Description of document:	Department of Health and Human Services (HHS) Office of Inspector General (OIG) Office of Audit Services (OAS) Audit Policies And Procedures Manual, 2016
Requested date:	11-February-2017
Released date:	01-May-2017
Posted date:	03-July-2017
Source of document:	FOIA Request Cohen Building, Suite 1062 Department of Health and Human Services 330 Independence Ave, SW Washington, D.C. 20201 Fax: 202-708-9824 Online FOIA Request Form

DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20201

FOIA Request 2017-0410

Freedom of Information Act Office
Cohen Bldg, Suite 1062
330 Independence Ave., SW
Washington DC 20201

May 1, 2017

This is in response to the February 11, 2017, Freedom of Information Act (FOIA), request you submitted to the Department of Health and Human Services (HHS), Office of Inspector General (OIG), seeking an electronic copy OAS Policies and Procedures Manual for the Office of Audit Services.

This office located two-twenty-one (221) pages responsive to your request; I have determined to release all two-hundred-twenty-one (221) pages without deletion.

There is no charge for FOIA services in this instance because billable fees are below the Department's $25 cost effective threshold.

I trust that this information fully satisfies your request. If you need any further assistance or would like to discuss any aspect of your request, please do not hesitate to contact our FOIA Requester Service Center at 202.619.2541 or email at FOIA@oig.hhs.gov.

For your information, 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 that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

Sincerely,

Robin R. Brooks
Director
Freedom of Information

Link to
Table of Contents

Do Not Release This Manual - Whether For A Fee Or Not – Without The Specific, Written Authorization Of The Deputy Inspector General For Audit Services!

Office of Audit Services

Audit Policies

And Procedures Manual

(Current Through TN 2017.02 – Issued December 14, 2016)

GLORIA L. JARMON
Deputy Inspector General
for Audit Services

Link to
Table of Contents

OAS AUDIT POLICIES AND PROCEDURES

Transmittals

Transmittal Number	Date	Material Transmitted
2000.01	01/03/2000	Manual Cover; Vision, Mission, and Values Page; Foreword, Table of Contents; and Chapters 10-01, 10-02, 10-03, 10-04, 10-05, 10-06, 10-07, 20-01, 20-02, 20-03, 20-04, 20-05, 20-06, 20-08, 30-01, 30-02, 30-03, 30-04, 30-05, 30-06 and 30-07
2000.02	03/27/2000	Table of Contents, and Chapters 30-01 and 30-05
2000.03	06/14/2000	Chapter 20-02
2000.04	06/16/2000	Table of Contents, Chapters 10-07 and 20-07
2001.01	08/01/2001	Manual Cover, Table of Contents, Chapters 10-02, 10-03, 10-04, 10-06, 10-07, 20-01, 20-02, 20-03, 20-04, 20-05, 20-06, 20-07, 20-08, 30-02, 30-04, 30-05, 30-06 and 30-07
2002.01	12/11/2001	Changed references to the new URL for the OIG website, i.e., http://oig.hhs.gov/, and updated hyperlinks
2002.02	02/15/2002	Chapters 30-01 and 30-05
2002.03	05/08/2002	Chapter 20-02
2003.01	12/04/2002	Chapters 10-04, 30-02 and 30-06
2003.02	01/06/2003	Chapter 30-07
2003.03	02/03/2003	Chapters 20-01, 20-06 and 20-07
2004.01	04/12/2004	Chapter 20-02
2005.01	01/14/2005	Manual Cover, Foreword, Table of Contents, Glossary of Abbreviations and Acronyms, Chapters 10-01,10-02, 10-03, 10-04, 10-05, 10-06, 10-07, 20-01, 20-03, 20-04, 20-05 and 20-07
2005.02	04/29/2005	Table of Contents, and Chapters 30-01, 30-02, 30-03, 30-04, and 30-05. Previous Chapters 30-03 and 30-04 were incorporated in Chapter 30-02. Chapters 30-06 and 30-07 were updated and renumbered as Chapters 30-04 and 30-05.
2006.01	11/14/2005	Chapter 20-06
2006.02	02/03/2006	Chapter 30-05
2006.03	02/15/2006	Chapter 30-02

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2007.01	06/06/2007	Table of Contents expanded to include subsections
2008.01	01/08/2008	Chapters 30-01, 30-02, and 30-03 revised to incorporate new requirements of the July 2007 Yellow Book and other recent OAS policy changes. Also, issued a new chapter, 30-06, which sets forth policies and procedures for preparing report covers, title pages, and page margin notices for reports issued by OAS.
2008.02	01/29/2008	Chapter 30-06
2008.03	02/21/2008	Chapters 20-01, 20-04, 20-05, and 20-07 revised to incorporate new requirements of the July 2007 Yellow Book and other recent OAS policy changes.
2008.04	04/15/2008	Chapters 10-01, 10-02, 10-07, 20-02, 20-03, 20-06, 20-08 and 30-05 revised to incorporate new requirements of the July 2007 Yellow Book and other recent OAS policy changes
2008.05	05/07/2008	Chapters 10-03, 10-04, 10-05, 10-06 and 20-01 revised to incorporate new requirements of the July 2007 Yellow Book and other recent OAS policy changes. Also, issued a new chapter, 20-10, which sets forth policies and procedures for executing scanning tools used to assess vulnerabilities in wireless networks, web applications, and local area networks.
2008.06	09/30/2008	Chapter 30-04 revised to incorporate recent OAS policy changes. Also, issued two new chapters, 20-09 and 20-11. Chapter 20-09 sets forth OAS policies and procedures for reporting to management any incident involving the suspected or confirmed: (1) loss or unauthorized disclosure of Personally Identifiable Information (PII) or loss of electronic media, (2) occurrence or appearance of a threat to an OIG computer system, or any activity that involves using an OIG system in an improper manner, or (3) breach or attempted breach of security in an information system. Chapter 20-11 sets forth OAS policies and procedures for safeguarding sensitive information (both electronic and hard copy) that has been entrusted to OAS. These two chapters replace and expand on the policy email, *Protection of Sensitive OAS Information and Procedures for Reporting Loss of Personally Identifiable Information*, dated January 4, 2007 from the Assistant Inspector General for Grants, Internal Activities, and Information Technology Audits.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2009.01	12/08/2008	Chapter 30-05 revised to incorporate requirements set forth in policy email addressing strengthening controls to ensure that no Personally Identifiable Information (PII) is contained in draft or final reports, including all appendixes, and that sensitive information is appropriately handled. Also, references the required Standard Documentation (SD) 14C, *Sensitive Information Certification*. Chapter 20-06 revised to reference safeguarding of information to Chapter 20-11, Protection of Sensitive OAS Information.
2009.02	06/10/2009	Chapter 20-06 revised to add requirements regarding request about OAS confidentiality standards and/or request to sign a letter of assurance as a condition of being given access to records that contain Personally Identifiable Information (PII) or other sensitive information. Chapter 20-09 revised to cite examples of reportable suspected or confirmed incidents resulting in the loss or unauthorized disclosure of PII or other sensitive data. Examples of reportable incidents include, but are not limited to: • Passphrase/password compromised • Received unencrypted sensitive information from outside the OIG via email • Transmitted unencrypted audit or sensitive information outside the OIG via the HHS OIG Delivery Server • Transmitted encrypted or unencrypted audit or sensitive information outside the OIG via email (OAS employees must use the HHS/OIG Delivery Server to transfer files *outside* the OIG containing audit and/or sensitive information regarding a planned or active audit, or OI or Department of Justice (DOJ) assist work. See Subsection, 20-11-40-06, *Securely Transferring Electronic Files Containing Audit and/or Sensitive Information Over the Internet or Intranet*.) • Unauthorized disclosure of sensitive information • Unauthorized viewing of sensitive information

