.

5. <u>Fraud Prevention Activities</u>. Fraud prevention activities include fraud prevention surveys and fraud awareness briefings. Fraud prevention surveys identify crime-conducive and systemic weaknesses in management controls within NARA units and facilities. Fraud awareness briefings increase NARA employees' awareness of fraud and fraud indicators.

The annual OIG Work Plan will include the following elements:

(a) NARA programs and operations selected for review and evaluation, with priorities and specific reasons for selection;

(b) scope and locations to be reviewed;

(c) anticipated benefits to be obtained from the review; and

(d) staff hours and other resources needed to perform the review.

Audit and evaluation suggestions should be submitted to the Assistant Inspector General for Audit (AIGA) during the year, as they are identified. After review by the AIGA and the IG, accepted suggestions will be incorporated into the annual audit planning process.

The IG will issue, by July 1, a request for audit suggestions to all office heads, staff directors, and directors of Presidential libraries and regional records services centers. As appropriate, the suggestions and comments of senior agency officials are integrated into the OIG's Work Plan. The final work plan is then approved by the IG. After IG approval, the plan is posted on the NARA OIG Web Site, and sent as e-mail to appropriate offices throughout the agency.

By September 30th, the annual OIG Work Plan should be completed and issued. The plan is flexible and may be changed during the year, to assign limited audit resources to higher-priority audits. The IG, in conjunction with the AIGA, shall determine the priority for conducting reviews.

6. Organizational Independence. The IG Act, as amended provides safeguards that we are independent from the agency. The IG Act as amended prevents the agency from interfering with our ability to perform the work and report the results impartially.

Contents

CHAPTER 2 – AUDIT PROCESS

1. AUDIT PROCESS

Audits conducted by the OIG generally progress through an audit process that includes the following:

(a) audit planning;

(b) audit guide preparation,

(c) audit announcement (see Attachment 2-1),

(d) entrance conference with the cognizant office head and staff,

(e) audit field work,

(f) exit conference with the office head and staff,

(g) draft audit report sent to the office head(s) for comment,

(h) final audit report sent to the Archivist,

(i) implementation of recommendations by the cognizant offices, and

(j) OIG follow-up reviews of corrective actions taken by management.

NARA 1201, *Audits of NARA Programs and Operations*, contains information about management and OIG responsibilities related to audits of NARA programs, activities, and functions; types of audits; audit planning; OIG audit process; and management response to OIG audit reports. (See Attachment 2-6)

TeamMate Electronic Work Papers (EWP) is an audit management system supported by Wolters Kluwer that will be our standard application for documenting our projects. While TeamMate does not replace performing the detailed work, it does provide a common platform for documenting, reviewing and sharing work during and after the project.

The AIGA will assign staff with adequate professional competence to perform the audit. The AIGA will base this decision on the auditor's knowledge, skills and experience appropriate for the audit. If the AIGA decides to use the work of a specialist, the nature and scope of the work should be documented.

2. AUDIT PLANNING

In planning an audit, the auditor should obtain pertinent information on the operation of the program, activity, or function. The principal purpose of planning is to gather information to assess risk within the context of the audit objectives. The information obtained during planning should be sufficient and adequate to justify a determination whether to continue into a detailed audit or terminate the audit with a close-out letter.

Standard audit steps for planning an audit have been established in TeamMate EWP and will automatically populate Folder A: Planning in every audit using TeamMate EWP. Folder A will document the following information related to information gathered on background, criteria and internal control on the audit subject. The auditor will gain the following information for purposes of assessing audit risk and planning the audit within the context of the audit objectives. At a minimum, the auditor will gather information to:

- Gain an understanding of the nature and profile of the programs and the needs of potential users of the audit report.
- Gain an understanding of the information systems controls for purposes of assessing audit risk and planning the audit within the context of the audit objectives.
- Gain an understanding of the results of previous audits and attestation engagements that directly relate to the current audit objectives.
- Identify sources of audit evidence and determine the amount and type of evidence needed given audit risk and significance. The strength and weakness of each form of evidence depends on the facts and circumstances associated with the evidence and professional judgment in the context of the audit objectives.
- Determine whether to use the work of other auditors and experts to address some of the audit objectives.
- Gain an understanding of the legal and regulatory requirements relevant to this audit.
- Gain an understanding of other requirements, such as contract provisions or grant agreements relevant to audit.
- Gain an understanding of internal controls as it relates to this audit.

The information gathered in planning will assist the auditor in developing the audit guide.

In planning the audit, auditors should assess risks of fraud occurring that is significant within the context of the audit objectives. Audit team members should consider fraud risks, including factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud. Auditors should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect the findings and conclusions.

When auditors identify factors or risks related to fraud that has occurred or is likely to have occurred that they believe are significant within the context of the audit objectives, they should design procedures to provide reasonable assurance of detecting such fraud. Assessing the risk of fraud is an ongoing process throughout the audit and relates not only to planning the audit but also to evaluating evidence obtained during the audit.

When information comes to the auditors' attention indicating that fraud that is significant within the context of the audit objectives may have occurred, auditors should extend the audit steps and procedures, as necessary, to (1) determine whether fraud has likely occurred and (2) if so, determine its effect on the audit findings. If the fraud that may have occurred is not significant within the context of the audit objectives, the auditors may conduct additional audit work as a separate engagement, or refer the matter to other parties with oversight responsibility or jurisdiction.

If the auditor believes it is likely that sufficient, appropriate evidence will not be available, they may revise the audit objectives or modify the scope and methodology and determine alternative procedures to obtain additional evidence or other forms of evidence to address the current audit objectives. The auditor should also evaluate whether the lack of sufficient, appropriate evidence is due to internal control deficiencies or other program weaknesses, and whether the lack of sufficient appropriate evidence could be the basis for

audit findings.

At the completion of audit planning, the audit staff should have gained sufficient information to identify the potential findings and determine the need for, and the areas to be covered in, subsequent audit work. A Go No Go meeting will be held with the AIGA to determine the need for, and the areas to be covered in, subsequent audit work. The results of the Go No Go meeting include:

(a) <u>Proceed with the Field Work</u>. An audit guide should be developed, detailing the audit steps, setting milestones for the field work, and developing and quantifying the potential deficiency areas identified and documented during the survey. The reasons for continuing should be fully justified, and the staff should update the Project Management Report reflecting new dates, staffing needs, etc.; and hold another entrance conference with appropriate officials of the entity being audited to advise them of the decision and the detailed audit and reporting process.

(b) <u>Issue a Management Letter</u>. A management letter should be issued to appropriate officials describing findings that are fully developed with conclusions and recommendations for corrective actions. An exit conference will be held with the appropriate NARA officials advising them of the decision, and obtaining comments and clarifications on the matters to be reported.

(c) <u>Cancel the Audit</u>. A close-out memorandum should be issued terminating the audit and advising appropriate NARA officials that no further work is contemplated. The IG must approve all project cancellations.

At the AIGA's discretion, a survey, a more in depth planning process of gathering data on the subject area, may be performed. A more in depth planning process is Surveys; which are commonly performed for areas being audited for the first time or where the OIG does not have a lot of information on the subject area. The objective, survey planning steps and outcome of the planning a survey will be defined when outlining the planning process survey. For example, the outcome of the planning steps a survey could be a 'issues'

table reflecting weaknesses identified and mitigated as well as weaknesses
identified and not yet mitigated.

3. AUDIT GUIDE
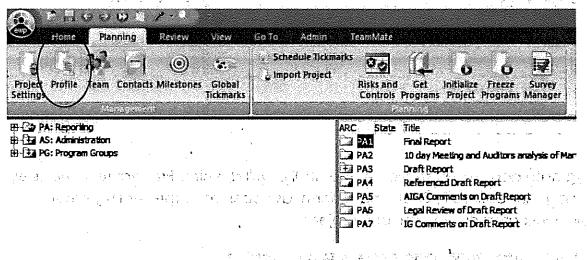
For each project, the auditor(s) will prepare a written audit guide. The audit
guide should contain the following information:
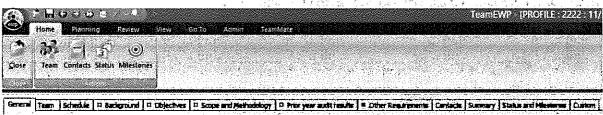
(a) title of the audit and project number;
(b) background information about the assignment and the significance of
 the issue and the audited entity that can help the auditors understand
 and carry out the audit guide;
(c) audit objectives, scope, and methodology;
(d) milestone dates (e.g., start date, report date, etc.);
(e) staff hour estimates;
(f) requirements such as travel, contracted audit services, or use of
 consultants and specialists; and
(g) steps/guidance to accomplish the audit objectives.
(h) for performance audits, design audit procedures to provide assurance
 that significant illegal acts will be detected and that the risk of illegal acts
 be assessed.
(i) for financial audits, design the audit to provide reasonable assurance of
 detecting misstatements that result from violations of provisions of
 contracts or grant agreements and could have a direct and material
 effect on the determination of financial statement amounts or other
 financial data significant to the audit objectives.

The AIGA, who is the approving official for the audit guide, must sign and date
the document. The auditor should provide the AIGA the audit guide for
approval when the guide is complete. The audit guide should be complete
before a significant amount of fieldwork is performed. Those responsible for
performing the effort should use the audit guide to monitor, control, and redirect
resources toward accomplishment of the audit objectives. The audit guide may
need to be revised in response to unforeseen events or problems. Under these
circumstances, any changes to the audit guide must be approved by the AIGA.

TeamMate EWP provides a method for documenting the above items in the EWP audit file. After an EWP audit has been set up, use the Profile section to document the subject audit title, project number, background, objectives, scope, methodology, milestone, staff hour estimates, requirements such as travel, contracted audit services, or use of consultant and specialist.
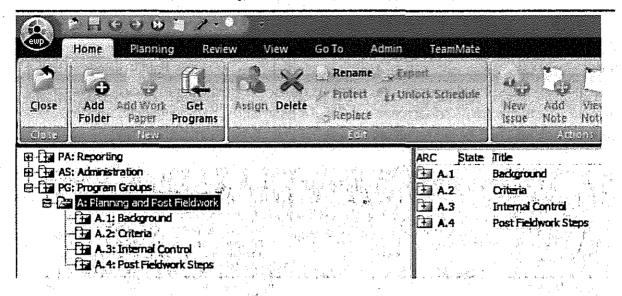
This information can be developed as the auditor completes GAGAS field work standards for performance audits. Standard audit steps have been established in the A.1, A.2 and A.3 folders consisting of planning steps to ensure each audit is adequately planned. Auditors will develop their audit guide and specific audit steps based on the work done in sections A.1 through A.3 as they document their understanding of the subject audit and develop audit steps necessary to address the audit objectives.
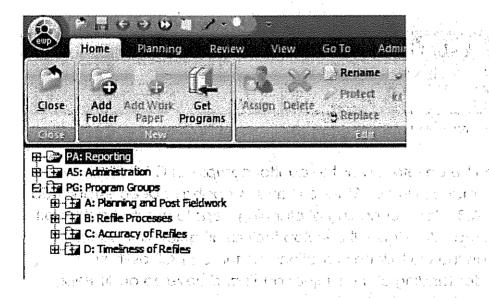
Using data acquired in section A, the auditor will develop Procedure Summaries and steps in sections B, C, D, and so forth, as necessary, representing each major work area or segment of a project.
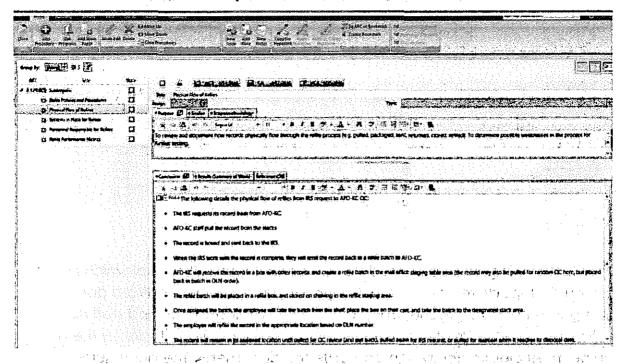
Each Procedure Summary, i.e. B.1.PS, representing each major work area or segment of a project. The steps within each Procedure Summary are necessary to complete to address the objectives of the audit. The auditor will summarize the results of the work performed for each step. See Chapter 4, number 5 of the

NARA OIG audit manual for more information of what needs to be included in summarizing work paper sections.

The auditor will generate an Audit Guide using the reporting tool which pulls all the audit steps developed in the Procedure Summaries into a Word document, along with the background, objectives, scope methodology and staff hour estimates from the Profile. The AIGA, who is the approving official for the audit guide, must electronically sign and date the document. The audit guide, located at AS2.b will document the approved audit guide. The auditor will use the Procedure Summaries as the audit guide to monitor, control, and redirect resources toward accomplishing the audit objectives. The audit guide may need to be revised in response to unforeseen events or problems. Under these circumstances, any changes to the audit guide must be approved by the AIGA.
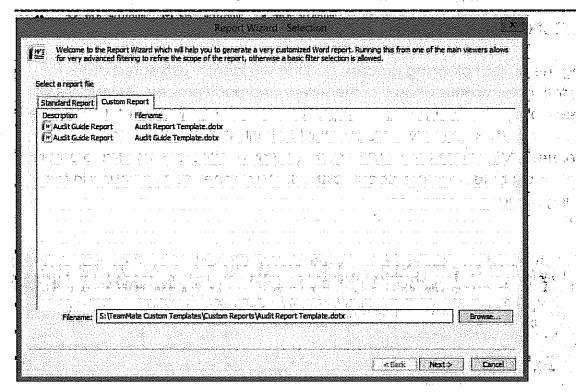
To generate the Audit Guide, select the Review menu. Generate Report.

The following dialog box will appear

Welcome to the Report Wizard which will help you to generate a very customized Word report. Running this from one of the main viewers allows for very advanced filtering to refine the scope of the report, otherwise a basic filter selection is allowed.

Select a report file

| Standard Report | Custom Report |

Description	Filename
Audit Guide Report	Audit Report Template.dotx
Audit Guide Report	Audit Guide Template.dotx

Filename: S:\TeamMate Custom Templates\Custom Reports\Audit Report Template.dotx   Browse...

< Back   Next >   Cancel

Select filename: Audit Guide template. The File Name should default to your S:\TeamMate Custom Templates\Custom Reports folder. Click Next.
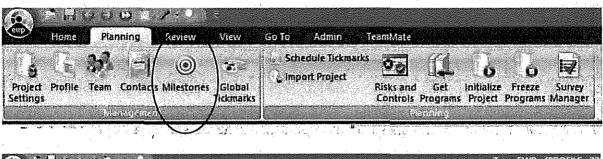
Select AS2 to save the Audit Guide at this location or save external to the audit file. Click Finish.
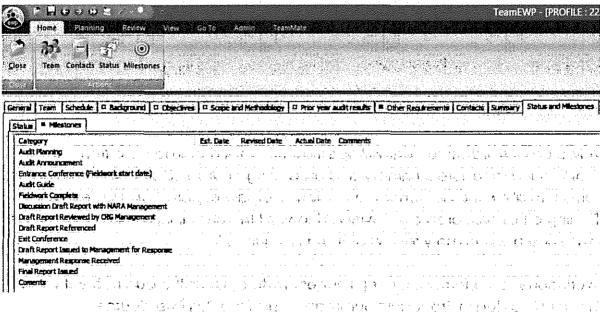
A Microsoft Word document will open as a file in AS2 pulling data from the Profile and Procedure Summary and producing an Audit Guide in a reviewable format to allow the document to be signed off as prepared and reviewed. Signing off as prepared and reviewed toward the beginning of the audit shows evidence of supervisory review of the audit guide.

Work done to perform audit steps necessary to address the audit objectives will be documented in Procedure Summaries using the Purpose, Source, Scope/methodology, Conclusion and Results fields and supported by and referenced to other work papers (See Chapter 4).

4. PROJECT MANAGEMENT REPORT

During the project planning process, auditors will identify estimated dates for completing the various phases of the survey and audit process. Milestones will be used to identify the planned completion dates and will be updated, as the project progresses, to show the dates that the milestones are actually completed. Milestones are used to monitor a project's progress and to ensure that all applicable steps are accomplished. Milestones can be found in the Planning menu.

5. ENTRANCE CONFERENCE

An entrance conference will be held with management officials before undertaking any audit, unless an exception is specifically authorized by the IG. Entrance conferences are optional for contract audits or audits of an investigative nature. If, for any reason, an audit announcement letter is not issued, documenting the entrance conference will fulfill the intent of the notification policy and applicable audit planning standards. The auditor will prepare an entrance conference memorandum for the work papers. In TeamMate EWP, the entrance conference is normally documented in section AS2 entitled Administration. Management has the right to waive the entrance meeting as long as the notification letter clearly states the objectives of the audit.

6. AUDIT FIELD WORK
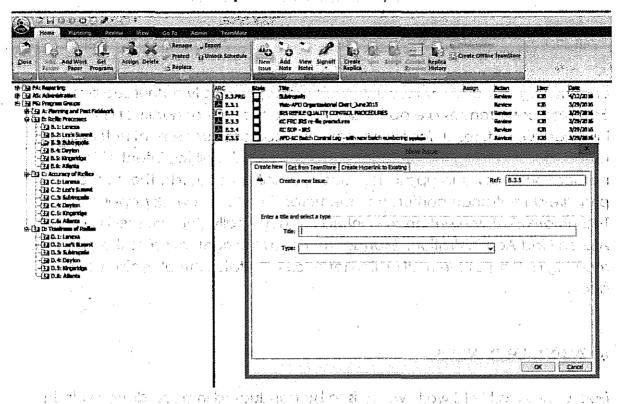
During the audit field work, which is to be conducted in accordance with the Government Accountability Office (GAO) *Government Auditing Standards*, the audit team is responsible for collecting, analyzing, and documenting the information necessary to accomplish the audit objectives. During this phase, the team ensures that the elements of a finding are sufficiently developed, work papers contain sufficient and appropriate evidence to support reportable findings and conclusions, and work papers are reviewed and any supervisory review notes are cleared.

Auditors will meet with the AIGA to discuss a project's status during, and at the completion of, the field work phase. These project status reviews are held to discuss the preliminary results of the auditors' effort, to determine whether the assignment objectives are still appropriate or need to be changed, and to ensure that auditors remain focused on the assignment requirements.

When auditors identify a potential finding, they must prepare an exception in section AS1 using the exception tool. An exception contains all the necessary elements of a finding (i.e., criteria, condition, cause, and effect).
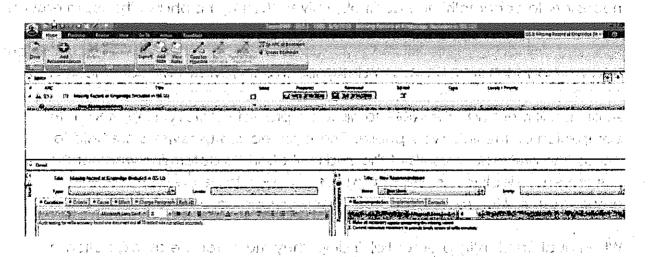
Clicking on the exception icon will open the following dialog box:
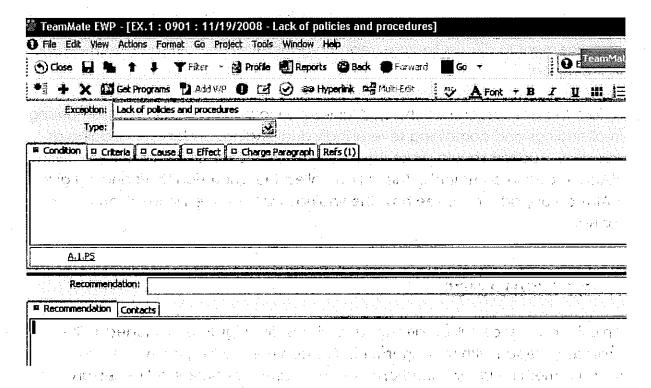
More than likely, the auditor will be developing a new exception specific to their audit. However, an exception/finding write-up may be stored in the TeamStore.

To create a new exception/finding, give the new exception a title. Leave
'Type' blank.

```
TeamMate EWP - [EX.1 : 0901 : 11/19/2008 - Lack of policies and procedures]
File  Edit  View  Actions  Format  Go  Project  Tools  Window  Help

Close  ↑  ↓  Filter  ▾  Profile  Reports  Back  Forward  Go  ▾

+  X  Get Programs  Add W/P  Hyperlink  Multi-Edit  A Font  ▾  B  I  U

Exception:  Lack of policies and procedures
      Type:

Condition | Criteria | Cause | Effect | Charge Paragraph | Refs (1)



A.1.P5

Recommendation:

Recommendation | Contacts
```

The auditor can document all the necessary elements of a finding in the
exception and cross-reference to supporting work papers. An exception(s) can
be printed using the Tools | Generate Report | Finding Sheet.

The auditors will discuss the potential findings and recommendations with the
staff of the offices audited as issues are discovered. The purpose of this
discussion is to disclose the potential findings and recommendations; identify
any clarifications needed; and, if possible, resolve any areas of disagreement
before a draft report is issued.

When an auditor becomes aware of abuse that could be quantitatively or
qualitatively significant to the program under audit, the auditor should apply
audit procedures specifically directed to ascertain the potential effect on the
program under audit within the context of the audit objectives. After performing
additional work, auditors may discover that the abuse represents potential fraud

or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

Throughout the fieldwork, the auditor will hold Message Meetings with OIG management to discuss findings, report organization and overarching message in the report.

Before the exit conference the auditor will be working on the Draft report pulling in all findings and combining several individual findings under one heading as needed. Auditors should share the Audit Results section of the draft report with NARA to obtain comments. This will be called the Discussion Draft and will give NARA an opportunity to see how the findings will be written in the Draft Report format.

7. EXIT CONFERENCE

An exit conference will be arranged to discuss findings to be included in the draft audit report with management. The conference may be waived by management if further discussions are not desired or considered necessary. The exit conference serves as a final opportunity to clarify specific findings, provide explanations, or to correct any misstatements and include upper management in these discussions. In TeamMate EWP, the exit conference is documented in the Administration section, AS2.

8. DRAFT REPORT

A draft report can be generated using the reporting tool. This is optional at this time. The auditor can generate a draft audit report using the reporting tool which pulls all the exceptions/findings and certain information from the Profile into a Microsoft Word document.

The draft report should be saved to folder PA3. The draft report generated is not a final document. It provides a good starting point for ensuring all issues are included in the draft report. However, tone, logical flow, executive summary,

charge paragraphs and other language will need to be tweaked for draft report issuance. For instance, you may find that several exceptions written up really relate to one cause and will be summarized in one section of the draft report. It is stressed that the draft report generated is just your initial starting point for writing your draft report. For example, pictures, tables and charts are encouraged to be added for clarity of issues.

To generate the Draft Report, select Tools | Generate Report. The following dialog box will appear:

Report Wizard - Selection

Welcome to the Report Wizard. This process will generate a Word report from the contents of the current viewer. Otherwise you can select any report type and scope.

Select a report file

Description	Filename	Type
Audit Guide Report	Audit Guide Report.dotx	
AUDIT OF NARA'S IMPLEMENTATION OF THE...	Draft Report.dotx	
Procedure Standard Report	pr_std.dotx	

File name: S:\TEAMMATE\Reports\Draft Report.dotx   Browse...

Next >   Cancel

Select Draft Report. The File Name should default to your S:\TEAMATE\Reports folder. Click Next.

Report Wizard - Destination ⊠

🗎   Select Report Destination and Title

⊙ Save report as a work paper stored within this project.

[Select a folder to add work paper OR select existing Word document to be overwritten.]

```
⊟ ⬜ PA: Reporting
   ⊞ ⬜ PA1: Final Report
   ⊞ ⬜ PA2: Auditors analysis of Management Response
   ⊟ ⬜ PA3: Draft Report
         🗎 PA3.b: Distribution List
         🗎 PA3.c: GAGAS Certification
      ⬜ PA4: Referenced Draft Report
      ⬜ PA5: AIGA Comments on Draft Report
      ⬜ PA6: Legal Review of Draft Report
      ⬜ PA7: IG Comments on Draft Report
```

○ Save as external Word document

Title: AUDIT OF NARA'S IMPLEMENTATION OF THE FEDERAL

[< Back]   [Finish]   [Cancel]

Select PA3 to save the Draft Report at this location. Click Finish.

A Microsoft Word document will open, as PA3.d or the next available ARC, pulling data from the Profile and Exceptions, producing a Draft Report in a revisable format, a Microsoft Word document.

The OIG will issue a draft audit report to cognizant NARA officials (usually the office heads) and request written management comments. The comments should include statements on:

(a) whether management concurs, partially concurs, or does not concur with each finding and recommendation; and
(b) explanations for any disagreements with the report's facts, findings, conclusions, or recommendations.

If management has additional documentation to support its position, it should be included in the response to the draft report. The OIG will modify the report as necessary, if management's comments are valid and supported with sufficient, appropriate evidence.

Generally, offices are allowed 40 calendar days to provide written management comments and action plans. Their comments may be paraphrased in the body of the final audit report, but must be included in their entirety as an appendix to the report. Offices will provide copies of all management comments to the Accountability.

If management is unable to provide comments within 40 calendar days, extensions may be granted by the IG. The final report may be issued without management comments, if the OIG does not receive the comments within a timely manner.

In TeamMate EWP, the draft report is documented in the Reporting section, PA3 and management's response and analysis is documented in PA2.

9. FINAL REPORT

The final audit report will be addressed to the Archivist who is responsible for ensuring that cognizant offices implement the report's recommendations. The report will include management's written comments on the draft report and OIG evaluations of management's comments. For audit follow-up and resolution purposes, copies of all final reports will be provided to Accountability. Final audit reports will generally be available to the public, unless restricted by law (proprietary, privacy act, or national security information is usually precluded from release).

In TeamMate EWP. The final report is documented in the Reporting section, PA1.

10. FOLLOW-UP

The OIG is responsible for performing follow-up effort, to ensure adequate implementation of report recommendations and to test the effectiveness of corrective actions taken by management. This responsibility includes:

(a) tracking and reporting on the status of all audit report recommendations,

(b) ensuring that final actions on recommendations are taken by management within 6 months from the date of report issuance, and

(c) following-up on the impact of actions taken in response to recommendations.

The auditor(s) who performed the audit is responsible for following-up on the report recommendations, until otherwise indicated.

Follow-up documentation is maintained in the audit report file system by the auditor. The report file should contain all the report follow-up documentation, including: management comments on the draft report, an audit action plan (prior to FY 2017), and any supporting documentation.

11.   PROJECT TERMINATION

If, at any time during the audit process the auditors conclude that a project should be terminated, the AIGA should be informed of the rationale for terminating that project. If termination is approved, a memorandum should be added to the project work papers documenting the decision to terminate the project. The memorandum will be signed by the AIGA and/or the IG and state the reason(s) for termination, e. g., no deficiencies were found or conditions changed during the field work.

After approval of the termination, a letter will be issued to management outlining the nature, scope, and results of the work performed, and advising that no further effort is contemplated.

12.   SUSPECTED IMPROPER OR ILLEGAL ACTS

In carrying out assignment responsibilities, auditors must be alert to any information indicating potential wrong doing. Suspected improper or illegal activities should be referred to the Assistant Inspector General for Investigations (AIGI) for possible further review.

Whenever an auditor suspects that an illegal or improper act may have occurred, the matter should be discussed with the AIGA, but not with agency management. Legal questions and potential noncompliance with laws and regulations arising during a project should also be discussed with the Counsel to the IG.

A memorandum will be used to make a referral to the AIGI. The memorandum should contain an introduction, background, discussion of suspected irregularities, and identify a point of contact to further explain the situation.

If the AIGI decides to conduct an investigation, the related audit activity should continue, to the extent that the audit work and/or issuance of a report will not impede the conduct of an investigation.

13. INDEPENDENCE

Audit staff is responsible for maintaining independence in all matters relating to audit or attestation engagement work. Independence comprises:

(a) Independence of Mind - The state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.

(b) Independence in Appearance - The absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised.

Auditors, specialists, and audit contractors, as well as the audit organization as a whole, are responsible for maintaining independence so that the opinions, findings, conclusions, judgments, and recommendations resulting from the work performed will be impartial and will be viewed as impartial by knowledgeable

third parties. OA staff members must consider not only whether they are Independent and whether their attitudes and beliefs permit them to be independent, but also whether there is anything about their personal or professional situation that might lead others to question their independence. All situations should be considered. Even an appearance of a threat to independence should be discussed with the staff member's supervisor to determine if the staff member should be recused from certain assignments.

If a threat to independence is identified prior to beginning fieldwork and the individual is recused from the assignment, there is no need to document the recusal. If a threat to independence is identified after the beginning of fieldwork and the application of safeguards cannot eliminate or reduce the threat to an acceptable level, the individual must be recused as soon as the independence issue is identified, and the action taken must be documented in a memorandum to the AIGA, and to the TeamMate work paper file. The AIGA will maintain a record of reported threats to independence and the safeguards applied to resolve the independence issue. In situations where the government auditor, because of legislative requirements or for other reasons, cannot decline to perform the work, the threats to independence will be reported in the scope section of the report.

If a threat to independence is identified after the final audit report is issued, the AIGA will assess the impact on the assignment and GAGAS compliance and advise the IG. If the IG concludes that the auditors did not conduct the assignment independently, and determines that the impact on the audit would have resulted in the auditor's report being different than the report issued had the auditors been aware of the threat, the impact should be communicated in writing to NARA management, requestors, or regulatory agencies, if applicable, so they do not continue to rely on the findings or conclusions that were impacted by the threat to independence.

The IG will determine whether to conduct additional audit work necessary to reissue the report or repost the original report if the findings and conclusions are unchanged based on the additional audit work.

Auditors should be independent from an audited entity during:

(a) any period of time that falls within the period covered by the financial statements or subject matter of the audit; and

(b) the period of the professional engagement, which begins when the auditors either sign an initial engagement letter or other agreement to perform an audit or begin to perform an audit, whichever is earlier. The period lasts for the entire duration of the professional relationship (which, for recurring audits, could cover many periods) and ends with the formal or informal notification, either by the auditors or the audited entity, of the termination of the professional relationship or by the issuance of a report, whichever is later. Accordingly, the period of professional engagement does not necessarily end with the issuance of a report and recommence with the beginning of the following year's audit or a subsequent audit with a similar objective.

Application of the Conceptual Framework
Many different circumstances, or combinations of circumstances, are relevant in evaluating threats to independence. Therefore, GAGAS establishes a conceptual framework that auditors use to identify, evaluate, and apply safeguards to address threats to independence. The GAGAS conceptual framework (see Attachment 2-4) assists auditors in maintaining both independence of mind and independence in appearance. It can be applied to many variations in circumstances that create threats to independence and allows auditors to address threats to independence that result from activities that are not specifically prohibited by GAGAS.

Auditors should apply the conceptual framework at the audit organization, audit, and individual auditor levels to:

(a) identify threats to independence;

(b) evaluate the significance of the threats identified, both individually and in the aggregate; and:

(c) apply safeguards as necessary to eliminate the threats or reduce them to an acceptable level. If no safeguards are available to eliminate an unacceptable threat or reduce it to an acceptable level, independence would be considered impaired.

Auditors should evaluate threats to independence using the conceptual framework when the facts and circumstances under which the auditors perform their work may create or augment threats to independence. Auditors should evaluate threats both individually and in the aggregate because threats can have a cumulative effect on an auditor's independence.

Facts and circumstances that create threats to independence can result from events such as the start of a new audit; assignment of new staff to an ongoing audit; and acceptance of a nonaudit service at an audited entity. Many other events can result in threats to independence. Auditors use professional judgment to determine whether the facts and circumstances created by an event warrant use of the conceptual framework. Whenever relevant new information about a threat to independence comes to the attention of the auditor during the audit, the auditor should evaluate the significance of the threat in accordance with the conceptual framework.

Auditors should determine whether identified threats to independence are at an acceptable level or have been eliminated or reduced to an acceptable level. A threat to independence is not acceptable if it either (a) could impact the auditor's ability to perform an audit without being affected by influences that compromise professional judgment or (b) could expose the auditor or audit organization to circumstances that would cause a reasonable and informed third party to conclude that the integrity, objectivity, or professional skepticism of the audit organization, or a member of the audit team, had been compromised.

When an auditor identifies threats to independence and, based on an evaluation of those threats, determines that they are not at an acceptable level, the auditor should determine whether appropriate safeguards are available and can be applied to eliminate the threats or reduce them to an acceptable level. The auditor should exercise professional judgment in making that determination, and should take into account whether both independence of mind and independence in appearance are maintained. The auditor should evaluate both qualitative and quantitative factors when determining the significance of a threat.

In cases where threats to independence are not at an acceptable level, thereby requiring the application of safeguards, the auditors should document the threats identified and the safeguards applied to eliminate the threats or reduce them to an acceptable level.

Certain conditions may lead to threats that are so significant that they cannot be eliminated or reduced to an acceptable level through the application of safeguards, resulting in impaired independence. Under such conditions, auditors should decline to perform a prospective audit or terminate an audit in progress.

If a threat to independence is initially identified after the auditors' report is issued, the auditor should evaluate the threat's impact on the audit and on GAGAS compliance. If the auditors determine that the newly identified threat had an impact on the audit that would have resulted in the auditors' report being different from the report issued had the auditors been aware of it, they should communicate in the same manner as that used to originally distribute the report to those charged with governance, the appropriate officials of the audited entity, the appropriate officials of the organizations requiring or arranging for the audits, those on the distribution list, Web posting users and other known users, so that they do not continue to rely on findings or conclusions that were impacted by the threat to independence. If the report was previously posted to the auditors' publicly accessible website, the auditors should remove the report and post a public notification that the report was removed. The auditors should then determine whether to conduct additional audit work necessary to reissue the report, including any revised findings or conclusions or repost the original report if the additional audit work does not result in a change in findings or conclusions.

Organizational Threats to Independence
Organizational threats to independence exist when the audit organization's ability to perform work and report results objectively is adversely impacted by its placement within government or the structure of the entity that the audit organization is assigned to audit. GAGAS paragraphs 3.27 through 3.32 specify various ways that an audit organization can meet the requirement for organizational independence. As a Federal Office of Inspector General, the NARA OIG meets the requirement; therefore, NARA OIG auditors are presumed

to be free from organizational impairments to independence. The IG Act, amended provides safeguards of independence for NARA:

- (a) statutory protections that prevent the audited entity from abolishing the audit organization;
- (b) statutory protections that require that if the head of the audit organization is removed from office, the head of the agency reports this fact and the reasons for the removal to the legislative body;
- (c) statutory protections that prevent the audited entity from interfering with the initiation, scope, timing, and completion of any audit;
- (d) statutory protections that prevent the audited entity from interfering with audit reporting, including the findings and conclusions or the manner, means, or timing of the audit organization's reports;
- (e) statutory protections that require the audit organization to report to a legislative body or other independent governing body on a recurring basis;
- (f) statutory protections that give the audit organization sole authority over the selection, retention, advancement, and dismissal of its staff; and
- (g) statutory access to records and documents related to the agency, program, or function being audited and access to government officials or other individuals as needed to conduct the audit.

Statement of Independence

Audit staff who sign annual independence statements should always be aware of any potential threat to independence and immediately notify the AIGA, if any potential threat arises subsequent to signing the annual statement.

At the beginning of each fiscal year, the IG, General Counsel to the IG, and the AIGA should complete and sign an individual Statement of Independence in Attachment 2-2. This form should be documented in each project's TeamMate file, section AS.1. Signed statements of independence may be scanned in the audit file.

At the beginning of each assignment, the auditor must complete and sign an individual Statement of Independence in Attachment 2-3. This form should be documented in the project's TeamMate file, section AS.1. In TeamMate EWP, users may electronically sign the Statement of Auditor's Independence in the

Administration section, AS2. In TeamMate the preparer's signoff reflects the auditor's electronic signature and the reviewer's signoff reflects the supervisor's electronic signature because each person has an individual login ID and password. Each person should fill out a separate individual independence statement and signoff as the preparer.

Throughout the project, the auditor should ensure that the independent referencer, contractor or other specialist, if they are assisting in audit analysis and research has a signed statement of independence documented in the TeamMate file. The auditor should also discuss the independence requirement with the supervisor throughout the project. This discussion serves as a reminder that employees should always be aware of any potential threat to independence.

If more than one auditor works on an assignment, the supervisor shall select one to be the project manager. The project manager should ensure that each team member completes and signs an individual Statement of Independence in Attachment 2-3 at the beginning of each audit. Throughout the project, the project manager should ensure that any team member added to the assignment (including the independent referencer, contractor or other specialist, if they are assisting in audit analysis and research) has a signed statement of independence documented in the TeamMate file. The auditor should also discuss the independence requirement with the team throughout the project. This discussion serves as a reminder that employees should always be aware of any potential threat to independence.

When using a specialist, such as, but not limited to actuaries, appraisers, attorneys, engineers, environmental consultants, medical professionals, statisticians, and geologists, select an individual or firm that is independent and objective. The OIG will review each specialist's qualifications to perform the audit or services. This is usually done through the contracting process. The OIG will request the specialist to submit their certifications and references. The OIG will request each specialist to represent that they are independent in mind and appearance and objective with respect to NARA and request the specialist to describe all work, including non-audit services, done with NARA within the last 3 years. The specialist should document the threats identified and the safeguards

applied to eliminate the threats or reduce them to an acceptable level. If the specialist cannot identify safeguards to eliminate threats identified or reduce them to an acceptable level, the OIG should not use the work of that specialist.

If any potential threat arises subsequent to signing statements of independence, employees should notify their supervisor immediately. Any questions regarding potential threats and the application of appropriate safeguards should be referred to the AIGA. If a potential threat is identified, the AIGA, will forward a copy of the employee's Statement of Independence to the Counsel to the Inspector General to ensure that the Statement is consistent with the annual financial disclosure form.

Identifying and Evaluating Threats to Independence
Threats to independence are circumstances that could impair independence. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised. Threats are conditions to be evaluated using the conceptual framework. Threats do not necessarily impair independence.

Threats to independence may be created by a wide range of relationships and circumstances. Auditors should evaluate the following broad categories of threats to independence when threats are being identified and evaluated:

(a) Self-interest threat - the threat that a financial or other interest will inappropriately influence an auditor's judgment or behavior;
(b) Self-review threat - the threat that an auditor or audit organization that has provided non-audit services will not appropriately evaluate the results of previous judgments made or services performed as part of the non-audit services when forming a judgment significant to an audit;
(c) Bias threat - the threat that an auditor will, as a result of political, ideological, social, or other convictions, take a position that is not objective;
(d) Familiarity threat - the threat that aspects of a relationship with management or personnel of an audited entity, such as a close or long

relationship, or that of an immediate or close family member, will lead an auditor to take a position that is not objective;

(e) Undue influence threat - the threat that external influences or pressures will impact an auditor's ability to make independent and objective judgments;

(f) Management participation threat - the threat that results from an auditor's taking on the role of management or otherwise performing management functions on behalf of the entity undergoing an audit; and:

(g) Structural threat - the threat that an audit organization's placement within a government entity, in combination with the structure of the government entity being audited, will impact the audit organization's ability to perform work and report results objectively.

Circumstances that result in a threat to independence in one of the above categories may result in other threats as well. For example, a circumstance resulting in a structural threat to independence may also expose auditors to undue influence and management participation threats. The auditor should evaluate both qualitative and quantitative factors when determining the significance of a threat.

Safeguards

Safeguards are controls designed to eliminate or reduce to an acceptable level threats to independence. Under the conceptual framework, the auditor applies safeguards that address the specific facts and circumstances under which threats to independence exist. In some cases, multiple safeguards may be necessary to address a threat. The specific safeguards applied to eliminate the threat or reduce it to an acceptable level will determine whether or not independence is impaired. The auditor should exercise professional judgment in making that determination, and should take into account whether both independence of mind and independence in appearance are maintained.

GAGAS provides a list of safeguards that may be effective under certain circumstances in addressing threats to independence. The list cannot provide safeguards for all circumstances. It may, however, provide a starting point for auditors who have identified threats to independence and are considering

what safeguards could eliminate those threats or reduce them to an acceptable level. (See GAGAS paragraphs 3.17 for examples of Safeguards)

Auditors must document the safeguards applied to the identified potential threats to independence on the independence form for each project or via a memo to the file in the audit or with the AIGA if it is a private concern.

Examples of safeguards include:
(a) consulting an independent third party, such as a professional organization, a professional regulatory body, or another auditor;
(b) involving another audit organization to perform or reperform part of the audit;
(c) having a professional staff member who was not a member of the audit team review the work performed; and
(d) removing an individual from an audit team when that individual's financial or other interests or relationships pose a threat to independence.

Depending on the nature of the audit, an auditor may also be able to place limited reliance on safeguards that the entity has implemented. It is not possible to rely solely on such safeguards to eliminate threats or reduce them to an acceptable level.

Examples of safeguards within the entity's systems and procedures include:
(a) an entity requirement that persons other than management ratify or approve the appointment of an audit organization to perform an audit;
(b) internal procedures at the entity that ensure objective choices in commissioning nonaudit services; and
(c) a governance structure at the entity that provides appropriate oversight and communications regarding the audit organization's services.

14.   Attestation Engagements

Attestation engagements can cover a broad range of financial or nonfinancial objectives and may provide different levels of assurance about the subject matter or assertion depending on the users' needs. Attestation engagements

result in an examination, a review, or an agreed-upon procedures report on a subject matter or on an assertion about a subject matter that is the responsibility of another party. Attestation Engagements will follow similar policy and procedures specific to the audits processes described above and document work performed similar to Chapter 4 on Work Papers.

For attestation engagements, GAGAS incorporates the AICPA attestation standards. Auditors should be knowledgeable in the AICPA general attestation standard related to criteria, the AICPA attestation standards for field work and reporting, and the related Statements on Standards for Attestation Engagements (SSAE), and they should be competent in applying these standards and SSAE to the task assigned. The auditor will review AICPA attestation standards and document in the work papers that they are knowledge and capable of applying the attestation standards to the attestation engagement.

The auditor must have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users and document the reason.

The auditor must adequately plan the work and must properly supervise any assistants.

The auditor must obtain sufficient evidence to provide a reasonable basis for the conclusion that is expressed in the report (see Chapter 4 on Work Papers).

When planning the engagement, auditors should communicate certain information, including their understanding of the services to be performed for each engagement, in writing to entity management, those charged with governance, and to the individuals contracting for or requesting the engagement. When auditors perform the engagement pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the entity, auditors should communicate with the legislative committee. In those situations where there is not a single individual or group that both oversees the strategic direction of the entity and the fulfillment of its accountability obligations or in other situations where the identity of those

charged with governance is not clearly evident, the auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. Auditors should communicate the following additional information under GAGAS:

 (a) the nature, timing, and extent of planned testing and reporting;
 (b) the level of assurance the auditor will provide; and
 (c) any potential restriction on the auditors' reports, in order to reduce the risk that the needs or expectations of the parties involved may be misinterpreted.

Auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that could have a material effect on the subject matter. When planning the engagement, auditors should ask entity management to identify previous audits, attestation engagements, and other studies that directly relate to the subject matter of the attestation engagement being undertaken, including whether related recommendations have been implemented. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current engagement objectives.

Auditors should prepare attest documentation in sufficient detail to enable an experienced auditor, having no previous connection to the attestation engagement, to understand from the documentation the nature, timing, extent, and results of procedures performed and the evidence obtained and its source and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions. Auditors should prepare attest documentation that contains support for findings, conclusions, and recommendations before they issue their report.

15.   Departures from GAGAS

When auditors do not comply with applicable GAGAS requirements due to law, regulation, scope limitations, restrictions on access to records, or other issues

impacting the audit, the OIG will document the departure from the GAGAS requirements and the impact on the audit and on the auditors' conclusions.

When auditors do not comply with any applicable requirements, the audit will (1) assess the significance of the noncompliance to the audit objectives, (2) document the assessment, along with their reasons for not following the requirement, and (3) determine the type of GAGAS compliance statement. The auditors' determination will depend on the significance of the requirements not followed in relation to the audit objectives.

16.   NARA 1201

NARA 1201 establishes policies and procedures for audits of programs and operations administered or financed by NARA, conducted by the Office of the Inspector General (OIG), independent public accountants (IPA), the General Accountability Office (GAO), and other audit bodies (See Attachment 2-5).

ATTACHMENT 2-1

OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
8601 ADELPHI ROAD   COLLEGE PARK, MD 20740-6001
www.archives.gov/oig

NATIONAL
ARCHIVES

DATE: XXXX

TO: [Name of SES official]
[Title of SES official]
[Department Component]

[Name of SES official]
[Title of SES official]
[Department Component]

FROM: James Springs
Inspector General

> Please note that one space is required after a period.

SUBJECT: [*Insert Name of Project in italics – use appropriate classification markings in the subject line*]

We are initiating an [audit/review] of [insert program/area being reviewed]. [Optional, as needed] We are conducting this [audit/review] pursuant to [please briefly explain here what/who is prompting the audit/review].

Our objective is to [insert audit/review objective].

Please provide (1) a point of contact that can provide technical guidance related to the subject audit, and (2) any documented organizational policies and procedures supporting the program/activity.

The audit will be conducted by [Name of Auditor (s)]. We will contact your office to arrange an entrance conference. During the meeting, we will provide further details on our objectives and scope. We have tentatively scheduled field work to begin [insert expected date that field work is scheduled to begin], and will conduct field work in [insert area/location field work will take place] and other locations as necessary.

Please call me with any questions, or your staff may contact Jewel Butler, Assistant Inspector General for Audits, at (301) 837-1732. [Avoid separating first and last names and telephone number]

cc: [Insert titles of individuals who are to receive a copy of the memo. Generally, include the standard NARA officials who usually receive these notifications).]

Page Numbering: If your transmittal memo exceeds one page, page numbering should begin on the second page. The numbers should be in the footer and centered.

ATTACHMENT 2-2

NATIONAL ARCHIVES

OFFICE OF INSPECTOR GENERAL

National Archives and Records Administration

STATEMENT OF INDEPENDENCE

DATE: FY 20XX

PROJECT TITLE: All OIG Projects and Assignments

In all matters relating to audits, and investigations (as required) the National Archives and Records Administration Office of Inspector General (NARA OIG), its employees, and others involved must be free from circumstances that would cause a reasonable and informed third party to doubt their integrity, objectivity, or professional skepticism, and must maintain independence of mind and in appearance **(See Government Auditing Standards for auditor independence (GAO "Yellow Book," December 2011 Revision, Chapter 3, paragraphs 3.02-3.59)**

Threats to Independence include personal, impairments, external impairments, and organizational impairments, but are not limited to,

> a. Self-interest threat - the threat that a financial or other interest will inappropriately influence an auditor's judgment or behavior;
>
> b. Self-review threat - the threat that an auditor or audit organization that has provided nonaudit services will not appropriately evaluate the results of previous judgments made or services performed as part of the nonaudit services when forming a judgment significant to an audit;
>
> c. Bias threat - the threat that an auditor will, as a result of political, ideological, social, or other convictions, take a position that is not objective;
>
> d. Familiarity threat - the threat that aspects of a relationship with management or personnel of an audited entity, such as a close or long relationship, or that of an immediate or close family member, will lead an auditor to take a position that is not objective;
>
> e. Undue influence threat - the threat that external influences or pressures will impact an auditor's ability to make independent and objective judgments;

f. Management participation threat - the threat that results from an auditor's taking on the role of management or otherwise performing management functions on behalf of the entity undergoing an audit; and
g. Structural threat - the threat that an audit organization's placement within a government entity, in combination with the structure of the government entity being audited, will impact the audit organization's ability to perform work and report results objectively.

Completing this form underscores the importance to adhere to standards of independence and objectivity, and must be certified by those working on audits as well as senior executives and others within NARA OIG who review audit reports. The Inspector General (IG), Counsel to the IG, Assistant IG, and others within NARA OIG who review audit reports, must sign an independence statement on an annual basis **(See NARA OIG Audit Manual, September 2013, 2-25 and attachment 2-3 (*Independence Declaration Documentation*)**.

Individuals who are unable to make this certification or believe a threat to their independence that could require safeguards may exist must notify a senior manager involved in their current assignment or, within another OIG Office (only if the impairment is with the IG).

- -

I certify that there are no impairments to my independence, and I will promptly notify my supervisor if a threat to my independence that may require safeguards should arise.

Print Name: _____

Title: _____

Signature: _____   Date: _____

ATTACHMENT 2-3

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

STATEMENT OF AUDITOR'S INDEPENDENCE

We, the undersigned, on the date shown, certify that no personal impairments exist that would inhibit our ability to be impartial, or that would give the appearance of not being impartial, during the performance of the subject project.

PROJECT TITLE _____

PROJECT NO. _____

I certify that I have read the Government Auditing Standards for auditor independence (GAO "Yellow Book," December 2011 Revision, Chapter 3, paragraphs 3.02-3.59) and to the best of my knowledge and belief, except as noted below, I am free both in mind and appearance from personal and external threats to independence with regard to the project indicated above.

I understand that I am responsible for identifying potential threats to my independence, notifying my supervisor of any potential threats, applying appropriate safeguards to address any threats, and recusing myself from individual assignments, if appropriate. I also understand that if I do not comply with the independence standard, I may be subject to sanctions up to and including possible termination.

This Statement of Independence applies to the entire period of professional engagement.

I considered threats to independence including:
- Self-interest threat
- Self-review threat
- Bias threat
- Familiarity threat
- Undue influence threat
- Management participation threat
- Structural threat
- Other: _____

Have any threats been identified by an auditor for this audit? _____ (Yes or No). If yes, please document safeguards for each threats indentified. Contract the AIGA for more information regarding the threats and safeguards identified. If private, threats and safeguards can be documented and sent directly to AIGA.

Safeguards for each threat:

ATTACHMENT 2-4
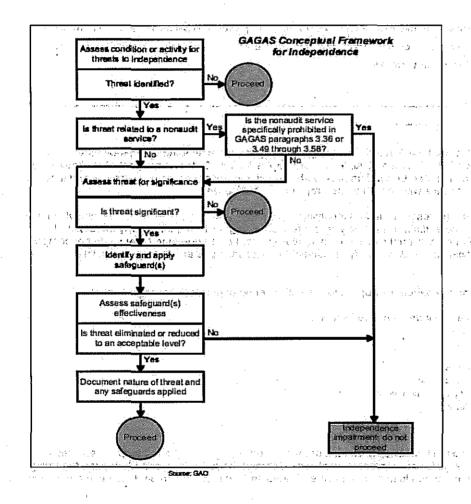
GAGAS Conceptual Framework for Independence

Comments:

In TeamMate the preparer and approver's signoff reflects the auditor's electronic signature because each person has an individual login ID and password.

GAGAS Conceptual Framework for Independence

Assess condition or activity for threats to independence

Threat identified? — No → Proceed

↓ Yes

Is threat related to a nonaudit service? — Yes → Is the nonaudit service specifically prohibited in GAGAS paragraphs 3.36 or 3.49 through 3.58? — Yes →

↓ No

Assess threat for significance ← No

Is threat significant? — No → Proceed

↓ Yes

Identify and apply safeguard(s)

↓

Assess safeguard(s) effectiveness

Is threat eliminated or reduced to an acceptable level? — No →

↓ Yes

Document nature of threat and any safeguards applied

↓

Proceed

Independence impairment: do not proceed

Source: GAO

ATTACHMENT 2-5

NARA 1201, Audits of NARA Programs and Operations

May 15, 2012

Transmittal memo

1201.1 What is the purpose of this directive?

1201.2 What is the authority for this directive?

1201.3 Responsibilities

1201.4 How are records created by this directive maintained under the NARA Records Schedule?

Supplement to NARA 1201, Audits of NARA Programs and Operations

1201.1 What is the purpose of this directive?

This directive establishes policies and procedures for audits of programs and operations administered or financed by NARA, conducted by the Office of the Inspector General (OIG), independent public accountants (IPA), the General Accountability Office (GAO), and other audit bodies.

1201.2 What is the authority for this directive?

a. Inspector General Act of 1978 as amended (5 U.S.C., Appendix)

b. Single Audit Act of 1984 (31 U.S.C. 7501 et seq.)

c. Accountability of Tax Dollars Act of 2002

d. OMB A-50, Audit Followup, September 1982

e. OMB A-123, Management's Responsibility for Internal Controls, December 2004 as amended

1201.3 Responsibilities

a. Archivist - The Archivist ensures that NARA resolves audit recommendations in accordance with applicable laws, regulations, and policies. This is accomplished by designating a senior management official to oversee audit follow-up, including resolution and corrective actions, and by ensuring that all managers understand the value of audits and are responsive to audit recommendations.

b. Audit liaison - The audit liaison is the local point of contact once an audit begins, coordinating meetings and documentation as needed. The audit liaison is responsible for tracking all open recommendations, preparing and distributing closing packages, and other related duties that may be assigned by the Executive.

c. Audit resolution official - The Chief Operating Officer (COO) is the designated audit resolution official, and as such, is directly responsible for ensuring that:

(1) Systems of audit follow-up, resolution, and corrective action are documented and in place;

(2) Timely responses are made to audit reports;

(3) Disagreement between office heads or staff directors and the OIG about report recommendations are resolved;

(4) Corrective actions are taken; and

(5) Semiannual reports on the status of recommendations are sent to the Archivist.

d. Executives, staff directors, and managers - ensure that staff fully cooperates with the OIG, including:

(1) Providing access to all information requested by auditors;

https://www.nara-at-work.gov/nara_policies_and_guidance/directives/1200_series/nara1201.html#   1/2

NARA 1201, Audits of NARA Programs and Operations | NARA@work

(2) Analyzing all applicable audit reports;

(3) Preparing timely, accurate, and complete responses to applicable audit reports;

(4) Ensuring that audit recommendations are addressed timely;

(5) Providing CP with information required for compiling audit status reports; and

(6) Consulting with the OIG before entering into audit services contracts.

(7) Completing redaction reviews within timeframes requested by the OIG.

e. Inspector General - The Inspector General:

(1) Provides policy direction for conducting, supervising, and coordinating audits of NARA programs;

(2) Selects and conducts audits of NARA programs, operations, contracts, and grants in conformance with GAO's Government Auditing Standards;

(3) Conducts or supervises audits of NARA contracts and grants;

(4) Promptly reports the results of audits to the Archivist;

(5) Reports results to Congress as warranted;

(6) Reviews implementation of audit recommendations; and

(7) Establishes guidelines for determining when it is appropriate to use non-Federal auditors and ensures that those auditors comply with GAO's Government Auditing Standards.

f. Performance and Accountability staff (CP) - CP coordinates audit resolution, reviews and monitors progress on corrective action plans, and manages the administrative and operational portions of the audit resolution process for the Audit Resolution Official. CP staff:

(1) Serves as initial point of contact for the OIG, GAO, and other audit entities to provide coordinated NARA response;

(2) Maintains official case files and database for all audits;

(3) Coordinates meetings, comments, and other responses especially for audits involving multiple offices;

(4) Works with the auditors and programs to ensure target dates are met and requests extensions as appropriate, bringing potential conflicts to the attention of the COO; and

(5) Produces semi-annual and other reports as requested.

1201.4 How are records created by this directive maintained under the NARA Records Schedule?

Maintain records created by this directive in accordance with the NARA Records Schedule, Appendix 12, Audits and Investigations.

Page last reviewed: Sep 17, 2015 - by Stuart A Culy

Notify the content author if this page contains out-of-date or incorrect information

Supplement to NARA 1201,

Audits of NARA Programs and Operations

TABLE OF CONTENTS

S-2

Guide to Audit Processes and Resolution

S1.   Types of Audits

a.   Audits are classified by the GAO's *Government Auditing Standards* (GAGAS) as either "financial audits" or "performance audits," depending on the audit objectives. Financial audits provide an independent assessment of whether an entity's reported financial information (e.g., financial condition, results, and use of resources) are presented fairly in accordance with recognized criteria. Performance audits provide findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria.

b.   Financial Audits

(1)   Financial statement audits – The primary purpose of a financial statement audit is to provide an opinion about whether an entity's financial statements are presented fairly in all material respects in conformity with an applicable financial reporting framework. Reporting on financial statement audits performed in accordance with GAGAS also includes reports on internal control over financial reporting and on compliance with provisions of laws, regulations, contracts, and grant agreements that have a material effect on the financial statements.

(2)   Financial-related audits – Other types of financial audits conducted in accordance with GAGAS entail various scopes of work, including: (1) obtaining sufficient, appropriate evidence to form an opinion on single financial statements, specified elements, accounts, or items of a financial statement; (2) issuing letters for underwriters and certain other requesting parties; and (3) auditing compliance with applicable compliance requirements relating to one or more government programs.

c.   Performance Audits

(1)   Program effectiveness and results audit objectives are frequently interrelated with economy and efficiency objectives. Audit objectives that focus on program effectiveness and results typically measure the extent to which a program is achieving its goals and objectives. Audit objectives that focus on economy and efficiency address the costs and resources used to achieve program results.

(2)   Internal control audit objectives relate to an assessment of one or more components of an organization's system of internal control that is designed to provide reasonable assurance of achieving effective and efficient operations, reliable financial and performance reporting, or compliance with applicable laws and regulations. Internal control objectives also may be relevant when determining the cause of unsatisfactory program performance. Internal control comprises the plans,

S-3

policies, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal control includes the processes and procedures for planning, organizing, directing, and controlling program operations, and management's system for measuring, reporting, and monitoring program performance.

(3)   Compliance audit objectives relate to an assessment of compliance with criteria established by provisions of laws, regulations, contracts, or grant agreements, or other requirements that could affect the acquisition, protection, use, and disposition of the entity's resources and the quantity, quality, timeliness, and cost of services the entity produces and delivers. Compliance requirements can be either financial or nonfinancial.

S2.   Audit Services

Under the Inspector General Act of 1978 (as amended), the Office of the Inspector General (OIG) is to provide a means for keeping the Archivist and the Congress fully and currently informed about problems and deficiencies relating to the administration of NARA programs and operations, and the necessity for and progress of corrective action. In obtaining the necessary information to accomplish this requirement, the OIG conducts a range of audit services. These services include—but are not limited to—contract closeouts, billing inquiries, control assessments, and procurement evaluations.

S3.   OIG Audit Plan

The OIG prepares and distributes an annual audit plan. Suggestions for audits may originate in several places:

a.   Mandatory by statute or regulation. These include the annual independent financial audit, an evaluation of NARA's compliance with the Federal Information Security Management Act (FISMA), and other periodic requirements such as compliance with the Improper Payment Eliminations and Recovery Act.

b.   Selected by the OIG. These are usually aligned with the NARA Strategic Plan and are based on risk, materiality, significance, or other criteria.

c.   Requested by Congress.

d.   Suggested by the Archivist or other management officials. These suggestions may originate as part of the annual request from the OIG for audit plan input or may be forwarded to the OIG as issues arise.

e.   Suggested by anyone inside or outside of NARA who contacts the OIG to suggest audit areas, or recommend or request audit assistance.

Annual audit plans are flexible and may be changed during the year to assign limited audit resources to higher priority audits. The OIG determines the priority for conducting audits.

S-4

S4.   Audit Lifecycle

a.   Whether the auditor is internal or external to NARA, or whether the audit is financial or performance, most audits follow the same general process. The Archivist and affected offices are notified; the auditor reviews documentation and performs independent testing; reporting happens; and recommendations are satisfied. Then the audit is closed. The following shows what generally happens during each of these audit steps:

Announcement

Written notification to the Archivist and affected Executive	Entrance conference(s) with office(s) to be audited, CP representative, and others as required

Fieldwork

NARA provides documentation and access	Auditor uses documentation as basis for testing	Pre-exit and exit conferences with affected parties

Reports

OIG/GAO draft report to the Archivist for comment	Final report issued to the Archivist and others as required	Action plan approved by the Archivist and sent to auditor

Resolution

Auditor concurs with plan or provides feedback	Documentation provided to the auditor and CP per action plan	Progress reports to the Archivist, inclusion in assurance statement if appropriate

S-5

b.   It is not possible to accurately gauge the time from notification through closure of an audit. Many factors, including audit scope, available resources (both OIG and program), the nature and complexity of findings, and resources to address recommendations influence total lifecycle time. There are some actions in the process that do have specific requirements and timeframes. They occur in all except the Announcement step and are explained more fully in the detailed sections below.