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2009.02	06/10/2009	Chapter 20-11 revised to: • Provide examples of PII in definition of sensitive information. • Clarify that OAS employees may not use Microsoft Outlook to transfer audit and/or sensitive information, including draft reports, whether or not encrypted, *outside* the OIG. • Add requirement that in lieu of the general disclaimer, all files sent outside the OIG, e.g., correspondence with law enforcement agencies or external peer review teams, containing sensitive, non-public information, such as PII or proprietary information, in addition to being encrypted must contain a special notice at the beginning of the email. Chapter 30-02 revised to: • State that headquarters review is required for headquarters signed and significant regional reports, including the first or "model" report for a nationwide audit. • Provide examples of giving an accounting of audit results for total activity audited in (1) dollars, and (2) sample of claims. • Clarify how to handle auditee's technical comments to draft reports. • Add guidance on how to handle PII contained in auditee's comments on draft and final reports. Chapter 30-04 revised to: • Clarify that for IG signed reports, the OIG Exec Sec prepares and maintains the distribution schedule • Clarify that OAS employees may not use Microsoft Outlook to transfer draft reports, whether or not encrypted, outside the OIG. Unrestricted draft reports, including limited official use draft reports are required to be encrypted before being emailed as an attachment using the HHS/OIG Delivery Server. Chapter 30-05 revised to: • Clarify who signs the SD-14C, *Sensitive Information Certification*, at the time of report packaging for regionally and headquarters signed reports. • Clarify the audit team and independent report reviewer responsibilities relative to PII and other sensitive information.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2010.01	03/15/2010	Chapter 20-07 revised to clarify when auditors should request advice from OCIG. Chapter 20-11 revised to: • Require that staff whole disk encrypt USB software-based encrypted drives with PGP before use (these drives are for OAS internal use only and should not be used to perform data exchange with auditees or others). • State that OAS no longer allows use of any partially encrypted drives. • State that staff should request auditees to consider the need to protect data before providing files to OAS via the auditee's USB drive or CD/DVD. • State that OAS no longer require encrypting files with PGP, or other software, when transmitting draft report files, final report files, and other audit files transferred *outside* the OIG via the HHS/OIG Delivery Server. Chapter 30-02 revised to: • State that an Executive Summary is not required for reports with no findings. • State that a Table of Contents is not required for reports with no findings and no Executive Summary. • State that the name of a sole healthcare practitioner should not be included in a report that will be posted on the Internet. Chapter 30-04 revised to: • State that OAS no longer requires encrypting files when using the HHS/OIG Delivery Server to transmit draft and final report files *outside* the OIG. • Prohibit posting to the Internet a transmittal letter to a sole healthcare practitioner even when the report will be posted on the Internet. Chapter 30-05 revised to clarify that the audit team's responsibilities include cross referencing any alternative text as appropriate for charts, graphs, and other images to the supporting audit documentation.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2010.01	03/15/2010	Chapter 30-06 revised to: • State that the name of a sole healthcare practitioner should not be included in a report title that will be posted on the Internet. • Clarify that the draft report notice is not usually applicable to special audits since these reports are not usually issued in draft. • Clarify that the bottom page margin notice for reports that contain limited official use information.
2010.02	03/23/2010	Chapter 30-01 revised to eliminate requirement to include Executive Summary material in the Memorandum of Impending Release (MIRs). This was done to streamline reports.
2010.03	04/01/2010	Chapter 20-01 revised to state that both the Audit Start Notice and Audit Notification Letters should briefly identify the method for securely transmitting audit information to OAS over the Internet. Revised templates for preparing the Audit Start Notice and Audit Notification Letters are available on the OAS Intranet. Chapter 20-02 revised: • Chapter name to *Sampling and Allocation/Calculation Techniques in Auditing* and updated a number of terminologies. To summarize these changes: o Terms deleted from policy: “mean, projected/projection, universe, unrestricted random sample” o “Estimation” relating to “Estimation Techniques in Auditing” has been changed to “allocation/calculation” o “Sample” terms include: “sample unit, sample size, sample design” o “Sampling” terms include: “sampling frame, sampling plan” o “Population” in certain circumstances was more precisely defined as “sampling frame” o “Item” in certain circumstances was more precisely defined as “unit” • Title of Standard Document SD-9 to “Sampling Plan” • Title of Standard Document SD-10 to “Allocation/Calculation Plan” Chapter 30-03 revised to eliminate requirement to include Executive Summary material in the transmittal memorandums to departmental officials. This was done to streamline reports

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2010.04	08/13/2010	Chapter 30-02 revised to require that acronyms or abbreviations defined in the executive summary and/or report must be defined again the first time they are used in the appendix(s).
2011.01	05/12/2011	Chapter 20-01 revised to: • Add a fourth planning consideration – "Requesting OI Clearance." When starting audits, auditors should request OI clearance to ensure that the auditee is not under OI investigation. Auditors should send their clearance requests through the OAS liaison within the applicable OAS Division. All clearance requests will be coordinated through OI headquarters. • Clarify that audit start notices and audit notification letters should be maintained in the TeamMate file. Chapter 20-06 revised to: • Clarify when TeamMate EWP should be used: o Must be used in all audits that are expected to result in an issued audit report. o May be used to document research and development efforts (however, the Master Audit File does not need to be retained and archived). • Clarify that the divisional/regional TeamMate Coordinators may finalize audits in TeamMate EWP, in addition to the audit teams. Chapter 20-07 revised to: • Eliminate Section 20-07-50, *Computer Matching*, and all references to Public Law 100-503, the *Computer Matching and Privacy Protection Act of 1988* (the Act), since the HHS OIG is no longer subject to the Act due to recent legislation. Chapter 20-11 revised to: • Allow employees to use Outlook Web Access (OWA) on their personally-owned computer – in an emergency. The chapter provides guidance when using OWA on a personally-owned computer. • Clarify when and how employees may and may not use wireless network connections from an/a auditee's office, HHS OPDIV office, hotel and home/apartment.