All timeframes noted in this supplement are calculated as *calendar* days.

S-6

S5.   **Announcement:** before the audit begins   ⟶

Written notification to the Archivist and affected Executive

a.   Regardless of who is performing the audit, it will always begin with formal, written notification. The Archivist, affected Executive(s), and CP receive notification from the OIG on all internal audits and those for which the OIG has contracted out, e.g., the annual independent financial statement audit. GAO sends a formal letter to the Archivist and an email of the letter to CP. In each case, CP works with the auditor on behalf of the Archivist and Audit Resolution Officer to ensure that all appropriate NARA staff are invited to the entrance conference.

b.   NARA components are also audited by other Federal agencies such as the Office of Government Ethics and the Office of Personnel Management. These audits are very narrow in scope and auditors generally communicate directly with specific program areas. Copies of notification letters should be forwarded to CP for the central audit files.

Entrance conference(s) with office (s) to be audited, CP representative, and others as required

c.   Entrance conferences mark the actual beginning of an audit. It is during the entrance conference that NARA designates a central point of contact for the audit and the auditor requests initial documentation.

d.   The time between the announcement letter and entrance conference is generally ten days to two weeks, but can vary depending on the number of participants and scope of the audit. For example, it may be easier to schedule two smaller entrance conferences for an audit that covers three or more program areas.

e.   The OIG is invited to GAO entrance conferences to avoid duplication and ensure effective coordination and cooperation with the GAO, as required by section 4(c) of the Inspector General Act.

S-7

S6. Fieldwork: review, monitor, and test ➔

a. Fieldwork is the period in which most interaction between auditors and staff will occur. This step can vary in length from 60 to 180 days or longer.

NARA provides documentation and access	Auditor uses documentation as basis for testing

b. Some audits will be more transactional, looking to review documentation of specific events to ensure that processes and control points are followed consistently and effectively. Other audits will focus on the process and seek to discern if the process itself is the most efficient and effective, and controls are adequate to prevent mistakes. Each of these will use appropriate laws, regulations, guidelines, or internally documented procedures as the benchmark against which tests are conducted. Points of contact or managers should ensure that the auditors receive the most current versions of any guidance and alert them if changes have occurred that may not be reflected in these documents.

c. During this time, Executives, staff directors and managers should also interact with auditors to keep abreast of findings and discuss any potential changes that could affect the final report. For example, an internal control point may require a review and sign off that is not consistently performed. The manager can alert staff via a memo, in a meeting, or by some other method, reminding them of this requirement. If the situation has been corrected by the conclusion of the audit, it could become an observation with a note in the report rather than a recommendation to be managed later.

Pre-exit and exit conferences with affected parties

d. GAO generally provides a "Statement of Facts" with proposed findings and recommendations at a pre-exit conference for which NARA can provide a verbal or written response. Whether this is an in person conference or a teleconference, Executives and others in affected offices are invited to meet. The Archivist, Deputy Archivist, Chief Operating Officer, and the Inspector General are also invited. Turnaround for comments on the statement of facts is ten days or fewer and is managed via email by CP.

S-8

e.   An OIG audit concludes with an exit conference in which participants receive a document similar to the GAO statement of facts but not intended for written comment. The OIG may make adjustments or ask for additional documentation based on discussion during the exit conference. Between 30 and 90 days can elapse from the time of the exit conference to receipt of a draft report.
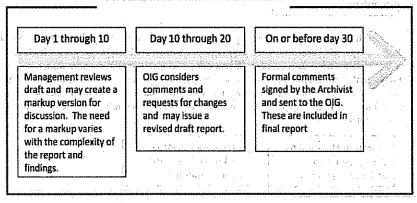
S7.   **Reports: from the draft report to the action plan** ⟶

> OIG draft report to the Archivist for comment

a.   This is the first of several steps with specific time targets.

b.   Not all audit-related reports are issued in draft. The Glossary in Appendix A lists the most common audit-related reports and when each one is appropriate.

c.   The OIG sends hard copy draft audit reports to affected Executive(s), and CP. In addition, CP receives and distributes an electronic copy for consolidating comments and change requests from all affected offices. CP works with the auditor on behalf of the Archivist and Audit Resolutions Officer to ensure that all appropriate NARA Executives receive a draft report for comment and that comments reach the OIG in a timely manner.

TYPICAL DRAFT REPORT TIMETABLE

Day 1 through 10	Day 10 through 20	On or before day 30
Management reviews draft and may create a markup version for discussion. The need for a markup varies with the complexity of the report and findings.	OIG considers comments and requests for changes and may issue a revised draft report.	Formal comments signed by the Archivist and sent to the OIG. These are included in final report

S-9

d.   As depicted above, the 30 day draft report response time is easily divided into three segments. The first 10 days should provide sufficient time for management review and informal comments. The comments should be conveyed in writing, and may take the form of an email or markup of the draft report. It is usually helpful to discuss these comments, so around the 10-day mark, management and the OIG meet to discuss proposed changes and any documentation provided by the program area to support proposed changes. We expect that some changes will be accepted and some not.

e.   During the second segment, 10 to 20 days, the OIG considers discussions and requests for changes, and other documentation that may be provided. Finally, as early as practicable in this segment, a revised draft may be issued.

f.   In the third and final segment, comments and changes not accepted are evaluated by management for inclusion in the formal comment memo. Formal comments for inclusion in the final report must include the following:

(1)   Whether management concurs, partially concurs, or does not concur with each recommendation;

(2)   Explanations for any disagreements with report findings, conclusions, or recommendations; (3) High level plans for implementing corrective actions[1]; and

(4)   Any additional documentation management has to support its positions.

> GAO draft report to
> the Archivist for
> comment

g.   The process for commenting on a GAO draft report is very similar to that of OIG draft reports. Comments are due within 30 days unless otherwise requested by GAO. GAO does not provide revised draft reports, so formal comments can include an attachment with technical comments to accommodate things not addressed through the statement of facts. On behalf of the Archivist and Audit Resolutions Officer, CP coordinates response preparation and establishes internal deadlines based on GAO suggestions.
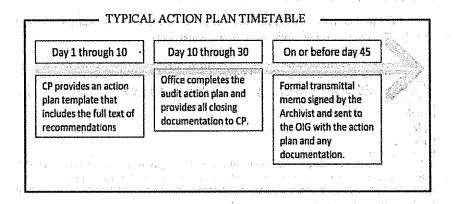
> Final report issued to
> the Archivist and
> others as required

> Action plan approved
> by the Archivist and
> sent to auditor

---

[1] Detailed plans for corrective action, including major milestones, documentation, and a timetable are provided in an action plan after the final report has been issued.

S-10

h.   OIG – The final audit report is addressed to the Archivist with a copy to CP, the appropriate Executive(s), and the unit(s) involved in the entrance and exit conferences. The report includes the written comments NARA officials provided on the draft reports, and OIG responses to those comments. We must respond with an action plan for implementing report recommendations and status reports on any completed or in-progress implementation efforts within 45 calendar days (see m. below).

SPECIAL NOTE about final audit reports: The OIG posts most final reports on the internet. Each final report cover letter includes a request for redaction suggestions and provides a timeframe for response (usually 7 days). Redaction discussions are between the Executives (or designees), the OIG, and NGC.

TYPICAL ACTION PLAN TIMETABLE

Day 1 through 10	Day 10 through 30	On or before day 45
CP provides an action plan template that includes the full text of recommendations	Office completes the audit action plan and provides all closing documentation to CP.	Formal transmittal memo signed by the Archivist and sent to the OIG with the action plan and any documentation.

i.   GAO – The final audit report is addressed to the Archivist with a copy to CP. Comments on final reports are due to GAO within the statutory 60-calendar day time limit. Copies are sent to OMB, the Chairman of the House Committee on Government Operations, and the Senate Committee on Governmental Affairs.

j.   Executives, staff directors, and managers prepare responses to the report's findings, conclusions, and recommendations, and identify any actions taken or planned in response to each recommendation. Action plans (for internal use only) are sent to CP with responses, but the action plans are not forwarded to GAO. Final responses are signed by the Archivist and addressed to the GAO official who signed the report. CP provides the OIG and appropriate management officials with a copy of the final responses.

S-11

k.   An action plan is a commitment to do something in a certain timeframe that will satisfy an audit recommendation. Executives, staff directors, and managers prepare action plans, including realistic target dates, addressing the recommendations in the final audit reports. Action plan items estimated to take longer than 120 days to implement must have phased steps at intervals of no more than 60 days. Revised action plans must be submitted to CP when an office determines that target dates cannot be met or within 15 calendar days after its target dates are missed. CP notifies the OIG.

l.   Recommendations implemented before, or when, final reports are issued are not included in action plans, but must be addressed in the cover memorandum transmitting the action plan. Include documentation supporting implemented items.

m.   Action plans in final draft form for OIG audit reports are due to the OIG 45 calendar days after the final report is issued. This begins a discussion period resulting in agreement between the program and the auditor on actions that will be taken to satisfy a given recommendation. Any lack of agreement will be adjudicated by the Audit Resolution Officer, and the Archivist will sign the final action plan.

n.   Action plans for GAO audit recommendations are due by the deadline established by CP. CP provides the OIG with copies of the action plans.

S8.   **Resolution**: correcting as appropriate and advising on progress ➤

> Auditor concurs with
> plan or provides
> feedback

a.   All recommendations exist in one of two states: open or closed. Only the auditor can decide that a recommendation is closed. But what happens when management does not agree with a recommendation or the auditor does not agree on the actions proposed to resolve a recommendation?

b.   OMB A-50 describes an open recommendation as either resolved or unresolved. When management and the auditor are unable to agree on action to be taken on reported findings and recommendations, the Audit Resolution Official evaluates the information presented by both the auditor and management and makes the final determination on what action(s) to take.

(1)   Unresolved (Open) – Recommendations are classified as unresolved until there is agreement between management and the auditor on management's implementation action plans, or until disagreements about the implementation are resolved by the audit resolution official.

(2)   Resolved (Open) – Recommendations are classified as resolved when the auditor agrees with the action plans proposed by management, or the audit

S-12

resolution official has resolved disagreements about implementation. This could include a statement that accepts the business risk of taking no action or a lesser action than recommended.

(3) Closed – Recommendations are classified as closed when action plans have been completed and accepted by the auditor. Although management may believe that no further action is required, only the auditor can classify a recommendation as closed.

> Documentation provided to the auditor and CP per action plan

c. Each Executive, staff director, and manager is accountable for satisfying audit recommendations related to its functions and programs. This includes completing actions by the targeted due date and providing agreed upon documentation to the OIG and CP. CP is available on request to review documentation and provide feedback prior to submitting it to the OIG.

> Progress reports to the Archivist, inclusion in assurance statement if appropriate

d. Audit progress reports at NARA are incorporated into the management assurance statement process. At a minimum, reporting should include basic, descriptive information about the audit, how many recommendations remain open and whether we expect to meet the target due date for actions. Information about recommendations that are past due should include why the date was not met, how we are mitigating the risk associated with the recommendation, and when we expect to complete the action(s).

e. Due dates for progress reports change annually based on external due dates. Specifics are found in interim guidances in the 160 series (Internal Controls).

f. CP submits semi-annual summary level progress reports to the OIG, the audit resolution official, and the Archivist on the resolution and implementation of audit recommendations during the previous 6 months. These reports provide narrative and statistical information on recommendations completed during the reporting cycle and the status of incomplete recommendations.

Appendix A, Glossary of Terms

Action plan. A document prepared in response to an audit by the program office that includes the action(s) the office will take to close the recommendation, planned completion date(s), and the documentation to be sent to the auditor. Appendix B shows an action plan template with instructions for each field.

S-13

Advisory Report. This report type is a mechanism recently has been used only for ERA updates. There is no formal definition for this report type in GAGAS.

Audit. An independent, objective, nonpartisan assessment of the stewardship, performance, or cost of government policies, programs, or operations, depending upon the type and scope of the audit.

Audit Memorandum. Audit memoranda are another method of communicating results of audits. They are used to address findings or deficiencies that are judged by the auditors not to be material or significant enough for inclusion in a formal audit report, or if there are no findings to report. A corresponding audit report should reference any findings communicated through the audit memoranda and should state that "other findings were reported to management in an audit memorandum".

Audit Report. A document issued by the auditor that contains: (1) the objectives, scope, and methodology of the audit; (2) the audit results, including findings, conclusions, and recommendations, as appropriate; (3) a statement about the auditors' compliance with generally accepted government auditing standards (GAGAS); (4) a summary of the views of responsible officials; and (5) if applicable, the nature of any confidential or sensitive information omitted.

The purposes of audit reports are to (1) communicate the results of audits to those charged with governance, the appropriate officials of the audited entity, and the appropriate oversight officials; (2) make the results less susceptible to misunderstanding; (3) make the results available to the public, unless specifically limited as with classified and internal use reports; and (4) facilitate follow-up to determine whether appropriate corrective actions have been taken.

Closing a recommendation. A recommendation is closed when management has implemented the agreed actions and required documentation is submitted to and approved by the auditor.

Documentation. Evidence showing that an action has been taken to close a recommendation. Required documentation is described and approved by the auditor in the action plan.

Finding. Statement made by an auditor in an audit report that defines the situation as it exists (condition), the required or desired state (criteria), the reason or explanation for the difference between the situations (cause), and the effect or potential effect that identifies the outcomes or consequences of the condition.

Management Letter. Management letters constitute another form of written communication between the OIG and NARA management. They are used to address issues that need to be quickly brought to management's attention and are addressed to the Archivist with a cc: to the affected office(s) and CP.

Recommendation. Actions to correct deficiencies and other findings identified during the audit and to improve programs and operations when the potential for improvement in programs, operations, and performance is substantiated by the reported findings and conclusions. These should flow logically from the findings and conclusions, are directed at resolving the cause of identified deficiencies and findings, and clearly state the actions recommended.

S-14

Resolution. (1) For most audits, the point at which the audit organization and agency management or contracting officials agree on action to be taken on reported findings and recommendations; or, in the event of disagreement, the point at which the audit resolution official determines the matter to be resolved. A report may be considered resolved despite the right of persons outside the agency to negotiate, appeal, or litigate. Resolution of a report with respect to parties outside the Government does not preclude further consideration of issues in the report by agency management. (2) For pre-award contract audits, the point at which the agreement is reached, a contract price negotiated, or proposed award canceled, whichever occurs first. (3) For GAO reports, the point at which the agency responds to the Congress, as required by the Legislative Reorganization Act of 1970.

Responsible office. The office that leads efforts toward resolution of a recommendation and its related action(s). This is most important when more than one office is affected by an audit.

S-15

Appendix B, Action Plan Template

CP provides a template for every audit with recommendations to each affected office. The template will include the number and text for each recommendation found in the audit.

Recommendation Number: Filled in by CP

Recommendation: Filled in by CP

Management discussion: Relates to our approach to the recommendation, not the actions we will take. For example, issuing a bulletin is an action. The background leading up to the need for a bulletin is a discussion point. Actions will then follow the discussion points. **This is an optional field – we will not always have the need for background**

Actions already taken: *Actions already taken* cover the time period from the beginning of audit fieldwork to the date of the action plan. We need to show how these actions affect the final product, and if not completed, account for potential changes in the interim milestones. **This is an optional field – we will not always have completed actions**

Action to be taken: *Action(s) to be taken* are steps with deliverables.

Planned completion date: The date we expect to be able to get the documentation to the auditor. That date requires that we have drafted, vetted, and done in final form whatever documentation will satisfy the recommendation. Often we can deliver a final draft and tack on a reasonable amount of time to implement it. The final then, is either a new final draft or a report on how well the first one worked. To comply with NARA 1201, Audit Resolution (and OMB-50) if a planned completion date goes out more than six months, we must provide interim milestones with dates. In effect, we are sending an update every six month to the audit entity (OIG, GAO, etc) that shows progress against the interim milestones - not a bad idea anyway, because it will show how serious we are even if we are slipping on dates.

Documentation to be sent: There is a recommendation and some 'thing" or "things" that will satisfy (totally close out) that recommendation. This is the *documentation to be sent*. It proves that we did what we set out to do, whether it is issuing a bulletin, developing a plan, or implementing a plan. Appendix C lists examples of documentation that is expected for certain types of recommendations.

Appendix C, Documentation Requirements

The following table provides examples of actions and documentation that follow from common recommendations.

Recommendation says	You do	Prove it
Develop, implement, and document a formal mechanism	Create or update a policy document such as a directive	Copy of final directive
Evaluate benefits and implement automated integrated researcher registration system	Establish working group to submit recommendations	WG recommendations and memo detailing next steps and assigning responsibility
Revise policy to include specific items	Revise policy	Copy of revised policy with citations for specific changes
Ensure risk assessments for major applications happen every three years	Create a schedule; conduct a risk assessment; generate a memo to file if system is no longer active	Provide access to completed risk assessments
Conduct training	Create or revise training and then conduct training	Describe training medium, access to or a copy of training, names and dates for attendees
Enforce a more formal, centralized process	Review current processes and revise as needed. ID internal control points to monitor and test. Evaluate test results, take action as appropriate	Copy of (revised) process, test plan, evaluation results with recommendations
Improve agency-wide inventory of large items	Assess inventory against documentation. Create plan to improve. Implement plan.	Results of assessment, improvement plan, implementation plan.
Implement and monitor controls	Create test plan. Follow the plan.	Results of tests

Contents

CHAPTER 3 – NARA OIG TEAMMATE PROTOCOL

1. INTRODUCTION

TeamMate Electronic Work Papers (EWP) is an audit management system developed and supported by Wolters Kluwer that enable us to move towards a paperless environment and bring efficiencies to our planning, fieldwork, review, reporting, and archival processes. Our TeamMate environment is maintained and managed by the NASA OIG.

TeamMate is our standard application for documenting our projects. While TeamMate does not replace performing the detailed work, it does provide a common platform for documenting, reviewing and sharing work during and after the project.

NARA OIG prepared this document to establish the standards and protocols that will be followed in performing all OIG audits. TeamMate on the Web also contains other TeamMate help files.

2. NASA OIG ENVIRONMENT ACCESS
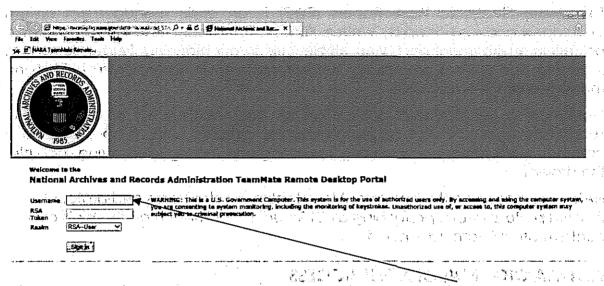
NASA has developed a web portal that allows users of the environment to access TeamMate from any computer that has an internet connection. However, it is the NARA OIG's policy for Auditors to only access this environment from a NARA OIG furnished laptop. This ensures that Auditors are accessing our audit work from a secure computer. The NARA OIG can access the NASA OIG environment from this website: https://naraoig.hq.nasa.gov/dana-na/auth/url_53/welcome.cgi?p=no-cert. In order to access the website and environment the user must have Active X enabled in their web browser. Typically this requires NARA IT staff to install it on your computer. The web browser of choice to access this environment is Internet Explorer (IE). However, once Active X is installed in IE, a user can access the environment using an IE plugin for Chrome. See **Andrew Clements** if you would like to have this plugin installed. NASA requires two factor authentication to access the environment. An auditor can access the environment by using either a RSA Token and PIN code along with a domain password or personal identity verification (PIV) card and PIN code.

<u>RSA Token Access</u>

In order to access the NASA environment using the RSA Token, the Auditor must determine if they want to use a RSA soft token issued to their NARA issued
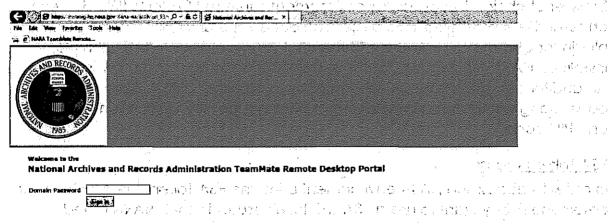
cellphone or a separate hard token that needs to be carried around. Either way NASA will issue the token for the Auditor to access the environment. Once the token is issued the user must create a PIN and Domain password with the help of NASA. When you go to the web you will see the following login screen:
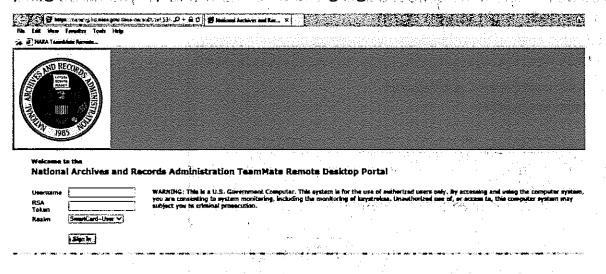

On the login screen you would enter your NASA assigned Username, which should be the same as your NARA assigned Username. Then in the RSA Token field you must first enter your 8 digit PIN followed by the code randomly generated by the RSA Token. Next ensure the Realm drop down says RSA-User. Then click Sign In.

Next you must enter your Domain Password. NASA's policy is for this to be a 12 digit with a combination of upper and lower case letters, numbers, and special characters. Once the password is entered then Click Sign In.
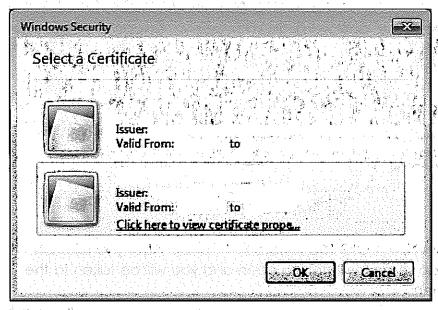
PIV Card Access

In order to access the NASA environment using a PIV card, the Auditor must contact NASA so they can capture the certificate stored on the card. When you go to the web you will see the following login screen:
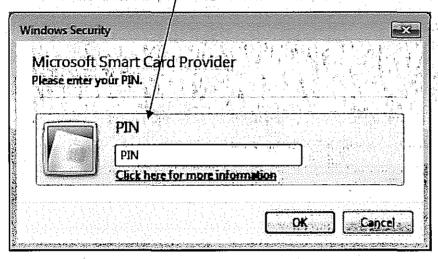
On the login screen you need to select change the Realm drop down box says SmartCard-User. Then put your PIV card into the card reader and click Sign In. Next the following pop-up box will appear asking you to select the certificate you want to select (typically it's the second one but not always) then click OK:
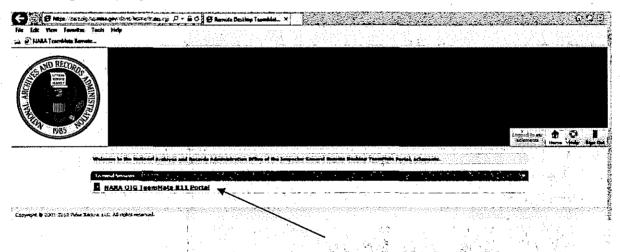
If you select the correct certificate, another pop-up will open and you will be asked to enter your 8 digit PIN assigned to the certificate on your PIV card. If you do not select the correct certificate or enter the wrong PIN you will be taken to the NASA login screen again.

NASA Environment
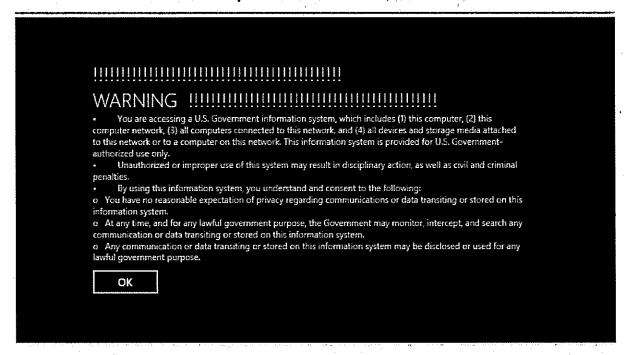
Once you are logged into the NASA OIG environment you will be taken to the following webpage:
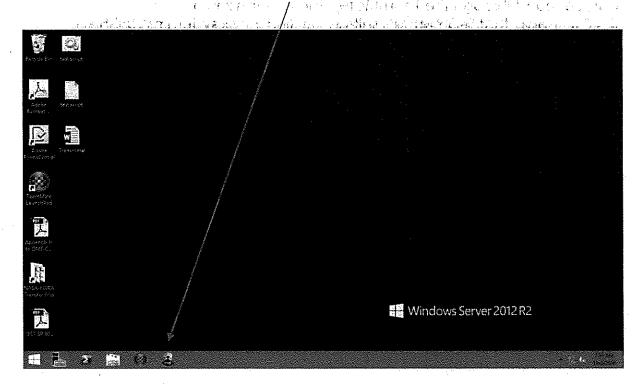
Click on the link that says NARA OIG TeamMate R11 Portal. After you click on the link a remote desktop session will start to open and you will be taken to the following Warning Banner:

WARNING !!!

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:

o You have no reasonable expectation of privacy regarding communications or data transiting or stored on this information system.

o At any time, and for any lawful government purpose, the Government may monitor, intercept, and search any communication or data transiting or stored on this information system.

o Any communication or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

OK

Ensure you read the Banner and click OK. You will then enter NARA's TeamMate environment NASA setup for us. In order to access NARA's audit projects click on the EWP Icon and the TeamEWP Explorer window will open.

3. PROTOCOL SHORT CUTS

This section presents a brief overview of the major OIG protocols required for TeamMate users.

Set-up

On the Browser Screen, after selecting the New Audit button, the New Audit Wizard will prompt you to enter information. For "Code," enter the project number received from the Assistant Inspector General for Audits (AIGA). For "Name," enter the title of the audit from the announcement memorandum. For "Unit," enter NARA OIG.

Evidence for audits should only appear in the B folder and below section of the CG Program Groups. All sections of the A folder must be completed or a waiver received from the AIGA. Note: Not all boxes within procedure summaries, exceptions, and the audit profile have to be filled in. For example, TeamMate includes a box to assign work papers to audit team members however; this is not needed in our current environment.

Attachments should contain a hyperlink to the procedure they belong to and the attachment source information should be entered in the "Source" box of the procedure. Any attached documents should have descriptive titles so they can be found through the TeamMate search mechanism.
It is OIG policy that TeamMate's self-generating index system establishes a sufficient index. No additional indexing/numbering is necessary.

Replications

NASA OIG hosts NARA's TeamMate environment. As a result, we are able to access the environment from any location that has an internet connection and no longer have a need for replicas.

References/Attachments/Work papers

Microsoft Excel and Microsoft Word should not be opened before you open TeamMate. Make sure to close Excel and Word before executing TeamMate. Opening Excel or Word before executing TeamMate may cause problems and result in loss of data.
Monitor the size of documents imported into TeamMate. If possible, scan or import only the pages needed to support work papers or exceptions. Two-way hyperlinking should be used whenever it makes sense.

Exceptions/Findings

The Exceptions section should be used as a "work in progress" section where all potential issues are recorded throughout the audit, evaluated, and then developed into a finding or deleted if found to be a non-issue.

Coaching Notes
Coaching notes must be used to show supervisory review and must be retained when the audit is finalized. All coaching notes must be signed off before issuance of the final report.
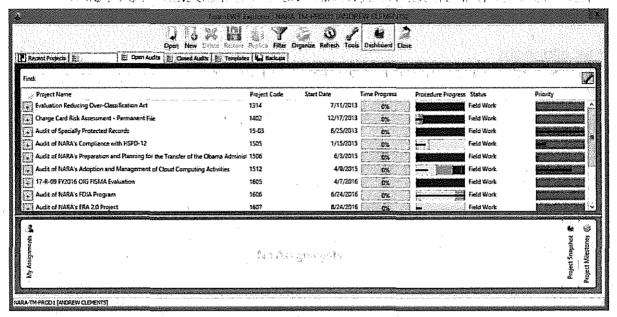
Miscellaneous
Classified information should not be stored in TeamMate.

---

4. SETTING YOUR TEAMMATE PREFERENCES

The TeamMate Explorer is a viewer that displays project files by file directory location.

You should think of the TeamMate Explorer as an electronic filing cabinet. Just as an office file cabinet has multiple "drawers," the TeamMate Explorer has multiple "tabs." Each "tab" maps to a directory on the NASA server.

Project Locations

By default there are 5 tabs installed with TeamMate:

- **Recent Projects** – Displays the last 25 projects recently accessed. The number (25) can be set in Tools | Preferences | Explorer tab. This tab is helpful in locating any projects you have recently worked on.

- **Open Audits** – Displays Open Audits in the centralized database. Open audits include audits that have not been finalized - final report and/or working papers are not complete.

- **Closed Audits** – Displays all closed audits. Closed audits include audits that have been placed in Issued state and are finalized.

- **Templates** – These are our default templates that we use.

- **Backups** – This is blank

5. STORING THE MASTER FILE DURING THE PROJECT

The TeamMate Master Project file (Open Audits directory) will contain all associated documentation for that project.

Centralized Database

TeamMate audits are stored on the centralized database on the server. New auditors are added to the list of users by the teammate champion. After an audit is created in TeamMate, the administrator can add users to work on the audit from the list of users as needed. Only users in each audit may change work papers in the audit. A history of user access and dates are kept on each work paper.

NARA Policy:

- While **working in or outside the office**, Master projects will be stored on the centralized database and contain open (ongoing) audits.

- **Replicas**, via **Update** files, are not to be used by the OIG.
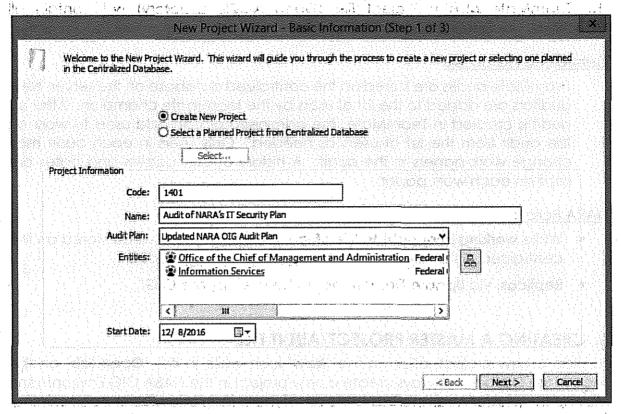
6. CREATING A MASTER PROJECT/AUDIT FILE

To plan a new project, click on the **'New'** icon while in the **'Open tab'** on the TeamMate Explorer. Always create a new project in the NASA OIG Environment. Moving the Master Audit increases the risk of more than one Master Audit existing. You cannot merge data from two Master Audit files. In addition, moving the Master file increases the risk of audit backups being stored on the same drive as the Master Audit.

Naming the Project

New Project Wizard - Basic Information (Step 1 of 3)

Welcome to the New Project Wizard. This wizard will guide you through the process to create a new project or selecting one planned in the Centralized Database.

⦿ Create New Project
○ Select a Planned Project from Centralized Database

Select...

Project Information

Code: 1401

Name: Audit of NARA's IT Security Plan

Audit Plan: Updated NARA OIG Audit Plan

Entities:
Office of the Chief of Management and Administration   Federal
Information Services   Federal

Start Date: 12/ 8/2016

< Back   Next >   Cancel

Code:	Example: 1401
	1401 is the first project started in FY 2014. The AIGA will assign project numbers.
Name:	Example: Audit of NARA's IT Security Plan
Audit Plan:	Choose the most recent audit plan
	NARA OIG is the owner of this audit

Entities: **Click on** [icon] **. This will open:**

Select all of the possible organizations relevant to the subject of the audit.
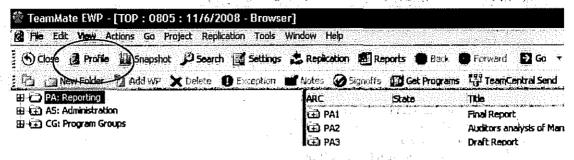
Start Date: Project Start Date – defined as the date that Field Work commences.
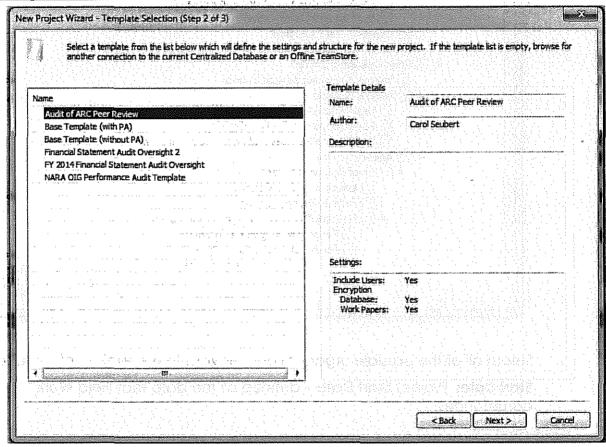
Click Next.
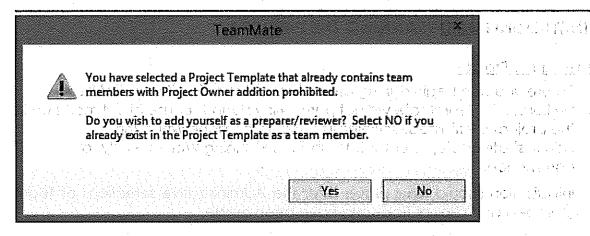
Note: The Code, Name, and Start Date can be updated in the Profile section, General tab, if needed.

Selecting a TeamMate Template

A TeamMate Library contains all standard planning information and department terms and standards, helps expedite the planning process, and provides assurance that our pre-defined best practices are included in every project file. Select the NARA OIG Performance Audit Template file and click next, the following dialog box will appear:

You have selected a Project Template that already contains team members with Project Owner addition prohibited.

Do you wish to add yourself as a preparer/reviewer? Select NO if you already exist in the Project Template as a team member.
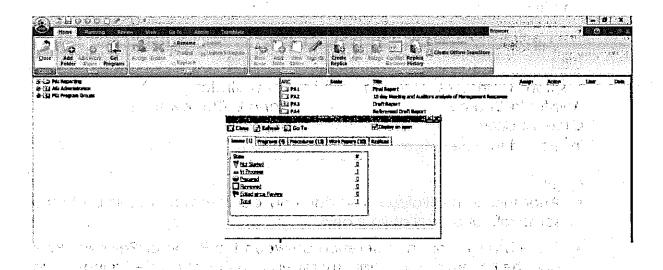
Select Yes and add yourself as a preparer/reviewer. Jewel Butler, AIGA and a TeamMate Administrator role have already been established in each NARA OIG Performance Audit Template. Enter your First Name, Last Name, Initials, and Title. Your login Name should already be filled in with your NASA login id. This version of TeamMate uses Window Authentication rather than passwords. As a result, once you log into the NASA environment you will automatically logged into TeamMate.

Click ok. The following snapshot and table of contents appears:

You are now ready to populate your audit file with data specific to the subject audit.

7. INITIALIZING AND PLANNING THE PROJECT

Initializing the Project

Before you can begin signing off work in a Master file, it must first be "initialized". TeamMate will not permit any signoffs or use of tickmarks until the project is initialized. Initialization should be done when the administrative setup is complete and the Planning Work is ready to commence.

Initialization should take place after the Administrative selections of Team Members and Global Tickmarks have been made.

Adding Team members, if needed

Most of our audits are one person audits, so adding team members may not be necessary until we add the person independently referencing our draft report.

To add team members within the project file, go to the Profile and open the Team Tab.

- Click "Get" and import the team member details, or

- Click "Add" and complete team member details.

Each NARA Auditor already has a profile in the TeamStore with his/her role and level.

Typical Roles and Levels have been defined as follows:

Title:	Role:
Assistant Inspector General for Audit	Administrator
Auditor-In-Charge	Preparer/Reviewer
Other Auditors	Preparer
Independent Referencer	Preparer
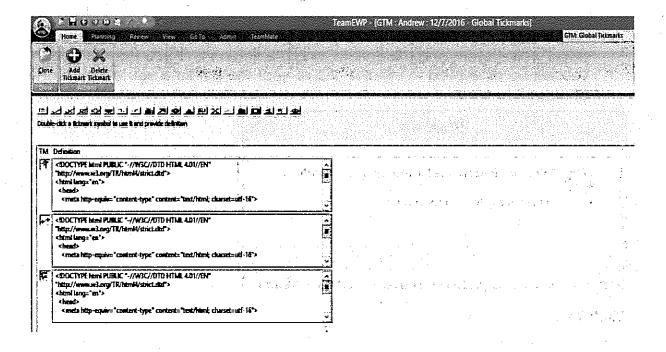
Note:
- After the file is initialized, you can only add team members up to the same role and level as your own.

- There is an important difference between the Preparer/Reviewer Role and the Reviewer Role. Team members with the latter role cannot make any edits to a project file other than signing documents off and raising coaching notes.

- Because most audits have only one auditor assigned, that person will have a preparer/reviewer role.

- The independent referencer will need to be manually added as a team member. Do not 'Get' from the TeamStore. Add 'Independent Referencer' in the title of the person whose role is to independently reference the draft report.

Adding Global Tickmarks

The following five global tickmarks are included in every audit set up using the NARA Standard Audit.tml. Prior to initializing, additional global tickmarks can be set up for use in all workpapers.

After initialization, tickmarks can be created specific to each workpaper, but cannot be used on any other workpaper. Provide Carol Seubert ideas for other global tickmarks to include in the
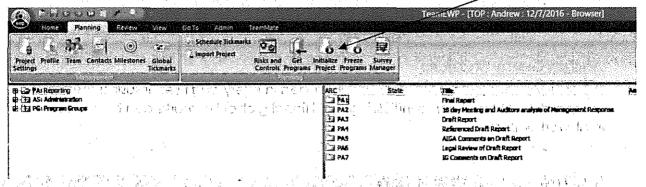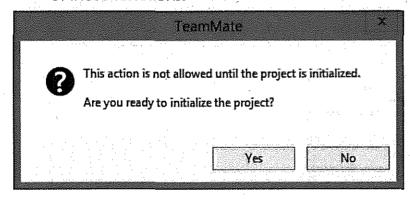
NARA Standard Audit.tml file

Initializing the Master File

From the Browser, select the Planning menu | Profile | Status and Milestones Tab. Check the Field Work (Initialize) box, and then click Yes. Another way to initialize a project is go to the Planning tab and select Initialize Project.

Remember: You must first initialize your file so that you can sign off procedure steps, workpapers, and exceptions, and use tickmarks. If you forget to do so, you will be prompted to initialize the project the first time you attempt one of these functions.

Click Yes.
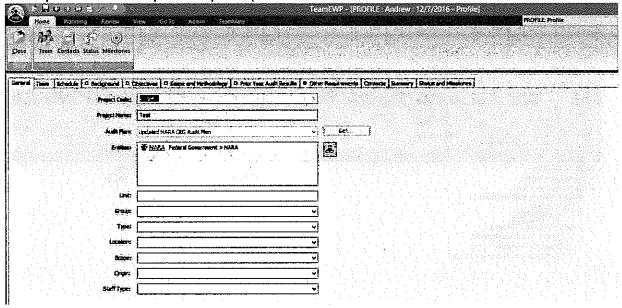
8. PLANNING THE PROJECT

The planning process is considered an essential part of NARA OIG audit process. See Chapter 2 of our NARA OIG Audit Procedures Manual for more information.

The Profile section summarizes the subject audit title, project number, background, objectives, scope, methodology, milestone, staff hour estimates, and requirements such as travel, contracted audit services, or use of consultant
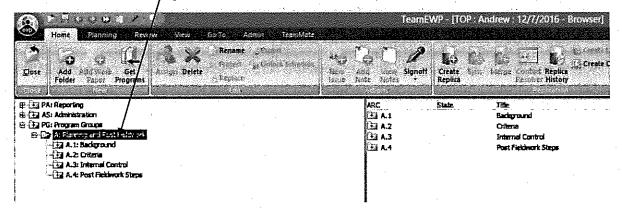
and specialist as required by Chapter 2.3 of the NARA OIG Audit Procedures Manual.
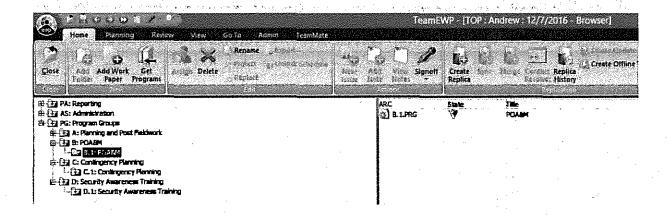
Then you must complete the fields in the General Tab of the Profile section of EWP.

This information can be developed as the auditor completes GAGAS Field work standards for performance audits. Audit steps have been established in the A.1, A.2, and A.3 folders consisting of planning steps to ensure each audit is adequately planned and folder A.4 are the Post Fieldwork steps. Auditors will develop their audit guide and specific audit steps based on the work done in sections A.1 through A.3 as they document their understanding of the subject audit and develop audit steps necessary to address the audit objectives.

Using data acquired in section A, the auditor will develop Procedure Summaries and steps in sections B, C, D, and so for the, as necessary, representing each major work area or segment of a project.
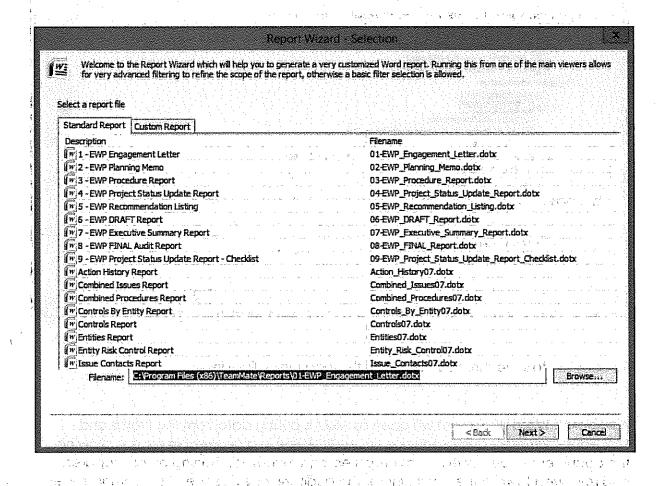
Each Procedure Summary, i.e. A.1.PS, represents each major work area or segment of a project. The steps within each Procedure Summary are necessary to complete to address the objectives of the audit. The auditor will summarize the results of the work performed for each step. See Chapter 4 of the NARA OIG audit manual for more information of what needs to be included in summarizing work paper sections.

The auditor will generate an audit guide using the reporting tool which pulls all the audit steps developed in the Procedure Summaries into a Word document, along with the background, objectives, scope methodology and staff hour estimates from the Profile. The AIGA, who is the approving official for the audit guide, must electronically sign and date the document. The audit guide, located at AS2.f will document the approved audit guide. The auditor will use the Procedure Summaries as the audit guide to monitor, control, and redirect resources toward accomplishing the audit objectives. The audit guide may need to be revised in response to unforeseen events or problems. Under these circumstances, any changes to the audit guide must be approved by the AIGA. See Chapter 2.3 of the NARA OIG Audit Procedures Manual
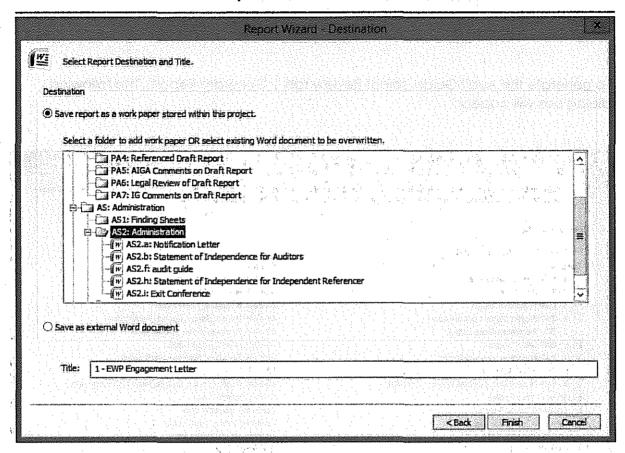
To generate the Audit Guide, select Review tab | Generate Report. The following dialog box will appear:

Select Audit Guide. The File Name should default to the NASA S:\TeamMate\Custom Reports drive. Select report and click next.
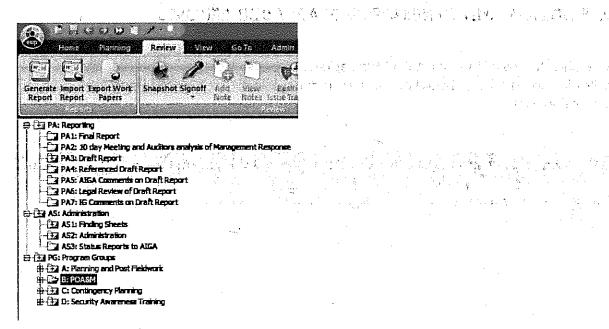
Select AS2.f to save the Audit Guide at this location. Click Finish.

A Microsoft Word document will open as AS2.f is pulling data from the Profile and Procedure Summary and producing an Audit Guide in a reviewable format allowing the document to be signed off as prepared and reviewed. Signing off as prepared and reviewed toward the beginning of the audit shows evidence of supervisory review of the audit guide, as required by the Chapter 2.3 of the NARA OIG Audit Procedures Manual.

Work done to perform audit steps necessary to address the audit objectives will be documented in Procedure Summaries using the Purpose, Source, Scope/methodology, Conclusion, and Results fields and supported by and referenced to other work papers.

Other Planning Items:

Other standard folders for each audit include:

Audits conducted by the NARA OIG also include the following standard work papers:
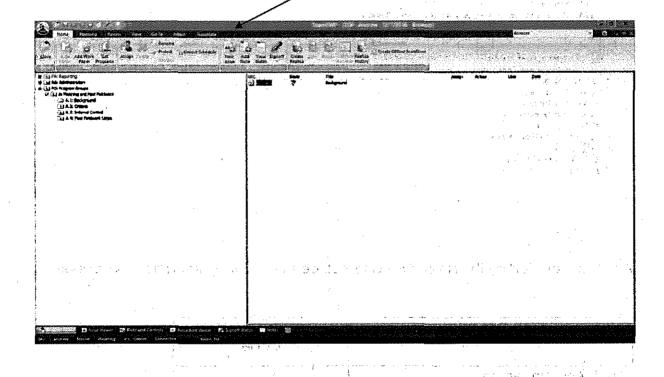
Work Paper Title	Work Paper Index Code
Audit Announcement	AS2.a
Auditors, AIGA, legal counsel and IG's Statement of Independence	AS2.b
Entrance conference	AS2.g
Exit conference	AS2.i

GAGAS Certification	PA3.a
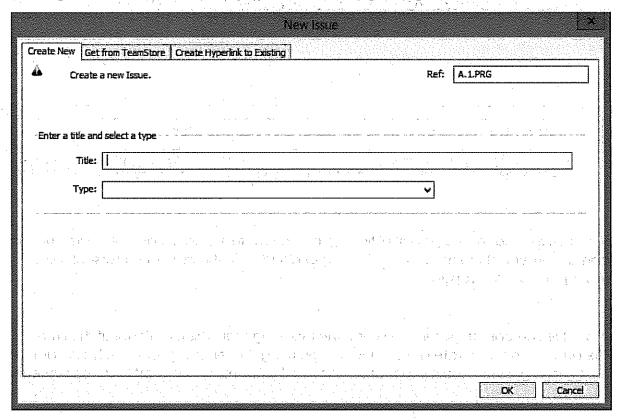
Implementation of recommendations by the cognizant offices and OIG follow-up
reviews of corrective actions taken by management are performed in separate
projects outside of each audit file.

9. FINDINGS AND GENERATING DRAFT AUDIT REPORTS

See Chapter 2.6 of the NARA OIG Procedures Manual. When auditors identify a
potential finding, they should prepare a Finding Sheet in section AS1 using the
exception tool.
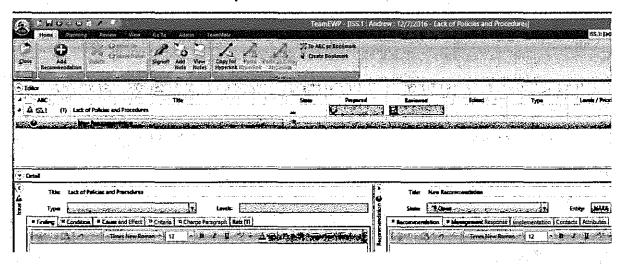
Clicking on the exception icon will open the following dialog box:

New Issue

| Create New | Get from TeamStore | Create Hyperlink to Existing |

⚠ Create a new Issue.   Ref: | A.1.PRG |

Enter a title and select a type

Title: [   ]

Type: [▼]

[OK] [Cancel]

More than likely, the auditor will be developing a new exception specific to their audit.

To create a new exception/finding, give the new exception a title. No type is necessary.
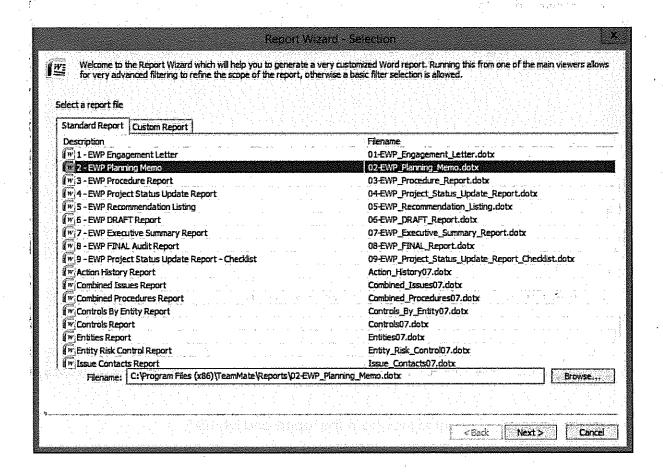
When auditors identify a potential finding, in TeamMate it is called an issue. The auditor can document all the necessary elements of a finding in the issue and cross-reference to supporting work papers.

A draft report can be generating using the reporting tool. This is optional at this time. The auditor can generate a draft audit report using the reporting tool which pulls all the issues/findings and certain information from the Profile into a Microsoft Word document.

The draft report should be saved to folder PA3. The draft report generated is not a final document. It provides a good starting point for ensuring all issues are included in the draft report. However, tone, logical flow, executive summary, charge paragraphs, and other language will need to be tweaked for draft report issuance. For instance, you may find that several exceptions written up really relate to one cause and will be summarized in one section of the draft report. It is stressed that the draft report generated is just your initial starting point for writing your draft report. For example, pictures, tables, and charts are encouraged to be added for clarity of issues.

To generate the Draft Report, select Review tab | Generate Report. The following dialog box will appear:

Select Draft Report. Then select the location you want to place it. Then hit NEXT.

Report Wizard - Data Preview

Select Filter to change the data. If initiated from within a viewer, select Cancel and use the Advanced Filters in the viewer to get more refined filtering.

Filter...

Title	Type
☑ Lack of Policies and Procedures	

Use checkboxes to determine what is included and use your mouse to drag-n-drop to reorder items

Unselect All

< Back   Next >   Cancel

Select the Findings you want to include in the report and hit NEXT.

Report Wizard - Destination

PF≡ Select Report Destination and Title.

Destination

⦿ Save report as a work paper stored within this project.

Select a folder to add work paper OR select existing Word document to be overwritten.

```
⊟ 🗀 PA: Reporting
    🗀 PA1: Final Report
    🗀 PA2: 10 day Meeting and Auditors analysis of Management Response
  ⊟ 🗁 PA3: Draft Report
        📄 PA3.a: GAGAS Certification
    🗀 PA4: Referenced Draft Report
    🗀 PA5: AIGA Comments on Draft Report
    🗀 PA6: Legal Review of Draft Report
    🗀 PA7: IG Comments on Draft Report
⊞ 🗀 AS: Administration
⊞ 🗀 PG: Program Groups
```

○ Save as external Word document

Title: | 6 - EWP DRAFT Report |

[< Back] [Finish] [Cancel]

Select PA3 to save the Draft Report at this location. Click Finish.

A Microsoft Word document will open as PA3.d or the next available ARC. TeamMate is pulling data from the Profile and Exceptions section produce a Draft Report in a revisable Microsoft Word document.

10. BACKING UP THE FILE

Backing up electronic work papers is very important. As a part of the service NASA provides us the automatically conduct full backups every weekend and nightly incremental backups. Incremental backups are only copies of the changes that were made to projects during the day not a backup of all the projects.

11. CREATING A REPLICA

NARA does not use Replicas anymore because we can access the NASA environment from any location that has an internet connection.

12. SCANNING

TeamMate can incorporate scanned images into the file. TeamImage software is included with TeamMate. However, it is highly recommended that auditors save scanned documents as PDF and not TeamImage because of the size of a TeamImage file.

13. INDEPENDENT REFERENCING

To ensure the quality of our work, the OIG Office of Audits Procedure Manual requires that audit reports be independently referenced prior to being issued in draft. Referencing is the process of marking a report (or a summary workpaper or an exception) with the location of the evidence that supports it. Referencing checks the accuracy of information contained in the report. To do so, the independent referencer generally verifies that the indexed information is sufficient and appropriate to support the report.

You can use TeamMate's electronic linking features to simplify the indexing process. When writing the report, insert the appropriate link to point others directly to the source. Thus, the user can electronically jump from one location to another by clicking the link indicator. EWP offers four electronic linking capabilities:

- Creating a bookmark and linking to it,

- Linking to an ARC (i.e., to an attached file)

- A one-way hyperlink, and

- A two-way hyperlink.

Which type of link to use depends on the format of the destination, i.e., the supporting documentation.

Note: The auditor should not link to a web site, since web addresses often change or cease to exist. If you wish to add a web page, save the page to a file and import it. Do not create links that would be broken once the audit is finalized and stored, such as linking to a document that is not in TeamMate.

14. PROJECT WRAP-UP

To preserve a finalized project file and protect from changes, TeamMate contains a finalization process that checks each procedure step, procedure summary, exception, supporting workpaper, and coaching note for prepare and review sign off. Then the process converts all team roles to read only. In the unlikely event that changes to the project file are required after finalization, TeamMate also creates an emergency back up copy of the master file that can be restored. **Only a team member with Reviewer rights, at minimum, can perform the finalization process.** This function is available under the Project | Finalize pull-down menu option.

It is our policy to run the finalization process only after issuance of the final report and approval from the AIGA. Each auditor is responsible for finalizing their project. Auditors should work with the AIGA to ensure all steps are signed off and all coaching notes have been addressed.

BEFORE FINALIZING—the auditor must create a guest account (set up the password as "password") with view only privileges. Also, change the project name to include the final report number (For example, the new project name would be: "14-01 Audit of XYZ").

It is also our policy to discontinue finalization if, during the finalization process, TeamMate detects any of the following:

- Procedure steps not signed off as prepared and/or reviewed
- Work papers not signed off as prepared and/or reviewed
- Exceptions not signed off as prepared and/or reviewed
- Coaching notes not addressed and cleared

Coaching Notes provide the opportunity for effective communication throughout the audit, and also provide evidence of supervisory review. Coaching Notes become a permanent part of the finalized audit because they provide evidence that an audit review took place. **It is OIG policy that all coaching notes be retained.**

BEFORE FINALIZING:

- The auditor must create a guest account (set up the password as "password") with view only privileges.
- Also, change the project name to include the final report number (For example, the new project name would be: "14-01 Audit of XYZ").
- Under Planning tab | Profile | Schedule tab make sure the actual end date reflects the date the final report was issued.
- Profile | status and milestones tab - complete milestones

- Profile | status and milestones tab - check the boxes first then change the date:
  - Post Field Work (Draft Report) - add actual date draft report was issued;
  - Responses Accepted - add actual date response received and
  - Issued (Final Report) - add actual date of final report.

FINALIZING: Go to the Review menu | Finalize and follow the instructions.

15. UPDATING THE TEAMSTORE AND LIBRARIES AND REPORTS

Periodically, we will update our standard Audit Templates, TeamStore files, and Reports.

- For example, we may change a planning procedure step contained in the Audit Template or add a new work paper that should be completed in every project using a Library.

- We will periodically need to add new standard procedure steps and exceptions to the TeamStore for use on future projects.

TeamStore

A TeamStore contains a list of team member details, audit steps, work papers, and findings (exception) write-ups. You can simply click and import team members, audit steps, work paper templates, or findings into and audit file.

This is done within an audit under Planning Tab | Get Programs. A new window will open.
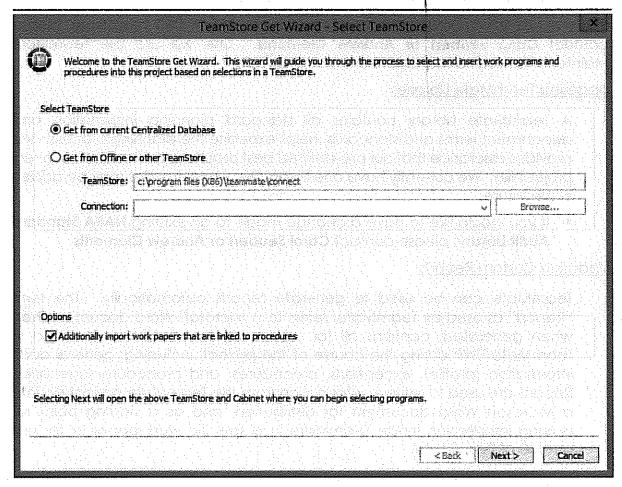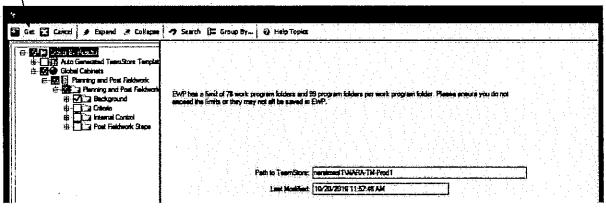
Select Next and you will be taken to the TeamStore Maintenance window. Select the Steps or documents you want to add from the left hand column then select GET.

If you would like to have a change made to the **NARA OIG TeamStore**, please contact **Carol Seubert or Andrew Clements.** She will use the TeamStore Maintenance tool to manage the NARA OIG.mdb.

Updating TeamMate Libraries

A TeamMate Library contains all standard planning information and department terms and standards, helps expedite the planning process, and provides assurance that our pre-defined best practices are included in every project file. We currently have one library file. More .tml files may be added in the future.

- If you would like to have a change made to an existing **NARA Standard Audit Library**, please contact **Carol Seubert or Andrew Clements.**

Updating Custom Reports

TeamMate can be used to generate reports automatically. The term "Report" as used by TeamMate, refers to a Microsoft Word document that, when generated, contains all (or subsets of) the data that is stored in TeamMate EWP during the course of the project, including: general audit information (profile), exceptions, procedures, and procedure summaries. Reports are used to retrieve information from the TeamMate project file into a Microsoft Word document for distribution, and as a starting point for revising information inside TeamMate in a specific work paper or for use outside of TeamMate.

16. TECHNICAL SUPPORT

A wide range of TeamMate support is available. If a challenge arises, you should consider the following options:

- Consult the **TeamMate On-line Help System**: Hit F1 from inside TeamMate to activate the On-Line Contextualised Help System.
- Consult the following **Quick Reference Guides:**

TeamMate Quick Reference Cards
Legend of TeamMate Symbols
Shortcut Keys for TeamMate
TeamMate 123
TeamMate Preparers Quick Guide
TeamMate Reviewers Quick Guide
TeamMate Replication Quick Guide
TeamMate Cross Referencing Quick Guide
TeamImage Quick Guide

- Consult the TeamMate EWP User Manual
- Consult the **Off-line TeamMate Support Guide dB**
- Consult the **TeamMate Support Guide dB** on the TeamMate Community Website:
- **https://www.teammatesolutions.com/Home.aspx**
- Contact those experienced with **TeamMate** in our office.
- Contact **TeamMate Support** as follows:

TeamMate AM and CM Support:

TeamMate's commitment to your organization's success extends well beyond the implementation of TeamMate Audit or Controls Management Software. Our expert support staff is available a minimum of eight hours per day, Monday through Friday, to assist our customers. Support is also provided outside business hours through our virtual 24-hour TeamMate Software Support Hotline, available by telephone in the United States, United Kingdom, Australia, and South Africa. We also offer TeamMate IT Services for technical installation support.