:

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2011.01	05/12/2011	Chapter 20-11 revised to (continued): • Require that OAS employees must now use the HHS/OIG Delivery Server to transfer limited official use final reports, e.g., recipient capability, bid proposal and contract closeout audits, files *outside* the OIG. Chapter 30-04 revised to: • Clarified that OAS employees must use the HHS/OIG Delivery Server to transfer limited official use reports (draft and final) outside the OIG firewall (OAS employees may not use Microsoft Outlook to transfer limited official use reports, whether or not encrypted, outside the OIG). • Eliminate the designated time period for top management officials such as OPDIV heads to respond directly to OAS. Addressees are still requested to respond directly to OAS with the status of actions taken on recommendations. With these reports, no action official is required. • Clarified that annotated restricted and limited official use reports should be transmitted via the HHS/OIG Delivery Server. Chapter 30-06 revised to: • Change the required notice for Limited Official Use Only reports to: "The organization for whom this report was prepared may distribute the report at its discretions."
2011.02	06/16/2011	Chapter 20-09 revised to: • Simplify the RIG and Headquarter Director responsibilities upon notification or discovery of the suspicion or detection of a loss, compromise, or theft of PII or OAS sensitive information or electronic media. • Add current contact information for the OIG Chief Information Security Office (CISO) and OIG Information System Security Officer (ISSO), including a toll free number. • Add email contact information about the OAS Incident Notification Team. • Update contact information for computer incident detection and reporting responsibilities.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2012.01	11/23/2011	Chapter 20-02 revised. The chapter focuses on two estimation techniques allowable for OAS reports: statistical sampling and mathematical calculations (the later term more clearly describes our second estimation technique previously called *allocation/calculation*). The chapter further explains that OAS will not report an estimate based on nonstatistical sampling. The section (now called judgmental sampling) describes why we do not use judgmental sampling for reporting estimates in reports, and defines procedures for the appropriate use of judgmental sampling in an audit.
2012.02	12/15/2011	Global changes: • Chapters: 10-01, 10-02, 10-06, 20-01, 20-02, 20-03, 20-05, 20-06, 20-07, 20-08, and 30-04 revised to update references to the *Government Auditing Standards* August 2011 edition. • Chapters: 10-01, 10-02, 20-01, 20-04, 20-06, and 20-11 revised to state that it is the policy of OAS to use TeamMate EWP to prepare TeamMate Current Issues, also known as OARS (Chapter 10-01) and add references to TeamMate Current Issues when referring to OARS. OARS are now created from TeamMate Issues within TeamMate EWP. Chapter 10-01 revised to: • State that it is the policy of OAS to use TeamMate EWP to prepare TeamMate Current Issues (in TeamMate R10) or Exceptions (in TeamMate R8), also known as Objective Attributes Recap Sheets (OARS). • Add that the DIG may grant a waiver of a specific policy contained in this manual on a case-by-case basis. All waiver requests should be submitted in writing to the DIG through the appropriate AIG or RIG. All waivers will be documented in the TeamMate file of the applicable audit. Chapter 10-03 revised to add a new area that is now part of the FMFIA Review – Billing for Reimbursable Audits. The review of this new FMFIA area is performed only at Headquarters. Chapter 10-07 revised to address the conceptual framework for independence added in the *Government Auditing Standards* 2011 edition to provide a means for auditors to assess auditor independence to activities that are not expressly prohibited.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2012.02	12/15/2011	Chapter 20-09 revised to: • Move reporting the receipt of unprotected personally identifiable information (PII) from third parties via email from this chapter to chapter 20-12. • Give guidance on the types of information about the incident that should be included in the employee's report: *Report of Suspected or Actual Loss, Compromise, or Theft of Personally Identifiable Information, OAS Sensitive Information, or Electronic Media.* • Rename to SD-19 to SD-19A*, Report of Suspected or Actual Loss, Compromise, or Theft of Personally Identifiable Information, OAS Sensitive Information, or Electronic Media* due to third party incident moved to new chapter 20-12. Chapter 20-11 revised to cite current Department definition of sensitive information. Chapter 20-12 new chapter added to: • Establish OAS policies and procedures regarding: o Notifying auditees, OPDIVs, organizations, and persons (third parties) contacted for information during the course of an audit how to properly safeguard personally identifiable information (PII) transmitted to OAS over the Internet. o Action required when OAS receives unprotected PII within an email (i.e., where unencrypted PII is contained within an email message or attachment) from any third-party. • Give guidance on the types of information about the incident that should be included in the employee's report, *SD-19B, Report of Receipt of PII not sent to OAS via the HHS/OIG Delivery Server or Other Approved Site.* • Refer to a new template for responding when OAS receives PII via email instead of via the HHS/OIG Delivery Server or other approved site. This template provides the sender with a statement to raise awareness of the importance of protecting PII and provides instructions in requesting authorization to use the HHS/OIG Delivery Server to securely send information to OAS. Chapter 30-02 revised to: • Add that OAS complies with the Plain Writing Act of 2010. • Add a requirement the audit team must not release a draft report in any form (e.g., a working draft) to any entity external to OIG prior to its formal release. The audit team may share the preliminary results of an audit with an auditee or OPDIV using OARS or another document that briefly outlines the audit results.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2012.02	12/15/2011	Chapter 30-02 revised to (continued): • Add a chart identifying criteria for IG and DIG signed reports moved from chapter 30-03 and revised. • Remove the definition of significant audit matters. Chapter 30-03 revised to: • Change from 60 days to 6 months the period internal auditees should be directed to provide OAS with the status of actions taken or contemplated on recommendations form the report issue date. • Update who may sign reports and moved information to chapter 30-02. Chapter 30-05 revised to remove the requirement to complete and sign the Standard Documentation (SD) 14C, *Sensitive Information Certification.* SD-14C has been removed from the OAS Intranet. Important note: The requirement that draft and final reports and their appendixes, with the exception of reports prepared for OI, OCIG, or DOJ, contain no personally identifiable information (PII) is still in place. Chapter 30-06 revised to give guidance for preparing report titles. Titles will briefly describe the results of the audit.
2012.03	1/26/2012	Chapter 10-01 revised to update references to the *Government Auditing Standards* December 2011 edition. Chapter 10-07 revised to give examples of safeguards designed to eliminate or reduce to an acceptable level threats to independence that may be effective under certain circumstances: • Consulting an independent third party, such as a professional organization, a professional regulatory body, or another auditor. • Involving another audit organization to perform or reperform part of the audit. • Having a professional staff member who was not a member of the audit team review the work performed. • Removing an individual from an audit team when that individual's financial or other interests or relationships pose a threat to independence.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2013.01	12/14/2012	Chapter 10-02 revised to state that an experienced staff member, the senior auditor, or the audit manager can sign-off on audit documentation. The level of staff members performing the sign-off and the extent of their review will vary and will depend on a number of factors including professional judgment, experience of the staff, and the complexity and significance of the audit. The audit manager is not required to sign-off on audit documentation for all audits. Chapter 20-06 revised: • Section renamed and revised to be consistent with *Government Auditing Standards* (Discontinued Audit Efforts are now called Terminated Audits). • Added that communication to management of the reasons for terminating the audit be documented in TeamMate, and if such communication might compromise an ongoing or contemplated investigation, the audit team should consult with OI for advice on handling the matter. • New requirement to record audit suspension start dates in WebAIMS, and to document the reason for the suspension in the "Comments" section within the WebAIMS audit record. When the audit resumes, the suspension end date should be recorded in WebAIMS. Chapter 20-10 revised: • Only two persons instead of five persons need approve the scan: the cognizant audit manager and the Information Technology (IT) Audit Director. • Only one auditor needs to conduct the electronic vulnerability scan instead of two. Each region should designate a backup auditor to execute the approved scan. The backup auditor must have received appropriate training and be identified on the SD-18. • Revised SD-18, Electronic Vulnerability Assessment Authorization Form for the two above items. • New actions needed to validate potential findings. • Vulnerability assessment reports generated by the scan applications should not be included as part of the audit report.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2013.01	12/14/2012	Chapter 20-11 revised: • OAS employees must not use CDs/DVDs to store sensitive information, except for TeamMate files maintained in the regional or divisional safes, without advance approval in writing from the Information Technology (IT) Audit Director. • Software used on IT audits may be kept on unencrypted media (exception to general requirement). • Identified actions employees must take to safeguard sensitive information stored on CD or DVD. Chapter 30-02 revised: • Any Congressional correspondence should be submitted to the Headquarters Review Team via email at OASHQReview@oig.hhs.gov. The Headquarters Review Team will coordinate its review with the Office of External Affairs. • Dropped requirement of including a title page in reports. All references to use of title page have been removed from the policy manual. • Section renamed and revised to be consistent with *Government Auditing Standards* (Discontinued Audit Efforts are now called Terminated Audits). • Added that communication to auditee management of the reasons for terminating an audit be documented in TeamMate, and if such communication might compromise an ongoing or contemplated investigation, the audit team should consult with OI for advice on handling the matter. Chapter 30-03 revised: • Dropped requirement that transmittal memorandums include information on the program, function or activity, and period audited. • Initial drafts may be issued to obtain comments from entities to which recommendation are not addressed prior to issuing another draft to the entity to which recommendations are addressed. Chapter 30-04 revised for clarity: Procedures of when to send reports to the OPDIV's audit liaison and when to send reports to the head of the entity and the entity's liaison, if any.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2013.01	12/14/2012	Chapter 30-06 revised: • Dropped requirement of including a title page in reports. All references to use of title page have been removed from the policy manual. • Dropped requirement to use blue cover reports and green cover reports to designate reports not containing or containing restricted or limited official use information. All references to use of blue or green cover reports have been removed from the policy manual. All report covers are now printed on white paper. • Each report cover will include the: o Name of the official signing the report and their title (i.e., Inspector General, Deputy Inspector General, Assistant Inspector General, or Regional Inspector General). If the official signing the draft report and the official signing the final report (or MIR) are not the same, the name and title of the official signing the final report should also be used on the draft report. o Following statement: *Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov*
2013.02	7/19/2013	Chapter 20-02 revised to add requirement in the chapter and in SD 9, *Sampling Plan* and SD-10, *Mathematical Calculation Plan* to (1) identify the sources of data to be used, e.g., National Claims History, or OIG Data Warehouse, (2) describe the data validation work performed by the audit team, and (3) reference the required SD-22, *Assessing the Reliability of Computer-Processed Data* in SD-9 and SD-10. Chapter 20-03 revised to require that auditors perform a data reliability assessment for all computer-processed data that support findings, conclusions, or recommendations. The assessment should be conducted early in the audit process, well before using the data in the audit. The auditors should document this assessment using SD 22, *Assessing the Reliability of Computer Processed Data*. Chapter 20-06 revised to remove the sentence, “To do so would violate software licensing agreements.” Reason: TeamEWP Reader R10 is license free. TeamEWP Reader is a new product released with TeamEWP R10. Chapter 30-02 revised to codify changes in the report writing and formatting implemented over the past year. Chapter 30-07 - new chapter added to establish policies and procedures for reporting and coding monetary recommendations in OAS audit reports.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2015.01	12/15/2014	Changes were made to numerous chapters to reflect current organizational structure and titles. Chapter 10-01: • Changed to incorporate references to the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. 200.513). We did not eliminate references to superseded circulars as they remain in effect for grants made before December 26, 2014. • Added a requirement to document critical team meetings in working papers. • Clarified that only the DIG may waive policy unless the specific policy itself designates another official. Chapter 10-03: • Changed to reflect that OMP now performs FMFIA reviews previously performed by AMP. Chapter 10-07: • Changed the WebAIMS independence statement to cover all jobs an auditor worked on, not just listed CINS. This change also reflects that an auditor's responsibility is to notify his or her supervisor of any impairment to independence. The supervisor is still responsible for working with the auditor to eliminate the threat or remove the auditor from the assignment. Chapter 20-01: • Clarified that OI clearance is not required for audits of State agencies or reimbursable audits. Note that if an audit of a State agency involves review of a specific provider, OI clearance with respect to that provider should be obtained. Chapter 20-04; • Eliminated all references to Disclosure Statement audits because these are the responsibility of the Division of Cost Allocation and OAS has not been asked to perform these for many years. • Added references to the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. 200.513).

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2015.01	12/15/2014	Chapter 20-08: • Deleted obsolete language about acknowledging allegations in writing. • Deleted obsolete language about early involvement of OAS management. Chapter 30-02: • Changed the dollar threshold for DIG signature from $1 million to $5 million. (Note – DIG signature is still required if the report (or MIR) is addressed to a Department official or OPDIV Head). • Added that AIGs may sign reports on an ad-hoc basis with the approval of the DIG. • Added that AIG signed reports that will be posted on the internet should be submitted to the Headquarters Review Team for review unless the DIG approves issuance without Headquarters review. Chapter 30-04: • Changed to reflect that posting of reports on the internet is now required within 3 days of issuance.
2015.02	3/9/2015	Chapter 20-06: • Clarified that audit documentation, including electronic media, should be retained for a minimum of 8 years from the end of the fiscal year in which the audit report was closed and the recommendation(s) resolved, which occurs when OAS accepts the OPDIV signed OIG clearance documents (OCD).
2015.03	3/16/2015	Chapter 20-02: • Clarified that methods of statistical sampling not described in the chapter may be used under a waiver from the OAS statistician • Clarified that statistical sampling may be used for purposes other than estimation if the OAS statistician is consulted during development of the sample plan • Clarified that the lower bound must be presented alongside the point estimate when the two figures differ materially • Clarified the circumstances under which plans should be submitted to the OAS statistician • Clarified what should be included in the Survey Information section of the sampling plan