North America
800.449.8112

You can also contact us by email - Send Email

TeamMate Analytics Support:
TeamMate Analytics Support Request

Contents

CHAPTER 4 – WORK PAPERS

1. POLICY

Work papers should be prepared in accordance with the general guidelines contained in GAO's *Government Auditing Standards* (Yellow Book) and with the additional requirements established in this procedures manual. As a general guideline, work papers should:

    (a) contain a written audit guide cross-referenced to the work papers;

    (b) contain adequate indexing and cross-referencing, schedules, and summaries;

    (c) be dated and signed by the preparer;

    (d) be reviewed by a supervisor; (This review should be documented in the work papers.)

    (e) be complete and accurate enough to provide proper support for findings and recommendations, and to demonstrate the nature and scope of work performed;

    (f) be understandable without verbal explanations;

    (g) be legible and neat, as practicable; and

    (h) be restricted to matters that are significant and relevant to the objectives of the project.

To protect the confidentiality of the information, work papers are not to be left unattended or accessible to unauthorized personnel. Audit documentation files are to be protected from scrutiny, theft, tampering, damage, or loss at all times. This protection may require the use of file cabinets, desk drawers, or briefcases with secure locks for Privacy Act information and other sensitive materials.

Under the Privacy Act, personally-identifiable information about a person, such as personal identifiers (e.g., names and Social Security numbers) are protected from disclosure. The Privacy Act provides penalties for any federal employee who divulges personal information, unless that information is exempt from the Act.

Access to work paper documentation by outside parties, either during or after the audit, will be determined by the OIG's Legal Counsel, in coordination with

the AIGA and the Inspector General on a case-by-case basis. In some instances, it may be necessary to provide copies of the audit documentation to program officials, so that they may respond to the findings and recommendations or implement corrective actions. In other instances, outside parties may request access to the work paper documentation through the Freedom of Information Act (FOIA).

OIG's Legal Counsel is responsible for processing the FOIA requests and releasing information under the Privacy Act. If management has marked information as sensitive, confidential or covered by some privilege, OIG will not disclose to a third-party without notice to and consultation with NARA. If information is not so marked but appears to be business sensitive, OIG will generally consult with NARA prior to disclosure.

We will use the "CP" designation, confidential and proprietary, in the schedule title to indicate when Personally Identifiable Information and/or propriety data is present.

2. WORK PAPER IDENTIFICATION AND CAPTIONS

Standards for identifying and captioning work papers are:

1. Each page or series of work papers is consecutively numbered.

2. The first page of a work paper should include the:

    a. name or initials of the auditor preparing the work paper, and the date it was prepared;

    b. work paper number or index designation; and

    c. following captions and information.

    <u>Source</u>. Each work paper should specifically identify where, or from whom, the information on the work paper was obtained. The source

should include the name, title, and office of the person providing the information. When appropriate, the source should also include the name of the record or document and the responsible office for control of the record or document. State the specific source of all information contained in the work papers so that someone not familiar with the audit can easily locate required information and recreate the sample selections. This applies to data furnished by the auditee, as well as data compiled by the auditor. The source is cited in sufficient detail to provide for the independent verification of the data.

Purpose. Each work paper should include a statement of purpose which specifies why the work paper was prepared.

Scope. The statement of scope should describe the period covered for the information obtained and the basis for the period covered. The scope may also describe the basis for selecting items for review and the relationship of the items reviewed with the total number of items. Describe the volume of transactions, number examined, and percentage of total volume represented by the test, geographic locations, period under review, and a description and justification of the method used in sample selection/methodology. Include the dates of transactions examined. When external factors impose constraints, such as data limitations or scope impairments, these factors must also be disclosed.

Results (Summary of Work). This field is used to provide details of the work performed - This contains the body of the work performed. The auditor fully documents their analysis of evidence (whether documentary, testimonial or physical), including the nature, timing, and extent of work completed. This section supports how the auditor reached the conclusion.

Conclusion. The results of work performed satisfying the Purpose. Concisely and clearly summarize the audit results. The documentation identifies any findings, including data related to condition, criteria,

cause, and effect. The conclusion must address the purpose of the work paper.

3. Each page of a work paper shows the number of pages in the work paper and the number of each page, to facilitate referencing to a specific page.

In TeamMate EWP, the above standards, a-c, are captured. Procedure Summaries, which are the audit steps, include fields to document the work paper's purpose, source, scope, results (summary of work), conclusions and references to supporting evidence. Each supporting piece of evidence (Microsoft Word, Microsoft Excel, TeamMate Image or Adobe .pdf) must be signed off using the electronic signature for each preparer and reviewer. Each procedure step and procedure summary must also be signed off using the electronic signature for each preparer and reviewer. Work papers are consecutively numbered and have a unique index designation to facilitate referencing.

At the end of each letter section, a procedure summary will be added with a procedure step to summarize this section of the audit and how it meets the objectives of the audit. For example, section B may have B.1, B.2 and B.3. Auditors must add B.4 as a summary for section B.

3. INTERVIEW FORMAT

All interviews will state, at the outset, the following information:

(a) date, time, and location of interview;

(b) name, position, and office of the official(s) interviewed;

(c) names of audit staff members present; and

(d) subject discussed in the interview.

Information obtained from follow-up interviews and telephone calls may be added to the initial interview write-up.

Interview write-ups may be documented in the results (summary of work) field of a procedure summary or in an individual work paper (i.e., Microsoft Word).

4. AUDIT EVIDENCE

There are different types and sources of evidence that auditors may use, depending on the audit objectives. Evidence may be obtained by observation, inquiry, or inspection.

- Auditors should evaluate the objectivity, credibility, and reliability of the testimonial evidence. Documentary evidence may be used to help verify, support, or challenge testimonial evidence.

- Surveys generally provide self-reported information about existing conditions or programs. Evaluation of the survey design and administration assists auditors in evaluating the objectivity, credibility, and reliability of the self-reported information.

- When sampling is used, the method of selection that is appropriate will depend on the audit objectives. When a representative sample is needed, the use of statistical sampling approaches generally results in stronger evidence than that obtained from nonstatistical techniques. When a representative sample is not needed, a targeted selection may be effective if the auditors have isolated certain risk factors or other criteria to target the selection. The sampling method used should be documented in the work papers. The sampling method used should be documented in the work papers. We generally judgmentally select a low sample size and judgmentally select sample items based on risk or a random basis and test key control attributes.

- When auditors use information gathered by officials of the audited entity as part of their evidence, they should determine what the officials of the audited entity or other auditors did to obtain assurance over the reliability

of the information. The auditor may find it necessary to perform testing of management's procedures to obtain assurance or perform direct testing of the information. The nature and extent of the auditors' procedures will depend on the significance of the information to the audit objectives and the nature of the information being used.

- Auditors should assess the sufficiency and appropriateness of computer-processed information regardless of whether this information is provided to auditors or auditors independently extract it. The nature, timing, and extent of audit procedures to assess sufficiency and appropriateness is affected by the effectiveness of the entity's internal controls over the information, including information systems controls, and the significance of the information and the level of detail presented in the auditors' findings and conclusions in light of the audit objectives.

Appropriateness is the measure of the quality of evidence that encompasses the relevance, validity, and reliability of evidence used for addressing the audit objectives and supporting findings and conclusions. Sufficiency is a measure of the quantity of evidence used for addressing the audit objectives and supporting findings and conclusions.

Auditors should determine the overall sufficiency and appropriateness of evidence to provide a reasonable basis for the findings and conclusions, within the context of the audit objectives. Professional judgments about the sufficiency and appropriateness of evidence are closely interrelated, as auditors interpret the results of audit testing and evaluate whether the nature and extent of the evidence obtained is sufficient and appropriate.

Auditors should perform and document an overall assessment of the collective evidence used to support findings and conclusions, including the results of any specific assessments conducted to conclude on the validity and reliability of specific evidence.

When assessing the sufficiency and appropriateness of evidence, auditors should evaluate the expected significance of evidence to the audit objectives, findings, and conclusions, available corroborating evidence, and the level of

audit risk. The steps to assess evidence may depend on the nature of the evidence, how the evidence is used in the audit or report, and the audit objectives.

When the auditors identify limitations or uncertainties in evidence that is significant to the audit findings and conclusions, they should apply additional procedures, as appropriate. Such procedures include

    (a) seeking independent, corroborating evidence from other sources;

    (b) redefining the audit objectives or limiting the audit scope to eliminate the need to use the evidence;

    (c) presenting the findings and conclusions so that the supporting evidence is sufficient and appropriate and describing in the report the limitations or uncertainties with the validity or reliability of the evidence, if such disclosure is necessary to avoid misleading the report users about the findings or conclusions (see paragraph 8.15 for additional reporting requirements when there are limitations or uncertainties with the validity or reliability of evidence); or

    (d) determining whether to report the limitations or uncertainties as a finding, including any related, significant internal control deficiencies.

5. ORGANIZATION OF WORK PAPER FILES

Work paper files contain a complete record of the project from the preliminary planning phase through issuance of the final report. The files should consist of several sections. Each section should contain a description of the basic documents and work papers included in the file and be listed in a table of contents with the applicable work paper index.

    1. <u>Administration Section</u>. In TeamMate EWP this is AS2

        (a) <u>Audit Announcement</u>. Copies of the audit announcement letter and memoranda of the entrance and exit conferences held with agency officials.

(b) <u>Audit Guide</u>. The audit guide and documentation of any changes made to the guide during the project. The guide is cross-indexed to the work papers showing the project results pertaining to each project objective and step. If a particular project objective or step was not addressed, the program will be annotated with an explanation.

(c) <u>Correspondence</u>. Project-related correspondence with management officials, contractor officials, and OIG officials.

(d) <u>Work Paper Files Index</u>. The table of contents for all other work paper files. In TeamMate EWP, the TeamMate browser acts act the work paper file index.

2. <u>Field Work Results Sections</u>. These sections contain work papers addressing the specific objectives and steps in the audit guide. Generally, these work papers are organized by project objectives and corresponding project steps in the order the objectives and steps appear in the audit guide. Simple projects may require only one section, but most projects require several. Project work paper sections can be established at the beginning of the project and modified as the project progresses, or they can be developed as the auditor performs the work. In TeamMate EWP, this would be folders starting with B.

3. <u>Report Section</u>. This section should contain the finding sheets and draft reports that have been submitted to the AIGA and the IG, review comments, independent referencer comments, the final draft report approved for release, responses to the draft report, analyses of the responses, final report issued, and subsequent updates on corrective actions. It is the official OIG record of the report. In TeamMate EWP, this would be folders starting with PA.

6. SUMMARIZING WORK PAPER SECTIONS

At the end of each letter section, a procedure summary will be added with a procedure step to summarize this section of the audit and how it meets the

objectives of the audit. For example, section B may have B.1, B.2 and B.3. Auditors must add B.4 as a summary for section B.

The procedure summary should include:

(a) a clear statement and description of the purpose or objective of the summary;

(b) an outline of the work performed which serves as the basis for the finding being described;

(c) a factual summary of the evidence and its source(s). This section should contain enough information to determine condition, criteria, cause, and impact of the findings;

(d) a bridge between the project results and the proposed recommendations; and

(e) what needs to be done to correct the problem(s).

7. NUMBERING WORK PAPERS AND WORK PAPER FILES

Work papers are numbered when prepared, or as soon as practical thereafter. Indexing identifies each work paper in accordance with a previously established indexing system.

In TeamMate EWP, the following standard format occurs. TeamMate EWP will automatically sequentially number evidence ~~work papers~~ as they are added to the audit file.

8. INDEXING AND CROSS-INDEXING WORK PAPERS

The work performed and facts contained in the summary (procedure step in TeamMate EWP) will be indexed to the work papers where that data was obtained. The objective should be cross-indexed to the audit guide and other cross-indexing may be necessary in the work papers.

Indexing (one-way and two-way) entails referencing the supporting or related work papers. A One-Way Reference is a direct index reference from a specific work paper location to another work paper. A reference link only exists at the starting link location. These types of links are handy for one-way informational references, such as "see memo on policy at ..." type references. A Two-Way Reference or point-to-point referencing refers to the ability to reference any two discrete locations or points together, to and from each other.

The following are indexed:

(a) work papers and attachments that relate to each other, in order to avoid conflicts of facts and data;

(b) work paper summaries (procedure steps within procedure summaries in TeamMate EWP) to the supporting work papers and attachments to assure objectives are addressed; and

(c) draft reports to work paper summaries and/or supporting work papers and attachments.

Each work paper attachment should also be referenced to the work papers summary/ procedure step in TeamMate EWP. Auditors should make sure all work paper attachments are captured in the source of a work paper summary/procedure step in TeamMate EWP. Two-way referencing should be done when possible.

A best practice is to add a reference to the each work paper attachment, i.e.:

> For PSSC: See F.1.PS Step "Routers"

This allows the work paper attachment to stand alone with a reference to the appropriate procedure step.

9. ACCESS TO WORK PAPERS

Work papers developed during the course of a project become the official records of the OIG and must be adequately safeguarded to prevent access by unauthorized persons or premature disclosure of information, and to ensure they are not lost, stolen, altered, or destroyed. When the auditor is working outside the OIG office, work papers which are not in use should be locked in a file cabinet or desk.

Under most circumstances, the use of work papers will be restricted to OIG employees. All other access to work papers must be specifically authorized by the IG. Requests for access to the work papers will be reviewed by the Counsel to the IG, before forwarding to the IG for approval.

Exceptions to disclosure include legitimate confidences which should be protected. Special care should be exercised on requests for information furnished by an informant other than in the regular course of official duties. Officials outside the OIG will not be allowed access to audit guides or other materials which provide detailed information on the scope and nature of our work, before the draft report is circulated.

In carrying out its audit responsibilities, GAO will require information on the scope and nature of audit work performed or planned by the OIG. Our policy is to make work papers, including audit guides, available to GAO for this purpose and to discuss fully with GAO the audit work performed or planned.

The IG retains responsibility for deciding whether information can be released to the public.

In accordance with NARA Records Schedule - Chapter 12 Audit case files of internal audits on NARA programs, operations, and procedures, and audits conducted on contractors. Records consist of audit reports, correspondence, and supporting work papers should be maintained by the Office of the Inspector General (OIG) and may be destroyed 8 years after year end of the completion of the final report (See Attachment 4-1).

Attachment 4-1

Chapter 12, Audits and Investigations

August 07, 2007

These operational records relate to audits of NARA programs and
contractors, progress reports of actions taken to resolve audit findings, and
investigations of possible unlawful activity.

- Audit Administration
- Audits and Investigations
- RESERVED
- Electronic Copies of Records Contained in this Chapter

Search the
Records
Schedule

[   ]
[SEARCH]

Audit Administration

File #	Description	Disposition
1201	**Audit Administration Subject Files**	
	Documents relating to the routine operation and administration of the audit function, but NOT routine program administration files described in file no. 110 (Chapter 1). Included in the subject files are pertinent laws, copies of contracts or other authoritative documents relating to specific audit functional areas, organizational charts and functional statements, surveys of procedures and controls, statistical tabulations, contractor's financial statements, analyses of cost trends, and significant findings of prior audits in each functional area.	Destroy when superseded or obsolete. (N1-64-87-1)
1202	**Audit Guidance**	
	Documents created in preparing, clearing, and issuing special instructions and guides for use by auditors in NARA internal and contract audits. Included are record copies of audit guides and instructions, clearance actions, and related records.	Destroy when superseded, canceled, or discontinued. (N1-64-87-1)
1203	**Audit Schedules**	
	Schedules of audits and background materials accumulated in the process of identifying areas for audit.	Cut off annually. Destroy when 5 years old. (N1-64-87-1)
1204	**Audit Report Chronological Files**	
	Records accumulated for reference and referral to contract audits, internal audits, clearances, and related information. Included are copies of final contract and internal audit reports.	Cut off annually. Destroy when 5 years old. (N1-64-87-1)
1205	**Audit Summaries**	
	Periodic audit digest and summaries, reports of actions taken as a result of the summaries, and related records created in preparing and circulating summarized information on the status of audit activities, selected audit findings and recommendations, and other audit matters.	Cut off annually. Destroy when 3 years old. (N1-64-87-1)

Audits and Investigations

File #	Description	Disposition
1206	**Audit Case Files**	
	Case files of internal audits on NARA programs, operations, and procedures, and audits conducted on contractors. Records consist of audit reports, correspondence, and supporting work papers. Files are maintained by the Office of the Inspector General (OIG).	Cut off annually after completion of final report. Hold 2 years and retire to records center. Destroy 8 years after cutoff. (N1-64-00-4, item 1)
1207	**Audit Resolution Case Files**	
	Case files used for tracking progress on internal audits, audits on contractors, and Government Accountability Office (GAO) audits. Included are notices of intent to audit, copies of documents	

National Archives and Records Administration
Office of Inspector General – Office of Audits

File #	Description	Disposition
	furnished to auditors, copies of tentative findings and recommendations, advance notice of major findings, reports of major findings, copies of draft and final reports, follow-up progress reports, comments, and related documents.	
1207-1	Files maintained by NARA Audit Resolution Official.	Cut off at the end of the fiscal year in which follow-up actions on report recommendations are completed. Hold 3 years and retire to records center. Destroy when 8 years old. (N1-64-87-1)
1207-2	Files maintained by designated central point of contact for a major office and by the audited unit.	Cut off at the end of the fiscal year in which follow-up actions on report recommendations are completed. Destroy when 3 years old. (N1-64-87-1)
1208	**Investigative Case Files**	
	Case files developed during investigations of known or alleged fraud and abuse and irregularities and violations of laws and regulations. Cases relate to agency programs and operations administered or financed by the agency, and to agency personnel, contractors, and other persons having a relationship with the agency. Complaint and investigative files may consist of memorandums of interview or activity, reports of investigation, and related documents, such as correspondence, notes, attachments, and working papers.	
1208-1	Complaint Files. Records contain information or allegations which are of an investigative nature, and may or may not relate or lead to an investigation. Files include: anonymous or vague allegations not warranting an investigation, matters referred to other NARA units or Federal agencies for handling, and support information for the initiation of an investigation.	Destroy 10 years after "closed final" date. (N1-64-07-1, item 1)
1208-2	Investigation Files (See "NOTE.*")	
	a. Case files EXCEPT those that are covered under file no. 1208-2b."	Destroy 20 years after "closed final" date. (N1-64-07-1, item 2a)
	b. Case files relating to unrecovered and alienated holdings."	Destroy 20 years after "closed final" date only if potential of recovery no longer exists. (N1-64-07-1, item 2b) "NOTE: Significant case files (i.e., those that result in national media attention, congressional investigation, and/or substantive changes in agency policy or procedure) are NOT covered by this chapter. Contact the NARA Records Officer to submit an SF 115 to NWML. (NARA will determine the disposition on a case-by-case basis.
1208-3	Case Management and Tracking System (CMTS)	
	a CMTS data	Delete when no longer needed. (N1-64-07-1, item 3)
	b CMTS-generated reports.	Destroy/delete when no longer needed. (N1-64-07-1, item 4)
1209	**Indexes to Case Files**	
	Indexes and registers used as references to investigative and audit case files.	Destroy or delete with the related records. (GRS 23, item 9)
1210	**Semiannual Report to Congress Files**	
	Reports prepared by the OIG and submitted to Congress, and working papers. The reports summarize OIG activities for the six-month periods ending March 31 and September 30.	
1210-1	Record copy.	PERMANENT. Cut off annually. Transfer to NARA in 5-year blocks when 5 years old. (N1-64-90-1)
1210-2	Other copies.	Destroy when 5 years old or when no longer needed, whichever is sooner. (N1-64-90-1)
1210-3	Working papers.	Destroy when 5 years old or when no longer needed, whichever is sooner. (N1-64-90-1)

RESERVED

File #	Description	Disposition

Electronic Copies of Records Contained in this Chapter

File #	Description	Disposition
1299	**Word Processing Files and Electronic Mail (E-mail) Records**	
1299-1	Word Processing Files. Documents such as letters, memoranda, reports, handbooks, directives, and manuals recorded on electronic media, such as hard disks or floppy diskettes, after they have been copied to an electronic recordkeeping system, paper, or microform for recordkeeping purposes.	Delete from the word processing system when no longer needed for updating or revision. (GRS 20, item 13 and N1-64-00-4, item 3a)

National Archives and Records Administration
Office of Inspector General – Office of Audits

| 1299-2 | E-mail Records. Senders' and recipients' versions of e-mail messages that meet the definition of Federal records, and any attachments to the record messages after they have been copied to an electronic recordkeeping system, paper, or microform for recordkeeping purposes. | Delete from the e-mail system after copying to a recordkeeping system. (GRS 20, item 14 and N1-64-00-4, item 3b) NOTE: Along with the message text, the recordkeeping system must capture the names of sender and recipients and date (transmission data for recordkeeping purposes) and any receipt data when required. |

Page last reviewed: Jun 09, 2015 - by Diana E Johnston

Organization Phone: 301-837-0880

Notify the content author if this page contains out-of-date or incorrect information

Contents

CHAPTER 5 – REPORTING RESULTS

1. POLICY

The purposes of audit reports are to (1) communicate the results of audits to those charged with governance, the appropriate officials of the audited entity, and the appropriate oversight officials; (2) make the results less susceptible to misunderstanding; (3) make the results available to the public, as applicable; and (4) facilitate follow-up to determine whether appropriate corrective actions have been taken.

An audit report represents our final product. The OIG's stature and image, in terms of how well the audit mission is accomplished, are measured and judged largely by the quality of written audit reports. Therefore, an OIG audit report must be a professional product in terms of content, organization, and appearance. Everyone involved shares in the responsibility of achieving excellence in report writing. Audit reports should be written in a modern, conversational style with language that is simple, clear, and concise.

2. STANDARD AUDIT REPORT FORMAT

Standard OIG audit reports will usually contain these parts:

(a) Transmittal Letter

(b) Cover (See Attachment 5-1)

(c) Table of Contents

(d) Executive Summary

(e) Introduction
   1. Background
   2. Objectives, Scope, and Methodology

(f) Findings Section(s)
  1. Summary Paragraph
  2. Development Section
  3. Recommendations

(g) Other Matters (if applicable)

(h) Appendices:
  1. List of Abbreviations and Acronyms (if applicable)
  2. Management's Response to the Report
  3. Report Distribution List

Auditors should use the Audit Report Formatting Checklist as a guide when formatting audit reports (see Attachment 5-2)

All audit reports must be saved as a .PDF file and be 508 compliant. Compliance standards are set by Section 508 of the Rehabilitation Act of 1973 that requires federal agencies to provide software and website accessibility to people with disabilities. When websites are 508 Compliant, they are accessible to all users. See Attachment 5-3.

3. Audit Report Signatures and Distribution

Audit reports are to communicate the results of audits to those charged with governance, appropriate officials of the audited entity, and the appropriate oversight officials. Distribution of audit reports supports transparency; makes results less susceptible to misunderstanding; and facilitate follow-up to determine whether appropriate corrective actions have been taken

The OIG will distribute audit reports to the appropriate audited entity officials, and as appropriate, to other officials who have legal oversight authority or who may be responsible for acting on audit findings and recommendations. The OIG will document any limitations to report distribution.

Draft Audit Reports
The Assistant Inspector General for Audits (AIGA) will sign all *draft audit reports* addressed to cognizant NARA Officials (Agency Heads or Designees) following

the Inspector General's (IG) review and approval of the draft report. The responsible Auditor will prepare the transmittal letter and distribution list ensuring the appropriate level of management receives the draft report.

Final Audit Reports:
The Inspector General (IG) will sign *all final audit reports* addressed to the Archivist of the United States. The AIGA will ensure the transmittal letter and distribution list includes the appropriate level of management.

4. AUDIT REPORT SECTIONS

(a) Executive Summary. This section summarizes the report. It provides a brief description of the more important findings, adverse effects, and recommendations in the report. It should provide readers with an accurate understanding of our major conclusions without having to read the entire report. Corrective action taken during the audit on audit findings will also be noted here. Where applicable, refer to interim reports that led to the corrective action.

(b) Introduction. This part of the report contains background information and provides details about the objectives, scope, and methodology of the audit.

   1. Background. The Background section is designed to give the reader an understanding of the nature and size of the audited program, function, or entity and any special problems, circumstances, or events related to the audit. For example, agency policies relating to the audit should be explained to put the audit results and recommendations into proper perspective. This section may also include legislative or regulatory criteria affecting the program, function, or entity. Data on available resources, such as personnel strength and funding, will also be included in most reports. Care should be taken to include only that background information which is relevant and necessary.

   2. Objectives, Scope, and Methodology. This section of the report will give the reader details on the objectives of the audit; what was audited; why the audit was performed; the auditing standards and methodology followed; the period of audit; and where the audit work

was done, including comments on a multi-location audit relationship, if applicable. Each report should include for an audit conducted in accordance with GAGAS the following paragraph:

> Our [performance or financial] audit [or attestation engagement] was conducted in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit [or attestation engagement] to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit [or attestation engagement] objectives.

If the audit is not conducted in accordance with GAGAS, the report should include a modified GAGAS compliance statement: Stating either that (1) the auditor performed the audit or attestation engagement in accordance with GAGAS, except for specific applicable requirements that were not followed, or (2) because of the significance of the departure(s) from the requirements, the auditor was unable to and did not perform the audit or attestation engagement in accordance with GAGAS. Situations when auditors use modified compliance statements include scope limitations, such as restrictions on access to records, government officials, or other individuals needed to conduct the audit. When auditors use a modified GAGAS statement, they should disclose in the report the applicable requirement(s) not followed, the reasons for not following the requirement(s), and how not following the requirements affected, or could have affected, the audit and the assurance provided.

Audits must state whether sampling results can be projected to the intended population when sampling is significant to the audit findings, conclusions, or recommendations. When using non-statistical sampling methods, include the following language in the report: "The results of a non-statistical sample cannot be projected to the intended population."

(c) Findings. According to the GAO Government Auditing Standards, the elements needed for a finding depend entirely on the objectives of the audit. Thus, a finding or set of findings is complete to the extent that the audit objectives are addressed and the report clearly relates those

objectives to the elements of a finding. For example, an audit objective may be limited to determining the current status or condition of program operations or progress in implementing legislative requirements, and not the related cause or effect. In this situation, developing the condition would address the audit objective and development of the other elements of a finding would not be necessary.

For our reports, a well-developed Findings Section will usually have certain characteristics and parts. It will begin with a brief summary paragraph of the overall condition, including what was found to be wrong or need improvement, and the actual or potential effect resulting from the condition. The rest of the section will develop the finding and include a comparison of "what is" (condition) with "what should be" (criteria), and an answer to the question "what does this mean?" or "so what?" (effect). Further, if an audit report is to be constructive, the reasons why (cause) there is a difference between "what is" and "what should be" must be identified and explained. Having identified the cause, the next logical step is to make a recommendation which will solve the problem.

Findings should normally be presented in order of significance. Do not try to enhance minor findings by putting them first or before more significant findings. Each auditor will apply professional judgment in deciding whether each finding is important enough to be included in the report, or would be more appropriately presented in an audit memorandum.

Whenever possible, combine similar or related minor findings into one significant finding. Doing this may enable you to better develop and show basic management weaknesses (causes), more significant actual or potential adverse effects, and support recommendations made to correct the underlying causes for a number of conditions and adverse effects.

In most instances, noncompliance with regulations should not be reported as the principal point of a finding unless the objective of the audit is to conduct a compliance review. The performance, or lack of performance, which is caused by deviations from regulations shall be given primary emphasis. When possible, tie findings and/or associated effects to the agency mission or to the NARA

Strategic Plan. This makes the finding more important, thereby making it easier to "sell to management."

If a comment in a finding represents an opinion or an assumption, it will be so identified. The basis for the opinion or assumption will be stated in the report and must be fully supported in the audit work papers.

All name references which directly identify individual persons shall be omitted from the findings of audit reports. Appropriate position titles may be used. Management's comments and reactions to findings should be credited to the responsible official by title, position, or office, to the maximum extent possible. If individual identification is necessary for understanding or to effect corrective action, furnish this information separately to the audited organization. The work paper file shall document that such information was furnished.

Even though audit reporting involves criticism, the criticism must be presented in a constructive manner. Wording will never be sarcastic or antagonistic. Reports should merely state the facts forthrightly along with the auditors' conclusions.

The findings section should also disclose any findings from a prior audit that have not been resolved and closed, and corrective action is still needed. Show the title and date of the audit report in which the prior finding appeared. Refer to or cite information from the prior report. Explore and comment on the reasons why only partial or no action was taken on the prior recommendation(s) and why full implementation is still needed.

Each finding will have a subject title and a section for recommendations. A separate section for Management Response and Evaluation of Management Response will be included in final reports, if appropriate.

(d) Appendices. Lists, copies of documents that support the report, including management's comments on the draft report, should be attached as Appendices. Assign each appendix an identifying title typed in capital letters and centered at the top of the page. Appendices will be identified by capital letters in the upper right hand corner of the page. If there is only one appendix, no capital letter should be used.

Performance Audit Reports

Auditors should report deficiencies in internal control that are
significant within the context of the objectives of the audit. Auditors
should also report instances of fraud, noncompliance with provisions
of laws, regulations, contracts, or grant agreements, or abuse that
have occurred or are likely to have occurred and are significant
within the context of the audit objectives.

Auditors should include in the audit report (1) the scope of their work on internal
control and (2) any deficiencies in internal control that are significant within the
context of the audit objectives and based upon the audit work performed.
Auditors should refer to that written communication (see Management Letter
section) in the audit report, if the written communication is separate from the
audit report.

In a performance audit, auditors may conclude that identified deficiencies in
internal control that are significant within the context of the audit objectives are
the cause of deficient performance of the program or operations being
audited. In reporting this type of finding, the internal control deficiency would
be described as the cause.

When auditors conclude, based on sufficient, appropriate evidence, that fraud,
illegal acts, significant violations of provisions of contracts or grant agreements,
or significant abuse either has occurred or is likely to have occurred, they should
report the matter as a finding.