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2015.03	3/16/2015	Chapter 20-02 (continued: • Eliminated the requirement for a minimum number of errors to make an estimate when certain conditions are satisfied and reduced the minimum number of errors to make an estimate when those conditions are not satisfied • Eliminated the requirement that the sampling plan include the elapsed time to locate sample items and time to evaluate sample items • Clarified that when a stratified sample includes a certainty stratum, a minimum of 100 sample items must be randomly selected • Removed references to estimating an unknown population size because this practice is very infrequent • Changed to require a waiver of any requirements in this chapter from the OAS statistician Chapter 20-09 • Changed to allow initial reporting of an incident via email alone (no telephone call required) Chapter 20-11 • Changed to reflect that OAS employees must not use OIG's Aventail VPN when using non-OIG computers (because OIG's Aventail VPN is not installed in non OIG computers) • Changed to reflect that employees must only access email on an OIG computer or other OIG device. • Clarified the circumstances under which an employee may use wireless access on an OIG computer in a public hotspot and the precautions required • Changed to reflect that OAS employees should use judgment when deciding whether to convert all electronic files to PDF before sharing them outside the OIG • Clarified that unrestricted draft reports sent to OPDIVs do not need to be sent using the OAS Delivery Server (this change was made to accommodate the Immediate Office's practice of sending draft reports to OPDIVs using MS Outlook) • Clarified that sensitive information (hard copy or electronic) can be sent using the U.S. Mail or OIG approved common carrier

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2015.03	3/16/2015	Chapter 20-11 (continued): • Deleted dated information about obtaining or retaining electronic hard copies and scanning hard copies • Eliminated discussion of OAS approved disposal resources and excessive language from the section of the chapter covering destruction of sensitive information • Modified the section on accessing OIG networks to reflect current OAS-wide practices Chapter 20-12 • Changed to allow initial reporting of an incident via email alone (no telephone call required)
2015.04	6/24/2015	Chapter 30-01 content revised and renamed. The chapter title was formerly (*Memorandums to Management*). The new title is *Informing Department Officials About Significant Preliminary Findings or Significant Risk and Significant Audits of External Entities.* The most significant changes are: • The definition of early alert has been expanded to cover situations where we do not expect to issue a report on the matter covered. • Early alerts of significant preliminary findings or significant risk resulting from an audit of Department programs or operations will generally be posted on the internet. (Consistent with past OAS practices, early alerts of significant preliminary findings resulting from an audit of a contractor, grantee, or other external entity generally not be posted on the internet). • The Department/OPDIV will be given an opportunity to comment (informally) on early alerts that will be posted on the internet.
2016.01	9/08/2016	Chapter 10-05 • Changed to reflect current terminology and training requirements and to incorporate information about the reporting options for contracted audits. Chapter 20-05 • Revised to clarify that a separate SD-8 has to be completed for each specialist or organization whose work is relied on in conducting the audit. Chapter 30-02 • Changed to include the elimination of most RIG cover reports and the introduction of Public Summary reports (summaries of restricted reports that can be posted on the internet). • Did not make changes to eliminate the proscription on releasing draft reports outside of OIG before they are officially issued.

OAS AUDIT POLICIES AND PROCEDURES

Transmittals (Continued)

Transmittal Number	Date	Material Transmitted
2017.01	10/25/2016	Chapter 10-07 • All non-administrative employees will certify their independence on *Annual Independence Certification Form.*
2017.02	12/14/2016	Chapter 30-01 • Eliminated the option to issue an early alert when we don't expect to issue a subsequent audit report • Changed to reflect that all early alerts, including those related to audits of entities outside the Department, will be posted on the internet unless the related report will be restricted or otherwise approved by the DIG • Added a requirement to use a Common Identification Number (CIN) on Early Alerts that is different from the CIN used for the audit • Added a requirement to obtain comments on an early alert from both the Department/OPDIV and an auditee outside the Department • Eliminated the requirement for all early alerts to be reviewed by the HQ review team (this is now at the discretion of the AIG) • Changed to reflect that an AIG may sign an Early Alert or MIR

DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDIT SERVICES

Our Vision

We make a difference by creating together a timely, valued product that is used by our customers.

Our Mission

We, the independent auditors for the Department of Health and Human Services, identify and report ways to improve, through a shared commitment with management, the economy, efficiency and effectiveness of operations and services to recipients of HHS programs.

Our Values

We value:

- timely, fairly presented, quality products that meet our customers' needs.
- integrity, honesty, independence, objectivity, proficiency and due care in performing our work.
- teamwork as crucial to achieving our mission.
- a work environment that supports our personal and professional needs and encourages us to be innovative and reach our full potential.
- open communications with our customers and each other.

AUDIT POLICIES AND PROCEDURES MANUAL

Foreword

The Office of Audit Services (OAS) *Audit Policies and Procedures Manual* provides policies, standards, technical guidance and other techniques aimed at producing quality, timely audit results while making the best use of available resources. The guidance is consistent with the U.S. Comptroller General's publication, *Government Auditing Standards*. These standards incorporate, by reference, generally accepted auditing standards for field work and reporting for financial audits issued by the American Institute of Certified Public Accountants. The OAS policy is to adhere to all applicable government auditing standards in every audit.

The Audit Process (TAP) Handbook and *Report Handbook* provide OAS auditors with additional guidance and tools for conducting audits and preparing reports. The *TAP Handbook* lays out a systematic approach to auditing based on ensuring team participation, setting clear objectives for each assignment, and maintaining a focus on development of the attributes of an audit finding. The Objective Attributes Recap Sheet (OARS), an integral part of TAP, focuses the audit team on the audit objective, provides a logical and documented progression through the phases of the audit, and integrates report preparation throughout the audit process. If the TAP process is applied effectively, the content of the audit report should be substantially developed during the course of the audit. *Report Handbook* provides assistance in drafting, fine tuning, and reviewing the audit report and provides a sample report format which is logical and easy to write, read and review. These handbooks, although primarily intended as guidance, contain certain policy implications which are incorporated by reference in the *OAS Audit Policies and Procedures Manual*.

Together with the *TAP Handbook* and *Report Handbook*, the *OAS Audit Policies and Procedures Manual* guides OAS staff in fulfilling their mission to identify and report ways to improve, through a shared commitment with management, the economy, efficiency, and effectiveness of operations and services to beneficiaries of HHS programs. The *OAS Audit Policies and Procedures Manual* may be revised from time to time as new challenges and concerns arise. Auditors should also refer to the OAS Intranet for audit guidance, technical information, audit resources and other information of interest.

TABLE OF CONTENTS
(as of December 14, 2016)

General Chapters

TABLE OF CONTENTS *(Continued)*

General Chapters *(Continued)*

TABLE OF CONTENTS *(Continued)*

Auditing Chapters

TABLE OF CONTENTS *(Continued)*

Auditing Chapters *(Continued)*

TABLE OF CONTENTS *(Continued)*

Auditing Chapters *(Continued)*

TABLE OF CONTENTS *(Continued)*

Auditing Chapters *(Continued)*

TABLE OF CONTENTS *(Continued)*

Auditing Chapters *(Continued)*

TABLE OF CONTENTS *(Continued)*

Auditing Chapters *(Continued)*

TABLE OF CONTENTS *(Continued)*

Reporting Chapters

TABLE OF CONTENTS *(Continued)*

Reporting Chapters *(Continued)*

TABLE OF CONTENTS *(Continued)*

Reporting Chapters *(Continued)*

TABLE OF CONTENTS *(Continued)*

Reporting Chapters *(Continued)*

TABLE OF CONTENTS *(Continued)*

Exhibits

Glossary of Abbreviations and Acronyms

AICPA	American Institute of Certified Public Accountants
AIG	Assistant Inspector General for Audit Services
AIMS	Audit Information Management System
API	Audit Planning and Implementation
ASBTF	Assistant Secretary for Budget, Technology and Finance
BPA	Bid Proposal Audit
CASB	Cost Accounting Standards Board
CFE	Certified Fraud Examiner
CFO	Chief Financial Officers Act of 1990
CGFM	Certified Government Financial Manager
CFR	Code of Federal Regulations
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIN	Common Identification Number
CISA	Certified Information Systems Auditor
CCA	Contract Closeout Audit
CMS	Centers for Medicare and Medicaid Services
CPA	Certified Public Accountant
CPE	Continuing Professional Education
DAB	Departmental Appeals Board (HHS)
DIB	Data Integrity Board (HHS)
DCA	Division of Cost Allocation
DCAA	Defense Contract Audit Agency
DOJ	Department of Justice
DIG	Deputy Inspector General for Audit Services
E-FOIA	Electronic Freedom of Information Act Amendments of 1996
F&ACA	Facility and Administrative Cost Audit
FAR	Federal Acquisition Regulation
FASA	Federal Acquisition Streamlining Act of 1994
FFP	Federal Financial Participation
FMFIA	Federal Managers' Financial Integrity Act
FOIA	Freedom of Information Act, as amended
GAM	Grants Administration Manual (HHS)
GPD	Grants Policy Directives (HHS)
GAO	Government Accountability Office
IRR	Independent Report Review
HHS	U.S. Department of Health and Human Services
HHSAR	HHS Acquisition Regulation
HRSA	Health Resources and Services Administration
IG	Inspector General - HHS
IG Act	The Inspector General Act of 1978
IRS	Internal Revenue Service
KSA	Knowledge, Skills and Abilities
NEAR	National External Audit Resource Center
OARS	Objective Attributes Recap Sheets

Glossary of Abbreviations and Acronyms (Continued)

OAS	Office of Audit Services (HHS/OIG)
OCIG	Office of Counsel to the Inspector General (HHS/OIG)
OGE	U.S. Office of Government Ethic
OI	Office of Investigations
OIG	Office of Inspector General (HHS/OIG)
OIG ES	Office of Inspector General Executive Secretariat
OMB	Office of Management and Budget
OPDIV	Operating Division
RCA	Recipient Capability Audit
RIG	Regional Inspector General for Audit Services
SAS	Statements on Auditing Standards (AICPA)
SSA	Social Security Administration
STAFFDIV	Staff Division
TAP	The Audit Process
TIMS	OIG Training Information Management System
WebAIMS	Web Audit Information Management System

Part I

General Chapters

AUDIT POLICIES

10-01-00 PURPOSE

This manual consolidates the policies, procedures, standards, technical guidance and other techniques to be followed by OAS staff in planning and conducting audit work of HHS and in preparing related reports on behalf of OIG.

The standards, definitions and audit requirements to be followed in executing the OAS mission were compiled from a variety of sources. This manual is intended to be consistent with external standards and to ensure that audit services conducted by or on behalf of OAS are fair, professional, objective and reliable.

10-01-10 STANDARDS AND AUDIT REQUIREMENTS

Generally accepted government auditing standards are set forth in the Government Accountability Office (GAO) publication entitled *Government Auditing Standards*. These standards, revised December 2011, describe the types of audits and attestation engagements that audit organizations perform, or arrange to have performed of government entities, programs and federal awards administered by contractors, nonprofit entities and other nongovernmental entities.

The December 2011 edition of *Government Auditing Standards* defines two types of audits, financial audits and performance audits. *Government Auditing Standards* also define attestation engagements, which are governed by the American Institute of Certified Public Accountants' (AICPA) Standards for Attestation Engagements. The types of audits and attestation engagements are briefly described below.

Financial audits include financial statement audits and other related services covered by the AICPA's *Statements on Auditing Standards.* Performance audits encompass a wide variety of audit objectives. *Government Auditing Standards* list four types of audit objectives: (1) program effectiveness and results, (2) internal control, (3) compliance (financial or nonfinancial), and (4) prospective analysis. OAS audits sometimes encompass multiple audit objectives (e.g., internal control and compliance). Attestation engagements concern examining, reviewing or performing agreed-upon procedures on a subject matter or an assertion. Chapter 2 of the *Government Auditing Standards* discusses types of audits and attestation engagements.

Within OAS, most audits we conduct are performance audits. Financial audits as required by the Chief Financial Officers (CFO) Act of 1990 are also performed. This work is often completed, under arrangement, by audit organizations other than OAS. OAS does not routinely conduct attestation engagements. Attestation engagements that are performed by OAS staff require prior written approval of the DIG. No OAS auditor will perform an attestation engagement without first receiving the appropriate training as determined by the AIG for Audit Management and Policy.

AUDIT POLICIES

10-01-00 PURPOSE

This manual consolidates the policies, procedures, standards, technical guidance and other techniques to be followed by OAS staff in planning and conducting audit work of HHS and in preparing related reports on behalf of OIG.

The standards, definitions and audit requirements to be followed in executing the OAS mission were compiled from a variety of sources. This manual is intended to be consistent with external standards and to ensure that audit services conducted by or on behalf of OAS are fair, professional, objective and reliable.

10-01-10 STANDARDS AND AUDIT REQUIREMENTS

Generally accepted government auditing standards are set forth in the Government Accountability Office (GAO) publication entitled *Government Auditing Standards*. These standards, revised December 2011, describe the types of audits and attestation engagements that audit organizations perform, or arrange to have performed of government entities, programs and federal awards administered by contractors, nonprofit entities and other nongovernmental entities.

The December 2011 edition of *Government Auditing Standards* defines two types of audits, financial audits and performance audits. *Government Auditing Standards* also define attestation engagements, which are governed by the American Institute of Certified Public Accountants' (AICPA) Standards for Attestation Engagements. The types of audits and attestation engagements are briefly described below.

Financial audits include financial statement audits and other related services covered by the AICPA's *Statements on Auditing Standards.* Performance audits encompass a wide variety of audit objectives. *Government Auditing Standards* list four types of audit objectives: (1) program effectiveness and results, (2) internal control, (3) compliance (financial or nonfinancial), and (4) prospective analysis. OAS audits sometimes encompass multiple audit objectives (e.g., internal control and compliance). Attestation engagements concern examining, reviewing or performing agreed-upon procedures on a subject matter or an assertion. Chapter 2 of the *Government Auditing Standards* discusses types of audits and attestation engagements.

Within OAS, most audits we conduct are performance audits. Financial audits as required by the Chief Financial Officers (CFO) Act of 1990 are also performed. This work is often completed, under arrangement, by audit organizations other than OAS. OAS does not routinely conduct attestation engagements. Attestation engagements that are performed by OAS staff require prior written approval of the DIG. No OAS auditor will perform an attestation engagement without first receiving the appropriate training as determined by the appropriate AIG.