When fraud, illegal acts, violations of provisions of contracts or grant
agreements, or abuse either have occurred or are likely to have occurred,
auditors may consult with authorities or legal counsel about whether publicly
reporting such information would compromise investigative or legal
proceedings. Auditors may limit their public reporting to matters that would not
compromise those proceedings, and for example, report only on information
that is already a part of the public record.

Financial Statement Audit Reports

For financial audits, including audits of financial statements in which auditors provide an opinion or disclaimer, auditors should report, as applicable to the objectives of the audit, and based upon the audit work performed, (1) significant deficiencies in internal control, identifying those considered to be material weaknesses; (2) all instances of fraud and illegal acts unless inconsequential; and (3) violations of provisions of contracts or grant agreements and abuse that could have a material effect on the financial statements.

For all financial audits, auditors should report material weaknesses and significant deficiencies in internal control. In assessing the significance of control deficiencies, (material weakness or significant deficiency) the auditor should consider qualitative considerations such as public accountability of the audited entity, legal and regulatory requirements, the visibility and sensitivity of the entity or program, the needs of users and concerns of oversight officials, and current and emerging risks and uncertainties facing the government entity or entity that receives government funding. The auditor should also consider, when assessing the significance of a deficiency in internal control:

(a) the likelihood that a deficiency, or combination of deficiencies, could fail to prevent or detect a material misstatement of an account balance or disclosure; and

(b) the magnitude of the potential misstatement.

When auditors conclude, based on sufficient, appropriate evidence, that any of the following either has occurred or is likely to have occurred, they should include in their audit report the relevant information about:

(a) fraud and illegal acts that have an effect on the financial statements that is more than inconsequential,

(b) violations of provisions of contracts or grant agreements that have a material effect on the determination of financial statement amounts or other financial data significant to the audit, and

(c) abuse that is material, either quantitatively or qualitatively.

When auditors detect violations of provisions of contracts or grant agreements or abuse that has an effect on the financial statements that is less than material but more than inconsequential, they should communicate those findings in writing to officials of the audited entity. When fraud, illegal acts, violations of provisions of contracts or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings, and for example, report only on information that is already a part of the public record.

Attestation Engagement Reports

For attestation engagements, auditors should report, as applicable to the objectives of the engagement, and based upon the work performed, (1) significant deficiencies in internal control, identifying those considered to be material weaknesses; (2) all instances of fraud and illegal acts unless inconsequential; and (3) violations of provisions of contracts or grant agreements and abuse that could have a material effect on the subject matter of the engagement.

For all financial audits, auditors should report material weaknesses and significant deficiencies in internal control.

When auditors conclude, based on sufficient, appropriate evidence, that any of the following either has occurred or is likely to have occurred, they should include in their report the relevant information about:

(a) fraud and illegal acts that have an effect on the subject matter that is more than inconsequential,

(b) violations of provisions of contracts or grant agreements that have a material effect on the subject matter, and:

(c) abuse that is material to the subject matter, either quantitatively or qualitatively.

Violations of provisions of contracts or grant agreements or abuse that has an effect on the subject matter that is less than material but more than inconsequential, should be communicate in writing to entity officials.

When fraud, illegal acts, violations of provisions of contracts or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings.

Auditors, even if they have resigned or been dismissed, should report known or likely fraud, illegal acts, and violations of provisions of contracts or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances.

(a) When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties.

(b) When entity management fails to take timely and appropriate steps to respond to known or likely fraud, illegal acts, violations of provisions of contracts or grant agreements, or abuse that:
    1. is likely to have a material effect on the subject matter and

2. involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance.

If the audited entity still does not take timely and appropriate steps as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding agency.

Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by entity management that it has reported such findings in accordance with laws, regulations, and funding agreements.

In presenting findings such as deficiencies in internal control, fraud, illegal acts, violations of provisions of contracts or grant agreements, and abuse, auditors should develop the elements of the findings to the extent necessary to achieve the engagement objectives. If auditors are able to sufficiently develop the elements of a finding, they may provide recommendations for corrective action.

Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as applicable, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value or other measures, as appropriate. If the results cannot be projected, auditors should limit their conclusions accordingly.

Reporting Audit Results[1]

Day 1	Draft Audit Report - The OIG will issue draft audit report to the Executive(s) of the appropriate office and Accountability (CA). The exit conference is also scheduled within 10 days after issuance of the draft audit report.
By Day 10	Exit Conference - The OIG will conduct an exit conference with the Executive(s) of the appropriate office and NARA's audit liaison to discuss the draft audit report, including informal comments and preliminary actions for the recommendations. CA will provide comments to the OIG prior to the exit conference.
By Day 15	Updated Final Draft Audit Report – The OIG will provide an updated final draft audit report to the Executive(s) of the appropriate office and CA.
By Day 40	Comments and Action Plans – Final written comments and actions are provided to the OIG by CA.
By Day 45	Final Audit Report – The OIG will issue a final audit report.
7 days after issuance	Redaction Suggestions – All redaction suggestions based on FOIA exemptions must be submitted to the IG's counsel within one week from the date the report is issued final.

The OIG will continue to conduct status meetings with management and provide information on findings identified throughout the audit process. Management is also encouraged to contact the auditor and meet as frequently as possible to ensure they are knowledgeable about pertinent audit findings. These status meetings allow the OIG and management to clarify data, misunderstandings of processes, and questions about findings that will be documented in the audit report.

---

1 The Reporting Audit Results cycle uses calendar days.

5. MANAGEMENT RESPONSE AND EVALUATION OF MANAGEMENT RESPONSE

This section will appear in final reports only. Comments will either be obtained at the exit conference or through written comments on the draft report. If management declines to comment on draft findings and recommendations, indicate this in the report and issue it.

Management's comments on each finding may be presented verbatim or summarized. A copy of management's written response, however, should always be included as an appendix to the report.

When summarizing the comments, be sure to state whether management agreed or disagreed with the findings and recommendation(s), and describe any corrective actions management has agreed to take. Be careful that management's comments are summarized correctly.

When the official comments oppose the draft finding and recommendation(s) and we conclude that management's position is without merit, we must effectively rebut its position and explain the reason for maintaining our position. In some cases, rather than place undue emphasis on a strong rebuttal following management's comments, it may be better to rewrite the finding, giving appropriate recognition to the comments and our reaction in the body of the finding. This treatment may be particularly desirable to avoid having to insert a lot of new material in our rebuttal. Conversely, it may be necessary to come up with more support for the finding, modify the finding, or drop it, if we think management's position is valid or casts doubt on our position. In short, we will not leave the reader with conflicting information without some attempt to clarify our position, reconcile the views, or modify the finding to eliminate inconsistencies or confusion.

If the recommendation, as presented in a draft report, is no longer appropriate or valid after we get management's response, we can, in the final report:

(a) drop any reference to the draft report recommendation and that part of the reply relating to it, or if it seems appropriate, briefly discuss the draft report recommendation and reply in the development section or in a footnote; or

(b) add new information and revise the finding as necessary (or drop the finding).

6. REPORT REFERENCING

Independent referencing is a vital component of the Office of Audits quality assurance and shall be completed before the issuance of the draft report and final report. Independent referencing does not relieve the audit team of its responsibility for the report, and is not a substitute for supervisory review.

Participating in independent referencing of our audit work is **NOT** optional. Independent referencing is a vitally important part of our quality assurance process and is everyone's responsibility. When and if selected to complete a referencing assignment, the referencing takes precedence over current assignment and requires the referencer's full attention.

Immediately following the Inspector General's (IG) approval of the draft audit report, the Assistant Inspector General for Audits (AIGA) or designee will assign a reference GS 12- GS 14, who was NOT part of the audit team conducting the work and contributing to the report. All efforts will be made to ensure the referencer assigned to the draft audit report will also reference the final audit report.

Once the referencer is assigned, they will be named as the Independent Reference Reviewer (IRR) and added to the TeamMate file as a "Preparer/Reviewer". Referencing should not start until the audit team has completed its report indexing to audit documentation and supervisors have completed their required reviews of the audit documentation.

The IRR is responsible for determining that every figure and statement is reported correctly. This includes ensuring that the opinions, conclusions, and

recommendations are reasonable and are consistent with, or supported by, the factual material examined. Audit conclusions and findings must be supported by sufficient and appropriate evidence. The IRR must insert a tick mark or initial to denote acceptance of the index supporting the evidence.

The IRR comments are used to document cases where the IRR questions the accuracy of, or support for, a statement, fact, or figure in the report. All IRR comments must be documented and addressed on a referencer worksheet (Attachment 5-4), in a comment box in the report Word document, or in TeamTalk within TeamMate.

Upon completion of IRR's review, the IRR notifies the designee for the team to begin addressing each of the comments. Attachment 5-5 are some general IRR Do's and Don't's.

The IRR will review the audit team's response to each comment. If the IRR is satisfied with the disposition of the comment, the IRR should document agreement by noting "Resolved" and document his/her initials.

If the IRR is not satisfied with the action taken by the audit team, he or she must raise those issues to the AIGA who is ultimately responsible for the accuracy of the report. If all comments are not resolved, the AIGA has the authority to accept responsibility for the disputed issues involving wording or interpretation of audit documentation, but not on disputed issues of fact. The AIGA is to consult with the IG regarding any disputed issues of fact or interpretation.

Once the review is completed and all comments are resolved, the IRR must complete the *IRR Checklist for Referencing Audits/Evaluations* (See Attachment 5-6)

7. REPORT AND RECOMMENDATION TRACKING

Offices provide written management comments and action plans during the draft report process. If NARA management is unable to respond in the time

frame specified in the action plans, it should notify the OIG in writing of the reason for the delay and provide a revised response date.

When management is forced by changing events to reconsider its position on any OIG recommendation, or if an alternative approach to correcting a weakness is decided on by management, the audit resolution official should provide the OIG with this information so that the OIG can fully consider management's comments, before reporting that management has not addressed an audit recommendation in the OIG's Semiannual Report to the Congress.

Periodic evaluations of the audit follow-up system should be conducted, to determine if the system results in efficient, prompt, and proper corrective action on audit recommendations.

8. MONETARY BENEFITS

Although the full impact of OIG reports, particularly those resulting in increased effectiveness or improved efficiency, cannot always be measured in terms of monetary impact, many audit recommendations produce a monetary impact that can be measured and supported. In this regard, OIG policy is that all audit reports will be evaluated to determine if they have potential monetary impact. Savings reported will be measurable, supportable, and attributable to the work of OIG.

9. ADVISORY AUDIT MEMORANDA AND AUDIT MEMORANDA

Advisory Audit Memoranda and Audit Memoranda (see Attachment 5-7 and 5-8) are another method of communicating the results of the audit to NARA management. They should be used to address findings or deficiencies that are judged by the auditors not to be material or significant enough for inclusion in the formal audit report, or if there are no findings to report. The audit report should reference any findings communicated in an audit memorandum to

NARA officials, and should state that "other findings were reported to management in an audit memorandum."

They may be issued in conjunction with an audit report, or may take the place of a formal audit report.

(a) Contents of an Audit Memorandum. The format may vary, depending on the specific requirements of the audit. However, an audit memorandum will contain most of the same information that is required to be included in a formal audit report. That is, audit memoranda should include:

1. a statement of the audit objectives and a description of the audit scope and methodology;

2. a full discussion of the applicable findings, and where applicable, the auditor's conclusions;

3. the cause(s) of problem areas noted in the audit, and recommendations for actions to correct the problem areas and to improve operations; and

4. the statement that "We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives."

(b) Procedures for Issuing Audit Memoranda. The preparation and issuance of audit memoranda will not require that all GAO *Government Auditing Standards* be complied with. Specifically,

1. Audit memoranda will be independently referenced.

2. Audit memoranda will be issued only in final form if no audit recommendations are made, therefore no management comments will

be solicited or included in them. However, accuracy of the material may be discussed with management, and verified.

3. Audit memoranda will be issued in draft if the memoranda contain recommendations. During performance of the audit, findings will be discussed with management officials and their views considered when preparing the audit memorandum.

4. Follow-up will be conducted for recommendations made in audit memoranda.

10.   MANAGEMENT LETTERS

In addition to the audit report and the audit memorandum, *management letters* (see Attachment 5-9) constitute another form of written communication with NARA management. They should be used to address issues that need to be quickly brought to management's attention or to communicate to NARA management internal control deficiencies, fraud, illegal acts, violations of provisions of contracts or grant agreements, or abuse that have an inconsequential effect on the subject matter audited or under an attestation engagement.

The format and contents of a management letter will vary, depending on the specific requirements of the issues or information to be conveyed to management.

Since management letters are not the product of an audit, there is no expectation of compliance with the GAO *Government Auditing Standards.* Specifically,

1. Management letters will be issued only in final form. That is, no management comments will be solicited or included in the management letter.

2. Follow-up may be conducted for recommendations, but not for suggestions, made in the management letter.

The issuance of management letters will be reported in the Semiannual Report to the Congress.

11. OTHER REPORT INFORMATION

No matter the type of report, a GAGAS audit report includes audit objectives, scope, and methodology; significant audit findings; conclusions; recommendations; internal control deficiencies; relevant information on fraud, illegal acts, or abuse, as appropriate. If all the above items are included in the report and the auditor following planning and fieldwork standards, a statement that the audit was made in accordance with generally accepted Government auditing standards; and, views of responsible officials concerning our findings and conclusions should also be included in the report. If the report does not include the items above you need to remove or modify the GAGAS statement.

When modifying the GAGAS compliance statement, the auditor must state either that (1) the auditor performed the audit or attestation engagement in accordance with GAGAS, except for specific applicable requirements that were not followed, or (2) because of the significance of the departure(s) from the requirements, the auditor was unable to and did not perform the audit or attestation engagement in accordance with GAGAS. Situations when auditors use modified compliance statements include scope limitations, such as restrictions on access to records, government officials, or other individuals needed to conduct the audit. When auditors use a modified GAGAS statement, they should disclose in the report the applicable requirement(s) not followed, the reasons for not following the requirement(s), and how not following the requirements affected, or could have affected, the audit and the assurance provided.

When auditors do not comply with any applicable requirements, they should (1) assess the significance of the noncompliance to the audit objectives, (2) document the assessment, along with their reasons for not following the requirement, and (3) determine the type of GAGAS compliance statement. The

auditors' determination will depend on the significance of the requirements not followed in relation to the audit objectives.

12.   Redaction Process

All audit reports must be saved as a .PDF file and be 508 compliant. Compliance standards are set by Section 508 of the Rehabilitation Act of 1973 that requires federal agencies to provide software and website accessibility to people with disabilities. When websites are 508 Compliant, they are accessible to all users. See Attachment 5-2.

All audit reports must be reviewed for redaction prior to posting on our public website. To make these reports available to staff and the public as quickly as possible, we will generally use the following process (NARA and/or the IG may deviate from this process if they determine it to be necessary):

Draft Audit Report

> **OIG:** When a draft report is issued (in both hard copy and electronic form), the cover letter will specify that agency redaction review needs to take place in the 30 day period for comments.

> **NARA:** Redaction recommendations must be included as an attachment with the formal comments memo for the Archivist's signature. NGC review for redaction recommendations must also take place within this timeframe. Packages without a redaction recommendation or an acknowledgement that no redaction is needed will be returned to the office for completion.

Final Audit Report

> **OIG:** Issues a final report and redacted version, if necessary (in both hard copy and electronic form). Since the final language may differ from the draft significantly, NARA will be given five duty days to review the final language and make any additional redaction recommendations.

NARA: Reviews final report for redaction recommendations and will respond to the OIG through CP within five duty days. If CP does not respond to the OIG with redaction recommendations or an acknowledgement that no redaction is needed within five duty days, or to request additional time, it will be interpreted as an affirmation NARA does not desire any further redactions.

OIG: The OIG makes redactions, if necessary and posts a copy in the Managers & Supervisors forum on the ICN within three duty days of receipt of NARA's response and forwards the final electronic redacted version to the Web staff for posting on archives.gov.

NARA: Web staff publishes redacted version on archives.gov within two duty days of receipt from OIG and notifies CP when posted.

Other OIG reports (Audit memos, management letters, and advisory reports issued in final and sent to the Archivist – in both hard copy and electronic form.)

NARA: Prepares a response for the Archivist's signature and performs a redaction review within 30 days, or whatever deadline is included in the report, including NGC's review. Redaction recommendations must be included as an attachment with the formal comments memo for the Archivist's signature. Packages without a redaction recommendation or an acknowledgement that not redaction is needed will be returned to the office for completion. If NARA does not plan to produce a response to the report, CP will notify the OIG so the report can be posted. If CP does not respond with redaction recommendations or an acknowledgement that no redaction is needed within 30 days, or whatever deadline is included in the report, or does not request additional time, it will be interpreted as an affirmation NARA does not desire any further redactions.

OIG: The OIG makes redactions, if necessary and posts a copy of the final report (with redactions if needed) in the Managers & Supervisors forum on the ICN within three duty days of receipt of NARA's response and forwards

the final electronic redacted version to the Web staff for posting on archives.gov.

NARA: Web staff publishes redacted version on archives.gov within two duty days of receipt from OIG, along with any responses from NARA, and notifies CP when posted.

ATTACHMENT 5-1

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION

OFFICE *of*
INSPECTOR GENERAL

NATIONAL
ARCHIVES

TITLE

DATE

OIG Audit Report No. XX-XX

Table of Contents

2
National Archives & Records Administration

OIG Audit Report No. XX-XX

Executive Summary

OIG Audit Report No. XX-XX

Background

4
National Archives & Records Administration

OIG Audit Report No. XX-XX

Objectives, Scope, Methodology

Audit Results

1. .

Recommendations

We recommend:

Recommendation 1:

Recommendation 2:

Recommendation 3:

Recommendation 4:

Management Response.

OIG Audit Report No. XX-XX

Appendix A – Acronyms

OIG Audit Report No. XX-XX

Appendix B – Management Response

OIG Audit Report No. XX-XX

Appendix C - Report Distribution

OIG Audit Report No. XX-XX

OIG Hotline

To report fraud, waste or abuse, please contact us:

Electronically: https://www.archives.gov/oig/referral-form/index.html

Telephone: 301-837-3500 (Washington, D.C. Metro area)
1-800-786-2551 (toll-free and outside the Washington, D.C. Metro area)

Mail: IG Hotline
NARA
P.O. Box 1821
Hyattsville, MD 20788-0821

ATTACHMENT 5-2

OFFICE *of* INSPECTOR GENERAL
NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION
8601 ADELPHI ROAD, COLLEGE PARK, MD 20740-6001
NATIONAL
ARCHIVES   *www.archives.gov/oig*

Audit Report Formatting Checklist

➢ Title Page
- o No Bold font
- o Normal Capitalization
➢ Footers
- o Use only the number for pages (e.g. 2, 3, 4)
- o Use *National Archives and Records Administration* below page number
- o Page 2 should be Table of Contents and be the first page number used – the title page is unnumbered.
➢ Table of Contents
- o If you have an appendix specific to your audit, it should come first. All audit-specific appendices should continue as Appendix B and so on. After the last audit-specific appendix, the next three appendices should be our three standard ones in this order:
  - ▪ Acronyms
  - ▪ Management's Response to the Report
  - ▪ Report Distribution List
- o Check the hyphens for the Appendices in both Table of Contents and on the Appendix page itself.
  - ▪ The hyphens should be:
    - 1) Appendix A – Acronyms
  - ▪ The hyphens should not be:
    - 1) Appendix A - Acronyms
➢ Line Spacing
- o All spacing to be Multiple 1.15 in body, footnotes, recommendations.

Spacing			
Before:		Line spacing:	At:
After:	0 pt	Multiple	1.15

☐ Don't add space between paragraphs of the same style

➢ Acronyms
- o Acronyms to be defined in Executive Summary and then again the first time they are used in the body of the report.
- o Check to make sure all acronyms in report are on acronym appendix.

- o
  - o Additionally, check to make sure all acronyms in appendix are included within the report. Using the find function (CTRL-F) helps with this task.
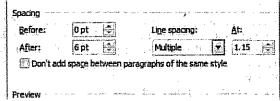- ➢ Footnotes
  - o 10 point Times New Roman
  - o No spacing between footnotes.
- ➢ Criteria
  - o Use bulleted list in Objectives, Scope, Methodology section to list the criteria used in the report.
  - o Use a, b, c format for bullets
  - o When citing criteria, do not use quotation marks around the language.
- ➢ Subheadings
  - o Use *italics*
  - o 6 pt space between heading and text

> Spacing
>
> | Before: | 0 pt | Line spacing: | At: |
> |---|---|---|---|
> | After: | 6 pt | Multiple | 1.15 |
>
> ☐ Don't add space between paragraphs of the same style
>
> Preview

- ➢ List with colons
  - o Use the following example (text, colon, two spaces, number, text, semi-colon, number, text...)
    - The following offices were surveyed. (1) Office A; (2) Office B; and (3) Office C.
  - o For longer sentences within a list, use a colon, then type in a bulleted list below:
    - For example, use this format for long sentences:
      1) Type the first sentence here;
      2) Then, the second sentence here; and
      3) The third sentence here.
- ➢ Tables/Charts/Exhibits/Etc.
  - o Title to be above table in 10 pt font, with 6 pt space between title and table (same as subheading)
  - o Text within table to be in Times New Roman 10 point.
  - o Title of table to be: Table 1
- ➢ Finding Titles
  - o Capitalize Key Words
  - o High-Level (e.g. Digitization Partnership Agreements)
- ➢ Break between findings – findings should always start on top of page.
- ➢ Recommendations
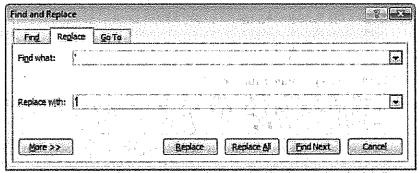
- o Template will have **Recommendation 1:** Text
➢ Apostrophes and Quotation Marks
  - o Use the replace function (CTRL-H) to change all throughout text, which will replace apostrophes and quotation marks throughout the report into the correct form.

➢ Watermark on draft report to read DRAFT
➢ Title Page and Header of draft to say:
  - o OIG Draft Audit Report No. XX-XX
  - o Check to make Draft is removed from both places for Final.
➢ For Distribution List, see AIGA's procedures.
➢ Miscellaneous items not covered in this checklist
  - o Should you run into any report format issues not considered in this document, use the GPO style guide and consult with the AIGA as necessry:
    https://www.gpo.gov/fdsys/pkg/GPO-STYLEMANUAL-2008/content-detail.html
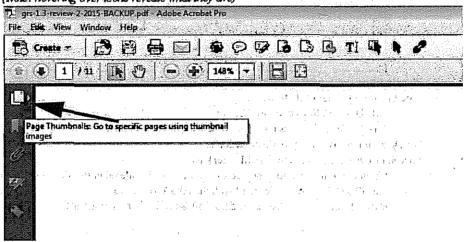
ATTACHMENT 5-3
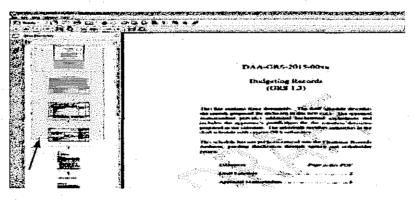
How to make a PDF accessible

1. Click File → properties, and fill in title of the document. List the author as *National Archives and Records Administration* (unless the author is an outside source). Then click the "Advanced" tab and select "English" for the language.

2. Click the page thumbnails icon:
(Note: hovering over icons reveals what they are)
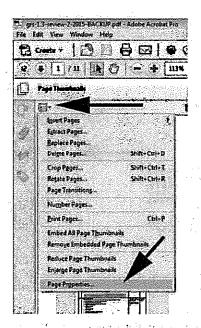
3. Select all the page thumbnails:
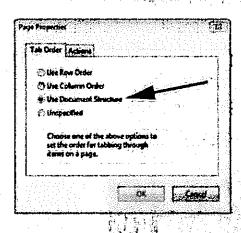
4. Select the options icon and scroll to Page Properties:
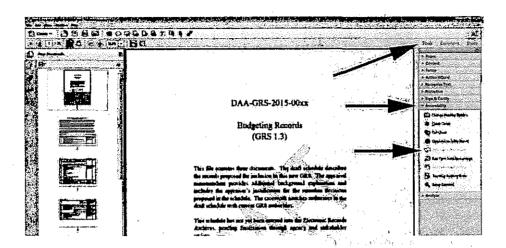
5. Select "Use Document Structure." Save.
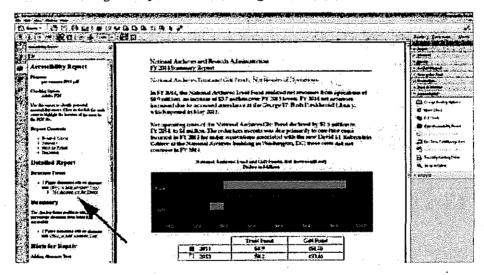
6. Now click on Tools → Accessibility and select "Add Tags to Document." Save again.
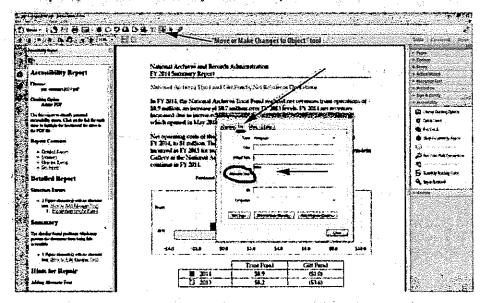
7. Then run a "Quick Check" and "Full Check" from the same menu. *(Leave all the default items checked and click "Start Checking," then click "ok" when a site report is ready.)*

8. Anything left to address will be listed in the Accessibility Report. If you need to add alt text, click on the link to go directly to the element missing alternative text.
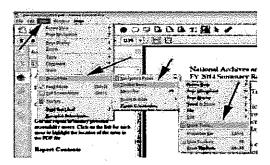
9. Then click on the highlighted object with the "Move or Make Changes to Object" tool, right-click and select "Properties," choose the "Tag" tab and in the "Alternate Text" box, type a description (this is what will be read by a screen reader).
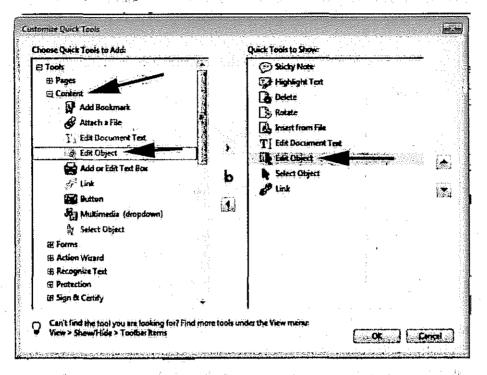
Note: this part of the process is not always intuitive – sometimes it will flag a footer or a line and not the whole graphic, you may have to experiment.

10. Do this for each image, save and rerun the accessibility check to make sure it clears.

....

Note: if you do not have the "Move or Make Changes to Object" tool in your navigation bar, you can add it:

That tool falls under "Content" → "Edit Object" *(double-click to add to the list of "Quick Tools to Show" and select "OK")*.

ATTACHMENT 5-4

REPORT REFERENCING REVIEW FORM

REPORT REFERENCING REVIEW			
REPORT TITLE AND NUMBER:			
REFERENCER:		**DATE:**	
COMMENT NUMBER	REPORT PAGE	COMMENT	AUDITOR'S ACTION (INITIALS/DATE)
1			
2			
3			
4			
5			
6			
7			
8			
9			

ATTACHMENT 5-5

IRR Do's and Don'ts

✓ DO verify that statements of fact, figures (including graphics), and dates are correctly reported.

✓ DO ensure that the report's findings, conclusions, and recommendations are supported by sufficient, appropriate evidence, and are logical.

✓ DO ensure the report addresses all audit objectives.

✓ DO ensure you sign an independence statement.

✓ DO verify evidence of supervisory review.

✓ DO work with the team to provide constructive notes.

✓ DO make the referencing job your *ONLY* priority!

⊘ DON'T provide editorial comments, unless they directly affect the message.

⊘ DON'T advise or comment about your (the IRR) preference.

⊘ DON'T look for a word-to-word match.

⊘ DON'T worry or comment about formatting issues or OIG report templates concerns.

⊘ DON'T change an incorrect index or fix a typo yourself. Instead, make a comment such as "Support was located on page 3 instead of 4, please verify."

December 2015

ATTACHMENT 5-6

Independent Referencing Checklist

Audit Number: _____

TITLE: _____

I have reviewed the report and work papers and determined that they are ready to be referenced.

Auditor _____ Date: _____

Audit Manager/AIGA _____ Date: _____

Referencing Dates _____ to _____

Draft _____ Final Report _____

Referencer Response	Yes	No *	N/A**

A. CRITICAL DATA ANALYSIS OF THE REPORT

1. Executive Summary. The Executive Summary stands
alone, concisely presents a persuasive case to the high level reader that
significant problems exist, proposes meaningful recommendations, and
properly summarizes the remainder of the report.

2. Introduction
   a. The Background provides information that the reader needs to
   understand the report and shows the nature, purpose, and size, of the
   entity's responsibilities and operations, key legislative requirements,
   and organizational data. It also shows any significant constraints and
   unusual circumstances or events that affected the entity's operations.
   b. The Objectives depict what was assessed and what was to be
   determined by the audit; they are specific enough to present the audit
   in a clearly focused, defined, neutral, and segmented manner.
   c. The Scope and Methodology:

   1) Relates the program universe to what was audited in order
      to place audit coverage into perspective.
   2) Identifies the significant internal controls assessed and the
      extent of the assessment (when the audit objectives include
      an evaluation of internal controls).
   3) Describes the extent of systems testing (general and
      application controls or alternative data reliability tests) when
      computer-based data was relied upon.

4) Describes the universe and sample design or explains the
basis for judgmental selections, including any bias and
problems in data quality.