The OAS operations are also guided by:

- The Inspector General Act of 1978 (IG Act). The IG Act, as amended, requires that audit work conducted by the Federal Inspectors General and by nonfederal auditors on their behalf comply with *Government Auditing Standards*.

- Council of the Inspectors General on Integrity and Efficiency (CIGIE). The CIGIE has promulgated standards in the publication, Quality Standards for Federal Offices of Inspector General, issued in October 2003.

These standards apply to governmental audit activities and are consistent with *Government Auditing Standards*. The CIGIE has also developed standards and detailed guidance for conducting external quality control reviews of OIG audit operations.

For financial statement audits performed in accordance with the CFO Act, the GAO has issued the *Financial Audit Manual*.

- Office of Management and Budget (OMB) Circulars. The OMB has issued various circulars and bulletins that either requires audits to be conducted in accordance with Government Auditing Standards or otherwise affect how audits of HHS operations and activities are to be conducted. Some OMB circulars relevant to our work are:

SELECTED OMB CIRCULARS

A-21	Cost Principles for Educational Institutions[1]
A-50	Audit Follow up
A-87	Cost Principles for State, Local and Indian Tribal Governments[2]
A-102	Grants and Cooperative Agreements with State and Local Governments
A-110	Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals and Other Non-Profit Organizations
A-122	Cost Principles for Non-Profit Organizations[3]
A-123	Management's Accountability and Control
A-127	Financial Management Systems
A-133	Audits of States, Local Governments, and Non-Profit Organizations
A-134	Financial Accounting Principles and Standards
A-136	Financial Reporting Requirements

Note: Circulars A-21, A-50, A-87, A-102, A-110, A-122, and A-133 will be replaced by 2 C.F.R. 200 Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards. See 2 C.F.R. 200 for effective dates.

In addition to the circulars, OMB has issued the following bulletin that is related to OAS work under the CFO Act: 07-04 Audit Requirements for Federal Financial Statements

[1] 2 CFR 220
[2] 2 CFR 225
[3] 2 CFR 230

- *The Audit Process* handbook. OAS issued this handbook to provide tools for auditors to conduct audits and prepare reports. The goal of the OAS is to have audits conducted in a simultaneous mode where all of the participants in the process are fully aware of and in agreement with the objectives of the audit and the attributes of the findings as they are developed. This handbook contains policy implications that are discussed in Section 10-01-30.

10-01-20 POLICY

It is OAS policy to adhere to all applicable *Government Auditing Standards* in every audit. OAS will incorporate applicable *Government Auditing Standards* into the audit process and, when appropriate, into procedures issued for guidance of OAS auditors. These standards are designed to set the tone for the use of professional judgment by those involved in performing work on a wide variety of assignments. Specific guidance on the OAS implementation is set out in subsequent chapters.

It is OAS policy to periodically review the procedures and practices followed in OAS audits and to initiate prompt action necessary to ensure compliance with *Government Auditing Standards*.

If OAS agrees to perform nonaudit services, *Government Auditing Standards* must not be cited in any report that results from such services.

10-01-30 THE AUDIT PROCESS

The Audit Process handbook also contains policy requirements for OAS audits. For these audits, it is the policy of OAS to use a teamwork approach to audits, use TeamMate EWP[4] to prepare TeamMate Current Issues,[5] also known as Objective Attributes Recap Sheets (OARS), and conduct team meetings at critical decision points in the audit.

A teamwork approach to audits can be especially effective when performed by qualified professionals who work together on an audit and are focused on clear objectives. In the OAS, a team is formed at the beginning of the audit and includes all participating staff auditors, senior auditors, and managers at both the regional and headquarters levels.

TeamMate Current Issues include an audit objective, the attributes relating to that objective, and the comments of auditee personnel.

Team meetings should be held throughout the audit as needed. An important key to successful audits is quality communication among all assigned team members. At a minimum, team meetings should be held during the planning, survey and reporting phases. Meetings can be conducted in person or by using other means such as teleconferences. At these meetings, team members should agree on the audit objectives and/or the finding attributes.

Each of these meetings should be documented in TeamMate, including: the date of meeting, attendees, and key decisions made as a result of the meeting

[4] EWP – Electronic Working Papers

[5] In TeamMate Release 10 the finding screen is called “Issue” and in TeamMate Release 8 the finding screen is called “Exception.” Both are the same in that they include an audit objective, the attributes relating to that objective, and the comments of auditee personnel. When needed to be reviewed outside of TeamMate EWP, an Issue or Exception report can be generated in TeamMate EWP by using the SD-4, OARS report.

10-01-40 WAIVER OF OAS POLICY

Only the DIG may grant a waiver of a specific policy requirement contained in this manual unless another official is designated by the policy being waived. All waiver requests should be submitted to the DIG (or other specified official) in writing through the appropriate AIG or RIG before the draft report is issued and will be considered on a case-by-case basis. All waivers will be documented in the TeamMate file of the applicable audit.

AUDIT SUPERVISION

10-02-00 PURPOSE

This chapter establishes policies and procedures relative to audit supervision in OAS.

10-02-10 STANDARDS

Chapter 6 of the *Government Auditing Standards* requires audit staff be properly supervised.

10-02-20 POLICY

It is OAS policy to properly supervise all staff to ensure that the audit objectives are accomplished and applicable standards are followed.

10-02-30 OVERVIEW

OAS uses a team concept to conduct audits, which enables all levels of management to be appropriately involved in all phases of the audit process. This team concept requires timely communication, full cooperation, and professional diligence at each level. The audit team can include staff auditors, senior auditors, managers, and directors at both the regional and headquarters level.

The most effective way to ensure quality in an audit assignment and to expedite its progress is by exercising proper supervision. Supervision adds seasoned judgment to the work performed by less experienced staff and facilitates on-the-job training.

Audit managers are responsible for assuring that staff are properly supervised and that the audit work is reviewed. The audit manager should also make sure that supervision and reviews are appropriately documented. Although supervisory authority rests with the audit manager, the manager may delegate supervisory tasks to other experienced team members, and/or other qualified personnel assigned to the manager.

Supervisory tasks can be performed by staff assigned to the audit, depending on the make-up of the audit team and the nature of the work being performed. In most cases, audit teams include a senior auditor who is directly involved in the daily audit operations. Audit managers can delegate supervisory tasks to senior auditors, including the review of audit documentation, and other responsibilities as outlined in the following section. Further, audit teams often include highly experienced staff members who are also capable of appropriate supervisory tasks. These staff members can review audit documentation of the senior auditor as well as provide supervision to less experienced staff members on the team. Staff members can contribute in the audit process by checking each other's work and serving as sounding boards to resolve complex issues.

10-02-40 SUPERVISORY RESPONSIBILITIES

Elements of supervision include providing sufficient guidance and direction to team members, keeping informed about significant problems encountered, reviewing the work performed, and providing effective on-the-job training. Team members should clearly understand their assigned tasks before starting the work. Staff should be informed of not only what work they are to do and how they are to proceed, but also why the work is to be conducted and what is to be accomplished.