5) The Methodology describes how the audit evidence was
obtained, and what was reviewed, assessed, and/or analyzed

3. Findings and Recommendations

a. The titles of the chapters identify the problem(s) being
reported.

b. The condition, cause, effect, and criteria are clearly and
concisely stated. Auditor developed criteria is based upon
authoritative sources.

c. The sample (or judgmental selection) and the related universe
of the program, operation, or activity are shown in order to place
the finding in proper perspective. The methodology used to
develop the finding is described.

d. The findings contain sufficient, appropriate evidence.

e. Conclusions are reasonable and appropriate, given the audit
disclosures. A convincing
case is made that the report's recommendations should be enacted.

f. Critical audit assertions are reasonable and supportable.
These assertions are statements of fact which are integral to the
audit findings.

g. The classification of an internal control weakness or
accounting system nonconformance as "material" or "significant"
is reasonable. A weakness not so
classified (i.e., "immaterial") is also reasonable.

h. Internal controls not prescribed, inadequate as prescribed, or
adequate but not functioning as prescribed are noted when
attributable to an adverse condition.

i. Effect, using statistical projections or other monetary values,
is fair and not misleading.
Statistical estimates show sampling precision.

j. Corrective action taken or planned during the audit has been
reported. If additional
action is required, it is described.

l. Issues disclosed by the auditee to the auditor have been so
recognized.

m. Attribution is provided for all testimonial evidence.

n. Recommendations convey the proposed solution to the
causes of the conditions presented in the findings and are
sufficiently detailed in order to facilitate final action.

B. DATA VERIFICATION AND VALIDATION OF THE REPORT AND WORK PAPERS

1. Headings in the Table of Contents agree with headings in the body of
the report and sections begin on the pages indicated.

2. All objectives are accounted for in the report, with either positive
comments or audit findings, and are traced to the audit program.

3. Scope/Methodology
   a.   Shows the name and location of the auditee and the sites visited (or refers to an exhibit).
   b.   Identifies programs, organizations, activities, and functions audited and shows the period of audit coverage, and when the audit was conducted.
   c.   States whether the audit was in accordance with appropriate standards, discloses any deviations, and includes statements of nonconformity. Discloses the scope limitations when the term "limited testing" is used.
   d.   Documents the sampling approach. If sampling is critical to audit findings/conclusions, provides details to include the sampling methodology, number of units tested, and the applicability of the sample results to the universe.
   e.   Documentation describes how the audit evidence was obtained, what was reviewed and assessed/analyzed

4. Findings and Recommendations

   a.   Lengthy or complex regulatory citations are paraphrased and footnoted.
   b.   The use of names or other identifiers in the report are dealt with properly.
   c.   Mathematical computations in the report are correct.
   d.   Recommendations are sequentially numbered.
   e.   If appropriate, a glossary of terms has been included to explain technical terms.
5. Exhibits/Attachments/Appendices
   a.   Contain descriptive titles so that the reader can clearly understand what is presented.
   b.   Are accurate, logical, orderly, clearly presented, and cross-referenced.
   c.   A Summary of Monetary Results was completed when report includes monetary results. All questioned items are properly identified. Amounts can be reconciled to the details and amounts recommended for recovery can be reconciled to the recommendations.
6. Ensure consistency of statements, facts, figures, opinions, conclusions, et al., throughout all report sections.
7. Work papers
a. The draft is cross-referenced to the work papers, the summary work papers to the detailed work- papers, and the work papers to the program. Cross-referencing accurately identifies where the supporting documentation is located.
b. The following can be traced and reconciled from the report to the work papers:

   (1)   Statements of fact
   (2)   dates

(3)   figures

(4)   titles (to include regulatory, instructional, etc., citations)   _____

(5)   quotations/paraphrases of policies/laws/ regulations   _____

(6)   dollar amounts   _____

(7)   comments by the auditees   _____

c. Evidence of ongoing supervisory reviews, such as comment notes,   _____
emails, memorandums of conversation, are filed. Work papers are
properly and timely reviewed by supervisors.

d. The sampling approach is documented. If a judgmental sample was   _____
authorized in the
audit program, the selection process is clearly identified.

e. If work of other auditors was relied on:
    (1) Inquiries were made into the professional qualifications and   _____
    independence of the auditors and is evidenced in the work papers.
    (2) The work papers were reviewed.

f. Computer-generated audit applications   _____
are documented in the work papers including the type of hardware and
software used, description of program logic and methodologies, and
location of computer tapes, disks or listings containing input-output data.

g. Graphs, tables, and charts are used when practical in place of   _____
voluminous or complex narratives, and are appropriate, meaningful, and
accurate.

h. The adequacy of corrective action taken on prior audits was evaluated.   _____

i. Testimonial evidence critical to the report was corroborated, when   _____
    possible, via documentary evidence.

j. Written representation from the persons from whom testimonial   _____
evidence was obtained were secured when the evidence could not be
otherwise corroborated.

* All "No" responses require a comment by the Referencer.

** All "N/A" responses require an explanation by the Referencer.

Signature of Referencing Auditor//Manager   Date

_____   _____

ATTACHMENT 5-7

NATIONAL
ARCHIVES

OFFICE of
INSPECTOR GENERAL

Date : December 11, 2014

Reply to: Office of Inspector General (OIG)

Subject : Advisory Audit Report No. 15-04, Status Update of the Electronic Records Archives Census and Classified Instances

To : David S. Ferriero, Archivist of the United States (N)

The purpose of this Advisory Audit Report is to update you on the status of the Electronic Records Archives (ERA) Census Data Storage (Census) and Classified Electronic Records Archives (CERA) Instances. The Census Instance, which stores the 2010 U.S. Census, cost over $1.4 million[1] and is functioning as intended. However, the National Archives and Records Administration (NARA) spent over $6 million on the development, software, hardware, and maintenance for CERA which did not meet its intended functionality and was never utilized. This was caused primarily by the ERA development contractor not being able to properly integrate the ERA Base System with CERA prior to the end of the contract. As a result, NARA continues to rely on legacy systems, external hard drives, and tapes to store and maintain classified records.

NARA built ERA to fulfill its mission in the digital age: to safeguard and preserve the records of our government, ensure that the people can discover, use, and learn from this documentary heritage, and ensure continuing access to the essential documentation of the rights of American citizens and the actions of their government. The total cost to develop the system was over $390 million[2]. The estimated annual cost to operate and maintain the ERA system is approximately $30 million[3].

One of NARA's primary challenges with ERA was to preserve different types of records along with the processes and documentation required for each type. Therefore, ERA was designed using separate subsystems, or instances, for each category of records. The initial three instances were the Federal Records Instance (Base ERA), deployed June 2008; the Executive Office of the

---

[1] The costs include development, hardware, software, migration, and maintenance.
[2] Source: NARA's ERA Exhibit 300 (5/24/2013 update) on the Office of Management and Budget's (OMB) Federal IT Dashboard.
[3] Source: NARA's ERA Exhibit 300 (5/24/2013 update) on OMB's Federal IT Dashboard. The estimated costs include the Operations and Maintenance contract, hardware/software licenses, technology refresh, government full time equivalents, and corrective and adaptive maintenance activities.

National Archives and Records Administration

President Instance (EOP), deployed December 2008; and the Congressional Records Instance (CRI), deployed December 2009. Two additional instances, Census and CERA were developed in Fiscal Year 2011.

We continue our on-going effort to review aspects of the ERA system. Previous audits include "Audit of the Electronic Records Archives System's Ability to Preserve Records" dated February 15, 2013 (Report No. 13-03), and "Audit of the Base ERA System's Ability to Ingest Records" dated September 19, 2013 (Report No. 13-11) addressing weaknesses related to the preservation and ingest processes. We addressed issues in the EOP Instance in Management Letter No. 13-02, "Status of the Upgrade to the Electronic Records Archives Executive Office of the President System", dated October 18, 2012; Advisory Report No. 13-07, "Status Update of the Electronic Records Archives Executive Office of the President System Upgrade", dated January 31, 2013; and Re-issued Advisory Audit Report No. 14-14, "Status Update of the Electronic Records Archives Executive Office of the President Data Migration Project", dated June 25, 2014. This initiative focuses on the Census and CERA Instances.

Census Instance

The U.S. Census counts every resident in the United States. Mandated by Article I, Section 2 of the Constitution, the first Federal Population Census was taken in 1790, and has been taken every ten years since. The 2010 census contained ten questions about age, gender, ethnicity, home ownership, and household relationships. The data collected by the decennial census determines the number of seats each state has in the U.S. House of Representatives, and is also used to distribute billions in federal funds to local communities.

Due to the confidential nature of the census records, Title 13 of the United States Code specifies enhanced procedures NARA must observe to ensure the non-disclosure of this information and to segregate it from other ERA holdings. In addition, there is a 72 year restriction on access to this data.

The Census Instance was created to manage the storage and retrieval of records related to the 2010 Census. NARA spent over $1.4 million for development, hardware, software, migration, and maintenance of the Census Instance. In 2011, NARA received the 2010 census data, consisting of more than 300 terabytes.[4] The U.S. Census Bureau shipped the data on storage devices including 18 racks of equipment. In 2013, the census data was migrated to new storage devices as part of an effort to replace and consolidate storage hardware for various ERA instances. This was done to improve the availability and reliability of the ERA system, decrease risk of data loss, improve responsiveness of the ERA applications, lower the floor space allocation and operating and utility costs, and create greater storage capacity for additional records in the ERA system. According to a NARA official, the Census Instance is being maintained and functioning as intended.

---

[4] A terabyte is about 1 trillion bytes or about 1,000 gigabytes.

CERA Instance

With the understanding that NARA will be receiving classified data, the need for a classified instance of ERA was established, as the ERA Base System only supports housing unclassified data. CERA was intended to meet the specialized requirements for ingesting, storing, preserving, and accessing classified records. However, NARA spent over $6 million on the development, software, hardware, and maintenance for a system that did not meet its intended functionality, and was never utilized.

According to a NARA official, the ERA development contractor delivered the CERA Instance, but was unable to get the system to work. The primary issue was integrating the unclassified ERA Base System, and CERA. NARA wanted to create records schedules and transfer requests in the unclassified Base System, load the data into CERA, and then have the ability to search for the data across both platforms. When a records schedule or a transfer request is created, an ID sequence number is produced identifying the record. If a user searched for a classified record in the unclassified system, it would link the ID number to the record and tell the user the record was classified or unsearchable in this system. If the user had the appropriate security clearance and access authority, they should have been able to go into CERA and search on the ID number to find the record. However, the development contractor could not get the two systems to recognize one ID number across both systems. Essentially, Base ERA and CERA were air-gapped (i.e., no interconnection or communication) by design and out of necessity. It is this requirement that prevents the two instances from keeping ID numbers synchronized. This fundamental design parameter could not be overcome at the time. Therefore, users would not be able to locate the correct records in CERA. Accordingly, CERA was never populated with records or used.

As CERA is not used, NARA continues to rely on legacy systems, external hard drives, and tapes to store and maintain classified records. According to a NARA official, the legacy systems have limitations in terms of scalability and file format handling. He further stated CERA was supposed to integrate ingesting, processing, and accessing classified electronic records. Further, the CERA equipment is reaching its end of life, and may become defunct. NARA officials have had discussions about possible using this equipment for other purposes. However, no decisions on repurposing the CERA equipment have been made.

We will continue to monitor this situation to see if the CERA equipment can be repurposed and used in some capacity. If NARA management determines the equipment cannot be repurposed, all maintenance agreements should be cancelled as soon as possible.

Scope and Methodology

In order to accomplish our objective we interviewed responsible NARA officials; and reviewed contract documentation, cost information, project management documentation, and applicable law. The contents of this report were discussed with responsible NARA officials, and those officials generally agreed with the contents. Our performance audit was performed at Archives II in College Park, Maryland between December 2013 and September 2014. We conducted this audit in accordance with generally accepted government auditing standards. Those standards

require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusion based on our audit objective. No recommendations were made as the objective was to provide an update.

Please provide a written response to these matters within two weeks of the date of this letter. If you have any questions concerning the information presented in this Advisory Audit Report, please do not hesitate to contact me at (301) 837-3000. As with all OIG products, we will determine what information is publicly posted on our website from this Advisory Audit Report. Should you or management have any redaction suggestions based on FOIA exemptions, please submit them to my counsel within two weeks from the date of this letter. Should we receive no response within this time frame, we will interpret that as confirmation NARA does not desire any redactions to the posted report.

James Springs
Acting Inspector General

cc: Swarnali Haldar, Chief Information Officer

ATTACHMENT 5-8

NATIONAL
ARCHIVES

OFFICE of
INSPECTOR GENERAL

Date: February 12, 2015

To: David S. Ferriero, Archivist of the United States

From: Office of Inspector General (OIG)

Subject: Audit Memorandum No. 15-08: NARA's Timeliness in Responding to Department of Veterans Affairs Record Requests

The National Personnel Records Center (NPRC) provides records to the Department of Veterans Affairs (VA) in the performance of their official duties relating to the adjudication of claims and providing medical care to veterans. Recent publicity about the VA concerning patient wait times, scheduling practices, and alleged patient deaths[1] contributed to an increase in military personnel record (MPR) requests from the VA and veterans. As a result, the National Archives and Records Administration (NARA) Office of Inspector General (OIG) performed this audit in conjunction with another NPRC audit.[2] The objective of this audit was to assess whether the NPRC was adequately fulfilling the VA requests in a timely manner. This audit memorandum focuses on the NPRC's response time to the increased requests for military records from the VA and veterans. It also discusses existing internal controls allowing veterans the capability to notify the NPRC promptly when a request is made for medical records.

Response Times and Pending Requests

In order to determine whether the NPRC is responding in a timely manner to requests from the VA and veterans, we reviewed response times to requests and the NPRC's volume of pending requests. Based on our review, it appears the NPRC responded to requests from the VA in a timely manner. However, the additional requests due to the VA allegations, decreased funding requests from the service branches, inadequate staffing, and the NPRC's recently implemented Quality Assurance Program[3] hindered the facility's ability to process other requests timely. The NPRC's prompt response is critical to veterans who may need medical appointments or benefits.

---

[1] *Veterans Health Administration: Review of Alleged Patient Deaths, Patient Wait Times, and Scheduling Practices at the Phoenix VA Health Care System* (VA Office of Inspector General Report No. 14-02603-267, issued August 26, 2014).
[2] *Audit of NARA's Processing of Military Interfiles and Refiles at the NPRC* (OIG Report No. 15-06, issued February 10, 2015).
[3] The Quality Assurance Program is a daily review of 10% of the requests completed at the NPRC.

The volume of requests received by the NPRC has grown significantly. The average weekly receipts of new requests has increased by 14%, since May 2014. Currently, it takes the NPRC an average of 3.54 days to process VA requests. As of October 2014, the pending requests for all types of requestors grew to 158,487 (See Table 1) and only 29% (45,982) of them were assigned[4] to technicians for fulfillment, leaving the remaining 71% (112,505) unassigned.[5] The majority (53%) of the pending requests were over 30 days old (See Table 2), with the oldest pending requests dating back to February 2012.

Table 1: Pending Requests (as of October 2014)

Separation Document (DD-214 or equivalent)	2,231	11,385	13,616
VA Requests	8,107	111	8,218
Other	102,167	34,486	136,653
Total	112,505	45,982	158,487

Table 2: Aging of All Pending Requests (based on Received in Center date[7])

10 days or less	17,716	7,685	25,401
11-30 days	40,595	7,718	48,313
31-60 days	48,277	9,784	58,061
61-90 days	5,876	17,844	23,720
Greater than 90 days	41	2,951	2,992
Total	112,505	45,982	158,487

Generally, pending requests can be categorized into three categories: separation document requests (DD Form 214 or equivalent[8]), VA requests, and other requests.[9] We were unable to identify if any of the pending requests were from veterans seeking records for medical appointments or benefits.

---

[4] Assigned requests have been assigned to an NPRC Archives Technician for completion.
[5] Unassigned requests have not been assigned to an NPRC Archives Technician for completion.
[6] The pending totals listed for separation documents and VA requests are comparable to the number of requests completed on a weekly basis by the NPRC for these two categories.
[7] The Received in Center date is the date the NPRC mailroom enters information from the SF-180 form into the Case Management and Reporting System (CMRS), the database used to manage requests.
[8] A report of separation is issued when a service member is released or discharged from active duty. The report contains information normally needed to verify military service for benefits, retirement, employment and membership in veterans' organizations
[9] Requests categorized as other can include requests for medical records, all documents in Official Military Personnel File, or other records.

Page 2

Based on discussions with management, additional resources were requested and approved for the NPRC. In September approximately 80 Archives Technicians were hired and additional Archives Technicians are expected to be hired over the next few months. All of these resources should allow the NPRC to significantly reduce the pending requests.

NARA's Notification of Medical Request Controls

We also reviewed controls in place to ensure veterans could notify the NPRC promptly if their request was for medical records. We determined the NPRC provides opportunities for veterans to indicate if the requests are for medical appointments or benefits. For example, when veterans submit a Standard Form 180 (SF-180[10]), they can voluntary identify the purpose of the request including if it is for benefits, employment, VA loan programs, medical, genealogy, etc. However, the NPRC does not track this information, and providing this information does not guarantee faster service. Also, veterans with an urgent request (e.g. upcoming surgery, funeral, etc.) can submit an emergency request to the NPRC, which can be completed within two working days. The NPRC has made all of this information available on NARA's website for veterans. However, if a veteran goes to NARA's veteran's page and clicks on the link for "Need Immediate Assistance" they are directed to the NPRC's general customer service line, which does not offer any option for those needing immediate help with medical records.

Recommendation 1

The Executive for Agency Services should consider adding an additional level of complexity in the Case Management and Reporting System to allow technicians the ability to indicate if records requests are for medical records based on review of veterans' Standard Form 180 (SF-180).

Management Response

Management concurred with the recommendation.

Recommendation 2

The Executive for Agency Services should consider updating the NPRC's Customer Service line to include an option for veterans to communicate with a customer service representative regarding urgent medical requests (e.g. upcoming surgery).

Management Response

Management concurred with the recommendation.

---

[10] Form used to request military records.

Page 3

This audit was conducted in accordance with generally accepted government auditing standards between June and December 2014. These standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As with all OIG products, we will determine what information is publically posted on our website from this Memorandum. Should you or management have any redaction suggestions based on FOIA exemptions, please submit them to my counsel within one week from the date of this letter. Should we receive no response from you or management by this timeframe, we will interpret that as confirmation NARA does not desire any redactions to the posted report.

Should you have any questions concerning this report, or require additional information, please contact me at (301) 837-3000.

James Springs
Acting Inspector General

Page 4

ATTACHMENT 5-9

NATIONAL
ARCHIVES

OFFICE of
INSPECTOR GENERAL

Date : September 11, 2014

Reply to: Office of Inspector General (OIG)

Subject : Management Letter No. 14-18, Customer Service Weaknesses at the National Personnel
Records Center

To : Jay Trainer, Executive of Agency Services (A)

The purpose of this management letter is to bring to your attention customer service concerns
and potential weaknesses expressed to us by veterans contacting the National Personnel Records
Center (NPRC). Over the past few months, the Office of Inspector General's (OIG) hotline has
seen an increase in the number of complaints received from veterans encountering problems
trying to obtain their records from the NPRC, and insisting they were unable to receive
satisfactory customer service regarding their requests. Veterans indicated (1) they received no
response to the status of their requests, (2) they were unable to make a formal complaint, or (3)
their requests were either processed partially, incorrectly, or not at all. Additionally, many
veterans complained their requests took an extremely long time to process.

Veterans noted frustration when trying to contact the NPRC's Customer Service Center.
Veterans can contact the Center via telephone or email, but indicated they were unable to reach
representatives, experienced long wait times, or their emails were unanswered. When we
reviewed the Daily Call Center – Queue Summary Report for the period of October 1, 2013
through June 30, 2014, we noted 176,136 calls were not queued when the Center was contacted.
A call not queued means the system never was able to even intake the call, thus the caller was
not able to get through at all. In fact, only 104,096 calls were received and queued by the system
during the period. However, even of these calls, 36,243 (35%) were abandoned before any
conversation took place. We have also been informed some veteran email requests going back to
January 2014 have yet to be answered.

Veterans are also not receiving complete information about their requests. For instance, when
one veteran requested medical records from a specific military treatment facility from the NPRC,
a form letter was sent indicating the records could not be located. However, while those specific
records could not be found, NARA's systems indicated records for that veteran from that facility
for that time period did exist. Yet this important information was not communicated in the
original form letter to the veteran. When we asked an NPRC customer service representative if
they could send the veteran a letter expressing these facts, we were informed the representative
was not allowed to by their supervisor. We were informed the veteran was denied benefits
because he could not provide the necessary medical records.

NARA's web site is http://www.nara.gov

When the OIG contacted NPRC senior management, it was apparent they were still actively trying to help this particular veteran. However, there appears to be a gap between the attitude and direction of senior management and the actual service provided in day to day operations. Thus the communication employees receive from their department managers may not always align with senior management expectations. During our discussions with NPRC senior management, we indicated NPRC's form letters may need to be customized when there is additional information available that may help a veteran. Senior management agreed.

We also received complaints of veterans receiving other's records, including disclosures of personal information. The OIG previously reported on erroneous disclosures by the NPRC, but the condition still exists. In FY 2013 the NPRC serviced 1,132,525 million requests with senior management indicating there were 162 known reports of erroneous release. However, this does not take into account individuals not reporting back to NARA when they receive someone else's records. While the reported releases equate to a 99.99% accuracy rate for the NPRC, any improper release of personal data should be of concern to management.

We suggest you consider the following to help address the customer service weaknesses at the NPRC:

- Identify a plan to reduce the number of calls not queued, abandoned, and emails not answered.
- Identify a plan to adequately staff the Customer Service Center.
- Provide more detailed guidance and allow customer service representatives the opportunity to provide accurate details on requests, including the ability to make changes to form letters.

It is imperative for veterans to receive the best customer service when contacting the NPRC. We look forward to your prompt response on how you are going to address these critical weaknesses. The Customer Service and Call Center Operations may be included in a future audit plan.

If you have any questions or require additional information regarding this letter, please contact me. As with all OIG products, we will determine what information is publicly posted on our website from this management letter. Should you or management have any redaction suggestions based on FOIA exemptions, please submit them to my counsel within one week from the date of this letter. Should we receive no response within this time frame, we will interpret that as confirmation NARA does not desire any redactions to the posted report.

JAMES SPRINGS
Acting Inspector General

cc: David Ferriero, Archivist of the United States (N)
    Jay Bosanko, Chief Operating Officer (C)

Page 2
NARA's web site is http://www.nara.gov

Contents

CHAPTER 6 – QUALITY ASSURANCE

1. QUALITY ASSURANCE PROCESS

The quality assurance process is designed to provide the OIG with reasonable assurance that the organization and its personnel comply with professional standards and applicable legal and regulatory requirements. The quality assurance process includes the following elements:

a. <u>Project Planning</u>. Project planning is a very important aspect of the quality assurance process. Before starting the field work phase of a project, the auditors must carefully define the objectives and the scope and methodology to achieve those objectives. The objectives are what the project is to accomplish, i.e., they identify the subjects and performance aspects to be included. Scope is the boundary of the project. The methodology comprises the work in data gathering and in the analytical methods auditors will perform to achieve the project objectives.

Insufficient planning results in poor quality work, broken promises, and, perhaps, hard feelings. On the other hand, too much planning is wasteful and unnecessarily restrictive.

b. <u>Ongoing Supervision</u>. The auditor and supervisor of each assignment shall exercise due professional care to assure conformance with GAO's *Government Auditing Standards* and NARA OIG policies and procedures. This is evidenced by the supervisor preparing Team Talk notes in each Teammate audit file to auditors and signing off on audit work papers in Teammate. The process includes making sure that audit work is well planned, the audit scope is appropriate, audit resources are economically used, audit findings are solidly supported, and the audit reports accurately reflect the results of the assignment.

In EWP TeamMate, supervisory review is evidenced by Team Talk notes and signing off of work papers electronically.

c. <u>Internal Quality Control System</u>. The OIG will maintain an internal quality control system for its audit work. This system, i.e., the organizational structure and established policies and procedures, will provide reasonable assurance that the OIG follows applicable auditing standards in its audits. Adequate controls must be incorporated into the audit process to promote compliance with applicable auditing standards and policies, e.g., supervisory review of work papers, cross-referencing of reports, formal audit guides, etc. Independent referencing will be accomplished for all audit reports (see Chapter 5). In addition, each audit will complete the **STATEMENT OF CONFORMANCE WITH AUDIT STANDARDS** (Attachment 6-1) to demonstrate and document conformance with generally accepted government auditing standards.

d. <u>Continuing Professional Education</u>. The OIG is responsible for establishing and implementing a program to ensure that auditors meet the continuing professional education (CPE) and training requirements in the GAO *Government Auditing Standards*. Documentation should be maintained for the education and training completed by the audit staff.

e. <u>Annual Quality Control Summary</u>. The quality assurance review process is designed to provide the OIG with reasonable assurance that the organization and its personnel comply with professional standards and applicable legal and regulatory requirements. The OIG will analyze its quality assurance process annually to identify any systemic issues needing improvement, along with recommendations for corrective action.

The AIGA will:
1. Select one to three audits each year for a quality assurance review to be reviewed by an auditor that did not work on the audit.
2. Ensure the assigned auditor uses the applicable Council of the Inspectors General on Integrity and Efficiency (CIGIE) peer review checklist to review the audit.
3. Ensure the auditor summarizes the results of the review including the auditors or AIGA comments.
4. Analyze and summarize the results of its monitoring control procedures each year.

5. Ensure QAR results are communicated to audit staff via email and /or during audit staff meetings.

6. Ensure a summary of issues found and corrective actions planned/completed as a result of the QAR will be documented and maintained.

7. QAR's are conducting and finalized no later than December 31st of each year.

f. <u>External Review</u>. The OIG will have an external quality control review (peer review) at least once every three years by an organization not affiliated with the OIG. The external review will be directed toward providing the OIG with reasonable assurance that work performed is in accordance with OIG policies, procedures, and plans; guided by GAO and PCIE standards; and carried out economically, efficiently, and effectively. The results of the external review will be documented in a formal report to be delivered to the IG, the Archivist, other auditors, and will be made available to the public, upon request. A copy of the report is sent to the NARA web team to be put on the OIG web page.

2. TRAINING PROGRAM

A successful training program requires constant assessment of changing needs, both present and future; encouragement of, and support for, individual development to meet those needs; and a commitment of sufficient resources to make it possible. Annually, the IG and the AIGA meet to discuss projected training requirements. Major elements of this program include:

a. <u>Training History Record</u>. An up-to-date, complete, and accurate record of each staff member's training.

b. <u>Performance Appraisal</u>. Method to identify, at least on an annual basis, those areas of an individual's performance that could be improved by additional learning, practice, or developmental experiences. Also, to identify training requirements for new or expanded subjects, including specific projects to be performed by the auditors.

3. TRAINING RECORDS

The OIG will maintain records of the CPE hours completed by each auditor subject to the CPE requirements. These records shall include the following information for each CPE program or activity attended or completed by the auditor:

    (a) sponsoring organization,

    (b) title of the program and a brief description of its contents,

    (c) dates attended for group programs or dates completed for individual study programs, and

    (d) number of CPE hours earned toward the GAO *Government Auditing Standards* requirements:
        (1) 80 hours over a two year period
        (2) At least 20 hours in a one year period
        (3) 24 hours directly related to government auditing, the government environment, or the specific or unique to NARA.

The auditor is responsible for providing the above information to the training coordinator, as well as evidence of completion (e.g., certificate of completion).

For CPE programs presented by the OIG, a record of the following information will be maintained:

    (a) a record of attendance or completion,

    (b) number of CPE hours earned by each participant, and

    (c) an agenda or outline of the program that shows the name(s) of the instructor(s); the subjects and topics covered; the dates and length of the program; and, when appropriate, the learning objective(s).

CPE's related to NARA must relate to NARA programs or mission related activities such as classifying records. CPE's related to NARA should not be administrative type training such as, the Hatch Act, Ethics, and IT security. CPE's related to the NARA environment must be approved by the AIGA to count toward each auditor's CPE requirements.

4. AUDITOR RESPONSIBILITIES

Individual auditors are responsible, in conjunction with the OIG, for seeking opportunities for CPE, for successful completion of CPE programs and activities, and for providing documentation of the CPE hours completed. In addition, individual auditors are responsible for monitoring their own progress towards meeting the CPE requirements.

5. PROFESSIONAL CERTIFICATION

To ensure continued high professional expertise, auditors are encouraged to seek professional certifications such as Certified Public Accountant (CPA), Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), and Certified Management Accountant (CMA). Depending on the availability of resources, the OIG will provide support by reimbursing employees for continuing education courses and granting administrative leave, as necessary, for training.

The IG also encourages the staff to belong to and actively participate as members on committees and as officers of professional organizations such as the Association of Government Accountants (AGA), Institute of Internal Auditors (IIA), American Institute of Certified Public Accountants (AICPA), and State Societies of CPAs.

Active participation by staff members in these types of professional organizations ensures that the OIG remains up-to-date on new audit concepts and techniques.

The auditor is responsible for providing professional certifications to the training coordinator.

6. HIRING, STAFFING AND PERFORMANCE APPRAISALS

The OIG will follow NARA Hiring Policies, Practices, & General Guidelines, located at http://www.nara-at-work.gov/staff_resources_and_services/employment/hiring.html

NARA guidance covers recruitment and hiring. In general OIG personnel hired must (a) have, at a minimum, a Bachelor's Degree from an accredited 4-year college or university; and (b) possess the knowledge and skills necessary to perform audits and/or investigations of NARA's programs, activities, and functions.

Staff assigned to an audit must possess the knowledge and skills necessary to accomplish the audit. For audit areas where additional knowledge or training would be helpful, auditors are encouraged to attend relevant courses before performing the audit.

During the annual performance appraisal process, OIG personnel are informed about any areas in which they are deficient or need improvement. Elements of an auditor's performance appraisal are included in the auditor's performance plan and signed by the auditor and supervisor annually. Supervisors provide any assistance and/or training needed to raise the employees' performance to an acceptable level.

The AIGA will assess skill needs to consider whether its workforce has the essential skills that match those necessary to fulfill a particular audit mandate or scope of audits to be performed. The AIGA may review the information (training, professional certificates) maintained by the training coordinator.

ATTACHMENT 6-1

STATEMENT OF CONFORMANCE WITH AUDIT STANDARDS

AUDIT TITLE: _____

ASSIGNMENT NUMBER: _____

PURPOSE: Demonstrate and document conformance with generally accepted government auditing standards.

BACKGROUND: The U.S. General Accountability Office (GAO) publishes *Government Auditing Standards*. This publication, also known as the "Yellow Book," contains standards for audits of (1) government organizations, programs, activities, and functions; and (2) government funds received by contractors, nonprofit organizations, and other non-government organizations. The Inspector General Act of 1978 (as amended) requires that audit work conducted by the Inspectors General, as well as audit work conducted by nonfederal auditors on their behalf, comply with the standards established by the Comptroller General.

The Office of Inspector General (OIG) Office of Audits Procedures Manual contains policies and procedures to implement the "Yellow Book" standards.

CONFORMANCE WITH STANDARDS: For each general, fieldwork, and reporting standard discussed below, we have documented our conformance with the standard.

General Standards:

1. Independence. In all matters relating to the audit work, the audit organizations and the individual auditors, whether government or public must be independent. Auditors must maintain independence of mind and independence in appearance. Chapter 2 of the Procedures Manual addresses auditor and organization independence.

    To the best of our knowledge, neither organizational nor personal nor external threats to independence, both in mind and appearance, have impaired this audit.

    (See W/P _____ for Statement of Auditor Independence.)

    Have any threats been identified by an auditor for this audit? _____ (Yes or No).

    If yes, see the AIGA for more information regarding the threats and safeguards identified.

2. Professional Judgment. Professional judgment should be used in planning and performing the audit and in reporting results.

    We believe that our workpapers and the resulting audit report adequately document our compliance with this general standard.

3. Competence. The staff assigned to perform the audit should collectively possess adequate professional competence for the tasks required. Chapter 6 of the Procedures Manual documents OIG procedures related to training.

Based on training records and our personal knowledge of each auditor's skills, the auditors listed below satisfied Yellow Book requirements for training and continuing professional education and collectively possess adequate professional proficiency for the tasks required:

Auditor:	
Auditor:	
Auditor:	

See the Administrative Officer for NARA OIG for the CPE Reporting spreadsheet supporting individuals' training.

4. Quality Control and Assurance. Each audit organization performing audits in accordance with generally accepted Government auditing standards should have an appropriate internal quality control system in place and should undergo an external peer review. Chapter 6 of the Procedures Manual addresses OIG procedures related to quality assurance.

We are aware that our audit is subject to the quality control system and external peer review.

Field Work Standards:

Chapter 7 of the Yellow Book lays out the following standards for fieldwork on *performance* audits:

1. Work is to be adequately planned.
   - Audit work should provide reasonable assurance about compliance with laws, regulations, and other compliance requirements when they are significant to audit objectives. Auditors should be alert to situations or transactions that could be indicative of illegal acts or abuse.
   - Auditors should obtain an understanding of management controls that are relevant to the audit and assess applicable internal controls when necessary to satisfy audit objectives. Audit work should provide sufficient evidence to support audit judgments about those controls.
2. Staff is to be properly supervised.
3. Sufficient, competent, and relevant evidence is to be obtained to provide a reasonable basis for the auditors' findings and conclusions.
4. Auditors should prepare and maintain audit documentation. Audit documentation related to planning, conducting, and reporting on the audit should contain sufficient information to enable an experienced auditor, who has no previous connection with the audit, to ascertain from the audit documentation, the evidence that supports the auditors' significant judgments and conclusions. Audit documentation should contain support for findings, conclusions, and recommendations before auditors issue their report.

The following workpapers document our conformance with fieldwork standards:
- *Audit is adequately planned (See W/P A.1.PS, A.2.PS and A.3.PS)*
- *Audit Program (See W/P _____)*
- *Supervisory review of workpapers is documented by supervisors on individual workpapers and individual audit steps.*
- *The audit program contains specific audit steps for evaluating compliance with laws and regulations related to our audit objectives. (See W/P _____ for a summary of audit work and conclusions related to compliance with laws and regulations.)*
- *The audit program contains specific audit steps for assessing internal controls related to our audit objectives. (See W/P _____ for a summary of audit work and conclusions related to internal controls.)*

The workpapers associated with this audit document evidence of our audit work. We believe the workpapers show that we have obtained sufficient, competent, and relevant evidence to support our audit judgments and conclusions. Additionally, the report referencer, legal counsel, and various levels of management as appropriate have been satisfied as to the basis and support for our audit conclusions.

<u>Reporting Standards:</u>

Chapter 8 of the Yellow Book describes a number of reporting standards for performance audits. Chapter 5 of the Procedures Manual details OIG's procedures for reporting results.

We believe that (1) our final report complies with all Yellow Book reporting requirements, and that (2) our compliance with Yellow Book reporting requirements is documented by the following:

- *A written audit report communicating the results of the audit has been prepared and, based on OIG procedures, will be available for timely use by management, legislative officials, and other interested parties (See WP_____.)*
- *Auditors should include in the audit report (1) the scope of their work on internal control and (2) any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed. Auditors should refer to that written communication (see Management Letter section) in the audit report, if the written communication is separate from the audit report. (See WP_____.)*
- *The report includes audit objectives, scope, and methodology; significant audit findings; conclusions; recommendations; internal control deficiencies; relevant information on fraud, illegal acts, or abuse, as appropriate; a statement that the audit was made in accordance with generally accepted Government auditing standards; and, views of responsible officials concerning our findings and conclusions. (See WP_____.) If the report does not include the items above you need to remove or qualify the GAGAS statement. (See WP_____.)*
- *The report explains:*
  - *the relationship between the population and the items tested; (See WP_____.)*
  - *the organizations, geographic locations, and period covered; (See WP_____.)*
  - *the kinds and sources of evidence; and (See WP_____.)*
  - *any significant limitations or uncertainties based on the auditors' overall assessment of the sufficiency and appropriateness of the evidence in the aggregate. (See WP_____.)*
- *In reporting audit methodology, auditors should explain how the completed audit work supports the audit objectives, including the evidence gathering and analysis techniques, in sufficient detail to allow knowledgeable users of their reports to understand how the auditors addressed the audit objectives. Auditors may include a description of the procedures performed as part of their assessment of the sufficiency and appropriateness of information used as audit evidence. Auditors should identify significant assumptions made in conducting the audit; describe comparative techniques applied; describe the criteria used; and, when sampling significantly supports the auditors' findings, conclusions, or recommendations, describe the sample design and state why the design was chosen, including whether the results can be projected to the intended population. (See WP_____.)*
- *Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as appropriate, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value, or other measures. If the results cannot be projected, auditors should limit their conclusions appropriately. (See WP_____.)*
- *The report is timely, complete, accurate, objective, convincing, clear, and concise. An issued report was subject to OIG policies and procedures for supervisory review, referencing, editorial review,*

policies, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal control includes the processes and procedures for planning, organizing, directing, and controlling program operations, and management's system for measuring, reporting, and monitoring program performance.

(3)   Compliance audit objectives relate to an assessment of compliance with criteria established by provisions of laws, regulations, contracts, or grant agreements, or other requirements that could affect the acquisition, protection, use, and disposition of the entity's resources and the quantity, quality, timeliness, and cost of services the entity produces and delivers. Compliance requirements can be either financial or nonfinancial.

S2.   Audit Services

Under the Inspector General Act of 1978 (as amended), the Office of the Inspector General (OIG) is to provide a means for keeping the Archivist and the Congress fully and currently informed about problems and deficiencies relating to the administration of NARA programs and operations, and the necessity for and progress of corrective action. In obtaining the necessary information to accomplish this requirement, the OIG conducts a range of audit services. These services include—but are not limited to—contract closeouts, billing inquiries, control assessments, and procurement evaluations.

S3.   OIG Audit Plan

The OIG prepares and distributes an annual audit plan. Suggestions for audits may originate in several places:

a.   Mandatory by statute or regulation. These include the annual independent financial audit, an evaluation of NARA's compliance with the Federal Information Security Management Act (FISMA), and other periodic requirements such as compliance with the Improper Payment Eliminations and Recovery Act.

b.   Selected by the OIG. These are usually aligned with the NARA Strategic Plan and are based on risk, materiality, significance, or other criteria.

c.   Requested by Congress.

d.   Suggested by the Archivist or other management officials. These suggestions may originate as part of the annual request from the OIG for audit plan input or may be forwarded to the OIG as issues arise.

e.   Suggested by anyone inside or outside of NARA who contacts the OIG to suggest audit areas, or recommend or request audit assistance.

Annual audit plans are flexible and may be changed during the year to assign limited audit resources to higher priority audits. The OIG determines the priority for conducting audits.

S-4

Contents

CHAPTER 7 – CONTRACTING FOR AUDIT SERVICES

1. POLICY

In accordance with the Inspector General Act of 1978, as amended, IGs are to ensure that non-federal auditors comply with GAO *Government Auditing Standards* when they audit federal organizations, programs, activities, and functions.

NARA 1201, Audits of NARA Programs and Operations, section 1201.3, Responsibilities, paragraph e.(7), states that the NARA Inspector General is responsible for (a) establishing guidelines for determining when it is appropriate to use nonfederal auditors and (b) ensuring those auditors comply with the government auditing standards.

To fulfill these responsibilities, the OIG closely controls and monitors all contractor work, to ensure that contract terms are met and that the GAO *Government Auditing Standards* are fully complied with in the performance of the effort. The OIG controls the selection of contractors, determines the scope of audits, and controls the release and distribution of final reports.

2. REQUIREMENTS FOR AUDIT SERVICES

NARA offices may submit requests for procuring audit services to the Acquisitions Branch (BCN). Any such requests received by Contracting Officers (COs) must be sent to the OIG. After receiving a request, the IG decides whether to use OIG resources to perform the requested audit services, or to contract for those services. If the decision is made to award a contract, the OIG will arrange for the requested audit services and act as the liaison between the contractor auditors and the CO.

The OIG may also contract for audit services when there is a shortage of in-house resources available or consulting expertise is required for a specific assignment.

3. PROCUREMENT PROCESS

When contracting for audit services, the OIG will follow the procurement process contained in the Federal Acquisition Regulation (FAR) and the NARA procurement guidance.

Request for proposal packages should include a requirement for prospective contractors to provide information and documentation related to previous relevant work experience, staff qualifications (education, experience, and professional certifications), technical approach, independence of the IPA to consider any existing, ongoing or planned nonaudit services, description of the IPA's system of quality control and the most recent peer review, if applicable, and references from other clients.

4. AUDIT SERVICES CONTRACT PROVISIONS

A contract for audit services should include the following:

(a) scope and objectives of the audit services to be provided;

(b) milestones for completion of the audit(s), or for major portions, and submission of audit deliverables;

(c) provision for review of deliverables and audit work papers by the OIG; and

(d) statement that the audit(s) will be conducted in accordance with GAO *Government Auditing Standards* and any other statutory, regulatory, or OMB requirements governing the audit(s).

5. OIG CONTRACT MONITORING RESPONSIBILITIES

After an audit services contract is awarded, a Contracting Officer's Representative (COR) will be nominated, in writing (see Attachment 7-1), to work directly with the contractor. An OIG employee, or another agency employee qualified to perform the monitoring of audit services contracts, will be designated by the IG as the COR for the contract and will act for the CO on technical issues relating to the audit services to be provided. The COR will be provided timely training from an approved source.

For oversight of audits performed by contractors, the COR should follow the United States Government Accountability Office and the President's Council on Integrity & Efficiency, Financial Audit Manual, section 650 if determining the degree of responsibility the OIG accepts with respect to using the work of the IPA and based on the degree of responsibility accepted, the COR should develop a reasonable strategy and plan for monitoring and accepting the IPA's work.

COR responsibilities include the following:

(a) participating in the entrance conference with the audited entity and period status meetings;

(b) monitoring contractor compliance with the contract scope of work requirements;

(c) periodically reviewing the contractor's progress and discussing any problems encountered, need for revising milestones, and significant audit results;

(d) resolving technical questions;

(e) handling administrative matters of the contract, to include approving invoices and monitoring budgets;

(f) reviewing the IPA's audit planning documents for consistency with the contract and GAGAS and resolving inconsistencies.

(g) reviewing contract deliverables, such as work papers and draft audit reports for conformance with the *Government Auditing Standards* and other applicable requirements; and

(h) assisting in contract closeout by forwarding to the CO all required statements and/or records, to ensure a complete contract file.

The COR cannot make any arrangements or commitments with the contractor which would modify the terms, conditions, or scope of the contract. The COR cannot alter or agree to any rate or price modification. These responsibilities reside with the CO and, if such modifications are necessary, the contractor will need to obtain written approval from the CO. Where the contract contemplates the issuance of task orders, the description of the work the contractor is obligated to perform must be found in each task order issued under the

6. QUALITY ASSURANCE

Assuring the quality of contractor performance is always important. When an OIG uses outside audit support to conduct an audit, the quality of the work of the firm and its employees will directly impact on the reputation of the OIG. For this reason, it is critical that the OIG carefully monitors the contractor's work. All audit work papers and report drafts should be reviewed, on a routine basis, by the COR.

The OIG emphasis on conducting performance audits is not commonly found in the private sector. Thus, whenever contractors are assigned responsibility to conduct performance audits as opposed to the more traditional financial audits, special attention must be paid by the COR to contractor compliance with GAO *Government Auditing Standards*.

COR's should follow the United States Government Accountability Office and the President's Council on Integrity & Efficiency, Financial Audit Manual, section 650 for financial statement audits as well as a guide for monitoring performance audits.

7. FINANCIAL STATEMENT AUDITS

The Chief Financial Officers (CFO) Act of 1990, the Government Management and Reform Act (GMRA) of 1994, and the Accountability of Tax Dollars Act of 2002 requires NARA to annually prepare and submit audited financial statements to OMB and the Congress. The agency's financial statements are to be audited in accordance with generally accepted government auditing standards by the OIG or by an independent external auditor, as determined by the IG.

The PCIE adopted a joint GAO/PCIE Financial Audit Manual (FAM) as the framework for conducting financial statement audits in accordance with the *Government Auditing Standards*; incorporated generally accepted auditing standards (GAAS) and attestation standards established by the AICPA; and OMB's audit guidance. The FAM, Chapter 650, *Using the Work of Others*, provides guidance on designing and performing appropriate oversight and other procedures when using the work of other auditors, including contracting for the entire audit. The OIG will utilize this guidance in performing oversight responsibilities.

a. Type of Reporting.

FAM 650 lists the various types of reporting when using an Independent Public Accountant (IPA). The type of reporting depends on the degree of responsibility the OIG accepts and the level of review performed by the OIG. Factors to be considered when deciding which type of reporting to use include the amount of assurance the OIG wishes to provide, legal requirements, and cost-benefit considerations.

The OIG will report on the financial statement by issuing a transmittal letter expressing negative assurance. Negative assurance indicates that the OIG has reviewed the IPA's reports and related documentation, inquired of their representatives, and states that the OIG found no instances where the IPA did not comply, in all material respects, with *Government Auditing Standards*. This is based on the OIG's decision not to assume the role of principal auditor for contracted audits, and the OIG's position that it would not be cost-beneficial to re-perform the contractor's work. Under this type of reporting, the OIG should evaluate the IPA's independence and objectivity, evaluate the IPA's qualifications, and maintain a level of review of moderate or low.

b. <u>Independence and Qualifications.</u>

When using an IPA, the contracting process is designed to select a firm that is independent in mind and appearance, and objective. The contract Statement of Work (SOW) or Performance Work Statement (PWS) should require firms to represent that they are independent and objective with respect to NARA and should request the IPA to describe all work, including non-audit services, done with NARA within the last 3 years. The IPA should identify threats to independence and safeguards to eliminate the threats or reduce them to an acceptable level.

The COR or AIGA should determine whether appropriate safeguards are available and can be applied to eliminate the threats or reduce them to an acceptable level. The COR or AIGA should exercise professional judgment in making that determination, and should take into account whether both independence of mind and independence in appearance are maintained. The COR or AIGA should evaluate both qualitative and quantitative factors when determining the significance of a threat.

Certain conditions may lead to threats that are so significant that they cannot be eliminated or reduced to an acceptable level through the application of safeguards, resulting in impaired independence. Under such conditions, IPA's should decline to perform a prospective audit or terminate an audit in progress.

The OIG should have a role in contracting for the IPA. However, if the OIG does not participate in contracting for the IPA firm, the OIG generally should obtain an overview of the contracting process; this should include reading the SOW, reading the proposal of the firm selected, and understanding the evaluations of the panel selecting the firm. If the IPA does not provide a representation to independence and objectivity in the proposal, then the OIG should obtain a written representation from the IPA.

The OIG should evaluate the IPA's qualifications to perform the audit. This is usually done through the contracting process. The IPA should be required to submit its latest peer review report, letter of comments, and response to the peer review report.

c. <u>Level of Review.</u>

The auditor should prepare a written plan for reviewing the IPA's work that documents the level of review the auditor will perform. The OIG will perform a **moderate** level of review. In some cases, more effort will be performed than is required by FAM 650 for this planned level of reporting responsibility. Under no circumstances will the level of review decrease (e.g., if there is a scope limitation, disclaimer of opinion, etc.). However, the level of our review may increase if the CPA firm's independence, objectivity, integrity, or staff qualifications decrease. OIG review of the IPA's audit documentation is not a replacement for, nor does it relieve the IPA of responsibility for, maintaining an effective system of quality control. The review of documentation should be conducted before the IPA issues the auditors' report, to ensure that the IPA's work papers support the auditors' report.

For a moderate level of review, the auditor will review more of the IPA's documentation, especially documentation evidencing important decisions. The auditor will document deficiencies noted with the IPA's audit documentation, including those indicative of weaknesses in the IPA's system of quality control. The OIG will provide the IPA with the review comments for a determination as to whether additional audit work is necessary. The OIG will follow-up with the IPA and review the actions taken by the IPA, if any, to ensure that all review comments are satisfactorily resolved. The OIG will notify the IPA firm's

management of any significant deficiencies identified with the IPA's audit documentation. The OIG will then prepare a summary memorandum documenting the IPA's review approach and results of the review. The memorandum should state whether the review disclosed instances where the IPA did not comply with GAGAS.

d. Oversight File Documentation.

The OIG will, at a minimum, retain the documentation listed in FAM 650A for the moderate level of review. This documentation may be maintained in EWP TeamMate. The oversight files shall include the title of the audit and the contract number. While the detailed documentation will not necessarily follow the typical audit documentation style of condition, criteria, cause, and effect, the files shall contain appropriate headers and sufficient information to ensure the objectives of the work and conclusions reached are clear and supported.

Contract Administration File	The file generally should include the following items:(1) Statement of Work, (2) Requisitions/ Delivery Orders, (3) Contractor security issues, (4) Contractor Invoices, and (5) Spreadsheet of audit costs.
Reporting File/Section	The file contain: (1) draft and final versions of audit reports and related transmittal letters, (2) copies of OIG comments to the IPA on the reports, (3) copies of NARA's written responses to the reports, and (4) other documentation considered important to supporting our review process of the reports.
Audit Administrative File/Section	An audit administrative file shall be maintained in order to document the OIG's review of the IPA's audit documentation. The file shall include at a minimum: (1) oversight planning memo, (2) IPA Independence memorandum, (3) entrance and exit conference memos, (4) audit program, (5) audit plan, (6) OIG assurance memo, (7) review work papers, (8) Schedule of Deliverables, and (9) Contractor Progress Reports

The COR should ensure the IPA designed the audit to provide reasonable assurance of detecting misstatements that result from

violations of provisions of contracts or grant agreements and could have a direct and material effect on the determination of financial statement amounts or other financial data significant to the audit objectives.

If specific information comes to the auditors' attention that provides evidence concerning the existence of possible violations of provisions of contracts or grant agreements that could have a material indirect effect on the financial statements, the auditors should apply audit procedures specifically directed to ascertaining whether such violations have occurred. When the auditors conclude that a violation of provisions of contracts or grant agreements has or is likely to have occurred, they should determine the effect on the financial statements as well as the implications for other aspects of the audit.

If during the course of the audit, auditors become aware of abuse that could be quantitatively or qualitatively material to the financial statements, auditors should apply audit procedures specifically directed to ascertain the potential effect on the financial statements or other financial data significant to the audit objectives. After performing additional work, auditors may discover that the abuse represents potential fraud or illegal acts. Because the determination of abuse is subjective, auditors are not required to provide reasonable assurance of detecting abuse.

e. <u>Review of IPA Auditor Reports.</u>

All "draft" IPA audit reports, including management letters, will be reviewed by the OIG before issuance to NARA management. The reports should be reviewed to ensure accuracy and conformance with applicable standards and specifications in the contract. The findings and recommendations should also be reviewed for clarity and specificity. The OIG will complete the FAM *Financial Statement Audit Completion Checklist* when reviewing the auditors' report. This checklist is a tool for ensuring that the auditors' report conforms to *Government Auditing Standards*. The OIG will provide review comments, if any, to the IPA for

any errors found or recommendations made for changes to the draft as a result
of the review.

The IPA will submit the final drafts, after appropriate revisions, to the OIG. The
OIG will prepare the draft report transmittal letter and transmit the draft reports
to the Archivist and other appropriate officials for comment. The time provided
to NARA management for commenting on the draft reports shall be agreed to
during the planning stages of the audit. Due to the statutory deadline for
reporting results, the OIG policy for submitting comments cannot be adhered to.

The IPA shall forward the required number of copies of the final report to the
OIG. The OIG will prepare the final transmittal letter and distribute the report to
the appropriate NARA officials.

f. <u>Other Duties.</u>

1. <u>Entrance and Exit Conferences.</u> An entrance conference will be held with
   management officials prior to the start of the engagement. The IPA will
   prepare the agenda and lead the discussion during the entrance
   conference.

   An exit conference will be arranged to discuss the auditors' reports with
   management.

2. <u>Management Representation Letter.</u> The OIG should ensure that the IPA
   obtains a management representation letter, including the summary of
   unadjusted misstatements. The representations supplement the audit
   procedures performed but are not a substitute for them. Statement on
   Auditing Standards (SAS) 89, *Audit Adjustments,* requires management to
   indicate in the management representation letter that unadjusted
   misstatements individually, or in the aggregate, are not material to the
   financial statements. SAS 89 also requires that a summary of unadjusted
   misstatements be attached to the representation letter.

3. <u>Legal Letter.</u> In accordance with AU Section 337, *Inquiry of Client's
   Attorney Concerning Litigation, Claims and Assessments,* the OIG should

ensure that management sends a letter of inquiry to the agency's General Counsel. Management should document in a schedule how the information contained in the legal counsel's response was considered in preparing the financial statements. Legal letters and management's schedules are required.

The OIG should ensure that OMB and GAO receive copies of the legal letters, if applicable, by the required due date.

4. <u>Invoices</u>. The OIG shall review the contractor's invoices for accuracy prior to the submission for payment. Review of invoices should include recalculating hours, ensuring the rate is the rate agreed to in the contract, reviewing the progress reports, and verifying that any travel expenses fall within the federal per diem rates, if applicable.

Attachment 7-1

OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
8601 ADELPHI ROAD   COLLEGE PARK, MD 20740-6001
www.archives.gov/oig
NATIONAL
ARCHIVES

Date : September 8, 20XX

Reply to
Attn of : Office of Inspector General (OIG)

Subject : Nomination of Contracting Officer's Representative

To : name, Director of the Acquisitions (BCN)

1. The Electronic Records Archives Program Office (NHE) is entering into an Interagency Agreement with the Defense Contract Management Agency (DCMA) for contract management services. Some of the services to be procured under this agreement may constitute audit services. Under the Inspector General Act of 1978, as amended, the NARA Inspector General is responsible for selecting and conducting audits of NARA programs, operations, contracts, and grants. Therefore, we wish to nominate Mr/Mrs./Ms. name as the Contracting Officer's Representative (COR) for the Interagency Agreement.

2. Mr/Mrs./Ms. name has over x years of federal government procurement experience auditing major weapon system acquisitions for the U.S. Air Force and acquisitions of large computer systems and management information systems for the U.S. Department of State. During his time at NARA, Mr/Mrs./Ms. name has completed a multi-segment audit of NARA's procurement operations, evaluating the management of various aspects of the agency's procurement process, as well as other acquisition-related reviews of NARA information technology programs.

3. Mr/Mrs./Ms. Name's title, business address, phone number, and fax number are:

    a. Title: xxx Auditor

    b. Business Address: Office of Inspector General (OIG)
                        8601 Adelphi Road, Room 1300
                        College Park, MD 20740-6001

    c. Phone: (301) 837-xxxx

    d. Fax: (301) 837-3197

4. In case of any problems, disagreements, or other questions pertaining to the COR's performance of duties, you may e-mail me at IG's email address@nara.gov, or call me at (301) 837-xxxx.

5. Mr/Mrs./Ms. name completed the Contracting Officer's Representative Initial Training Course (40 hours) on May 21, 19XX, and the Federal Acquisition Institute COR Mentor

Program on September 3, 20XX.

6. At present, Mr/Mrs./Ms. name performance rating elements do not include the COR function. However, his next performance plan will be modified to include the COR function.

7. The COR should be assigned the following duties:

a. Ensure the contractor delivers all contractual goods and services in accordance with the contract delivery schedule. This includes determining causes when the contract is not progressing as expected and making recommendations to the contracting officer for corrective action.

b. Control all government technical interface with the contractor.

c. Ensure that a copy of all government technical correspondence is forwarded to the contracting officer for placement in the official contract file.

d. Promptly furnish documentation on any request for change, deviation, or waiver, whether generated by the government or the contractor.

e. Monitor contractor performance to ensure individual contractor employees are of the skill levels required and are actually performing at the levels charged against the contract during the performance period.

f. Monitor contractor performance to ensure that the labor hours charged against the contract are consistent and reasonable for the effort completed and that any travel charged was necessary and actually occurred.

g. Monitor Government Furnished Information and Material. Ensure that the information and material provided the contractor is authorized by the contract.

h. Complete the COR Report of Contractor's Performance in accordance with the schedule established in the contract administration plan for the contract.

Name
Inspector General

Contents

CHAPTER 8 – NONAUDIT SERVICES

1. BACKGROUND

Nonaudit services, sometimes referred to as consulting services, are professional services other than audits and attestation engagements.

Nonaudit services differ from the traditional professional services provided by an accounting or consulting firm to the audited entity. These types of services are often performed in response to a statutory requirement, at the discretion of the authority of the audit organization, or for a legislative oversight body or an independent external organization and do not impair auditor independence.

Examples of these types of services include (a) providing information to a requesting party without auditor evaluation or verification of the information or data; (b) providing training, speeches, and technical presentations; (c) providing oversight assistance in reviewing budget submissions; (d) identifying good business practices for users in evaluating program or management system approaches, including financial and information management systems; and (e) providing audit, investigative, and oversight-related services that do not involve a GAGAS audit (but which could be performed as an audit, if the audit organization elected to do so).

The GAO *Government Auditing Standards* do not cover nonaudit services since such services are not audits or attestation engagements. Therefore, auditors must not report that the nonaudit services were conducted in accordance with GAGAS.

2. SAFEGUARDING AUDITOR INDEPENDENCE

Using professional judgment, the auditors must, before agreeing to provide a nonaudit service, evaluate whether providing the nonaudit services creates a threat to independence, either by itself or in aggregate with other nonaudit services provided, with respect to any GAGAS audit it performs.

A critical component of this determination is consideration of management's ability to effectively oversee the nonaudit service to be performed. The auditor should determine that the audited entity has designated an individual who possesses suitable skill, knowledge, or experience, and that the individual understands the services to be performed sufficiently to oversee them. The individual is not required to possess the expertise to perform or reperform the services. The auditor should document consideration of management's ability to effectively oversee nonaudit services to be performed.

Auditors performing nonaudit services for entities for which they perform audits should obtain assurance that audited entity management performs the following functions in connection with the nonaudit services:
- (a) assumes all management responsibilities;
- (b) oversees the services, by designating an individual, preferably within senior management, who possess suitable skill, knowledge, or experience;
- (c) evaluates the adequacy and results of the services performed; and
- (d) accepts responsibility for the results of the services.

The OIG will:
- (a) document consideration of audited entity management's ability to effectively oversee a nonaudit service to be provided by the auditor as indicated in paragraph 3.34; and

- (b) document the auditor's understanding with an audited entity or those charged with governance regarding the following:
  - objectives of the nonaudit service;
  - services to be performed;
  - audited entity's acceptance of its responsibilities;
  - the auditor's responsibilities; and
  - any limitations of the nonaudit service.

- (c) Evaluate the impact of previously performed nonaudit services on the auditor's independence on a prospective or current engagement and address threats identified.

(d) Disclose the nature of the threat to independence that could
not be eliminated or reduced to an acceptable level, and
modifying the GAGAS compliance statement. This situation
applies to an auditor in a government entity that may be
required to perform a nonaudit service as a result of
constitutional or statutory requirements

The OIG will not provide nonaudit services that involve performing management functions or making management decisions, and will not audit its own work or provide nonaudit services in situations in which those services are significant or material to the subject matter of the audits.

3. ESTABLISHING PROJECT EXPECTATIONS

For nonaudit services initiated by management request, the auditors will meet with the requesting official(s) to gain a complete understanding of the project's nature, objective, and scope, as well as the expected completion date and format for reporting results. Management officials must be informed of any changes in the review parameters or planned completion dates.

4. COMMUNICATING WITH MANAGEMENT

Auditors should maintain a continuing dialogue with NARA managers as the project progresses and should hold regular status meetings with designated points of contact to keep management informed. These meetings allow for early discussion of potential observations, afford managers the opportunity to provide additional information that could be pertinent to projects, and allow NARA officials to consider alternative actions.

The auditors should also communicate, with the requestors of the services and with those charged with governance, that the work performed does not constitute an audit under GAGAS.

5. REPORTING AND DISTRIBUTING RESULTS

Project results can be provided to management in a report or a briefing. Whatever format is used, the auditors should present the results clearly, accurately, and objectively. Any unconfirmed data or assumptions made should be identified.

Project reports must be referenced prior to transmittal to management. Draft reports are not issued, but discussion drafts may be used to facilitate meetings with management officials. Reports will contain suggestions for improvements, but not recommendations or written management comments, since the interpretation and use of the data is optional at the discretion of the requesting official(s).

If the project was requested by management, the reports, presentations, or briefing papers used to convey project results are distributed only to the official(s) requesting the project. Broader distribution of the results can be made by the requesting official(s), but the results will not be released by the OIG unless the information is requested by external oversight activities, e.g., the Congress, or under the Freedom of Information Act (FOIA).