Skills and knowledge vary among auditors. Accordingly, work assignments should be commensurate with abilities. Collectively, the work assignments should ensure efficient and effective achievement of audit objectives.

Team members providing supervision to staff should clearly convey their expectations. Similarly, staff should keep supervisors informed on significant audit activities. Also, supervisors should deal in a timely manner with changing or unanticipated priority audit matters.

Supervisory review of audit work should continue throughout the audit to ensure:

- The team establishes audit objectives at the start of the audit and adjusts them based on audit developments.
- The TeamMate Current Issues, also known as Objective Attributes Recap Sheets (OARS), are appropriately prepared.
- A written audit plan is properly prepared and followed.
- The work conforms to audit standards and OAS policies and procedures.
- The audit objectives are accomplished.
- The audit documentation provides sufficient, appropriate evidence to support findings and conclusions and provides sufficient data to prepare the audit report.
- The report effectively communicates the results of the audit.

10-02-50 PROVIDING SUPERVISION

Supervisory review of audit work should continue throughout the audit. The extent of supervision provided depends on many factors, including the size and complexity of the audit, the significance of the work, and the experience of staff performing the work.

With experienced staff, the supervisor's role may be more general. Supervisors may outline the scope of the work and leave details to the audit staff. With less experienced staff, supervisors may need to specify audit procedures to be performed as well as techniques for gathering and analyzing data. Within OAS, senior auditors generally fulfill this role.

Proper supervision is facilitated throughout the audit process through the use of team meetings. Team meetings provide a forum for many supervisory responsibilities to be performed. At these meetings staff members can address issues, and supervisors can provide input as part of the decision making process.

TeamMate Current Issues can also facilitate meaningful audit supervisory and management review. The OARS helps supervisors plan the audit, assess progress, review findings, outline the report, and conduct conferences.

10-02-60 DOCUMENTING SUPERVISION

Supervision should be documented. Since supervisory review is accomplished through various means, the nature of the documentation will also vary. Evidence of audit supervision could include records of team meetings, review notes, and sign-offs of audit documentation.

Supervisory review, including the audit manager's involvement with the team, is often provided through meetings, phone calls, and e-mails. These communiqués should be documented. For example, if guidance is provided by the audit manager via telephone, a log of the conversation and a brief description of the guidance/decision could be included in the audit documentation.

The most notable evidence of supervision is usually demonstrated by sign-offs or review notes in the audit documentation. Sign-offs can be either on individual documents or a series of documents.

An experienced staff member, the senior auditor, or the audit manager can sign-off on audit documentation. The level of staff members performing the sign-off and the extent of their review will vary and will depend on a number of factors including professional judgment, experience of the staff, and the complexity and significance of the audit. The audit manager is not required to sign-off on audit documentation for all audits.

QUALITY CONTROL AND ASSURANCE

10-03-00 PURPOSE

This chapter sets forth OAS policies and procedures on quality control and assurance. These policies incorporate the requirements of the Federal Managers Financial Integrity Act (FMFIA) and the Office of Management and Budget (OMB) Circular A-123, *Management Accountability and Control*, into the OAS system of quality control.

10-03-10 STANDARDS

Chapter 3 of the *Government Auditing Standards* requires that each audit organization performing audits or attestation engagements in accordance with *Government Auditing Standards* establish a system of quality control that is designed to provide the audit organization with reasonable assurance that the organization and its personnel comply with professional standards and applicable legal and regulatory requirements, and have an external peer review at least once every 3 years.

Quality Standards for Federal Offices of Inspector General recommends that each OIG establish and maintain a quality assurance program to ensure that work performed: (1) adheres to established OIG policies and procedures; (2) meets established standards of performance, including applicable professional standards; and (3) is carried out economically, efficiently, and effectively.

The Federal Managers Financial Integrity Act (FMFIA)[1] requires that:

- Internal accounting and administrative control standards be developed by the Government Accountability Office (GAO).
- Annual evaluations be conducted by each executive agency of its system of internal accounting and administrative control in accordance with guidelines established by the Director of the OMB.
- Annual statements be submitted by the head of each executive agency to the President and the Congress on the status of the agency's system of internal controls.

OMB Circular A-123 provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal controls. Management is responsible for establishing and maintaining internal controls to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations.

[1] Guidelines for complying with the FMFIA are included in OMB Circular A-123, *Management's Responsibility for Internal Control*.

10-03-20 POLICY

The OAS quality control system is designed to ensure that all OAS work complies with *Government Auditing Standards* and adheres to established OAS policies and procedures. OAS quality control consists of two elements: an internal quality control and assurance system, and external quality control reviews.

- Internal Quality Control and Assurance System - This system includes quality control procedures and functions, including internal quality control reviews (IQCR), that help to ensure that OAS work is performed in conformance with applicable standards.

- External Quality Control Reviews – *Government Auditing Standards* require that audit organizations performing audits and attestation engagements in accordance with *Government Auditing Standards* must have an external peer review, performed by reviewers independent of the audit organization being reviewed, at least once every 3 years.

OAS should make its most recent peer review report publicly available; for example, by posting the peer review report on the Internet.

10-03-30 SYSTEM OF QUALITY CONTROL

The OAS quality control system encompasses the OAS organizational structure and policies and procedures established to provide a reasonable assurance that OAS conforms with *Government Auditing Standards*. The purpose of monitoring compliance with quality control policies and procedures is to provide an evaluation of whether: (1) OAS is adhering to professional standards and legal and regulatory requirements; (2) the quality control system has been appropriately designed; and (3) quality control policies and procedures are operating effectively and complied with in practice. The OAS quality control and assurance system is comprised of six general and three review elements.

GENERAL ELEMENTS

- Leadership - The Assistant Inspectors General for Audit (AIGs) have overall responsibility for the quality of audits and the communication of policies and procedures relating to quality. (See Section 10-03-40, *Internal Quality Control Reviews*.)

- Independence, legal, and ethical requirements - In all matters relating to the audit work, OAS and the individual auditor must be free from personal, external, and organizational impairments to independence, and must avoid the appearance of such impairments of independence. (See Chapter 10-07, *Independence*.)

- Initiation, acceptance, and continuation of audit engagements - OAS will undertake audit engagements only if it can comply with professional standards and ethical principles and is acting within the legal mandate or authority of the audit organization.

- Human resources – OAS policies and procedures are designed to provide it with reasonable assurance that it has personnel with the capabilities and competence to perform its audits in accordance with professional standards and legal and regulatory requirements. (See Chapter 10-04, *Training and Professional Development*.)

- Audit performance, documentation, and reporting - The policies and procedures contained in this manual provide OAS with reasonable assurance that audits are performed and reports are issued in accordance with professional standards and legal and regulatory requirements.

- Monitoring of quality - OAS maintains an ongoing assessment of the work completed on its audits to provide reasonable assurance that the policies and procedures related to the system of quality control are suitably designed and operating effectively. (See Section 10-03-40, *Internal Quality Control Reviews* and Chapter 30-05, *Independent Report Review.*)

REVIEW ELEMENTS

- Independent report review - Independent report review is an integral part of the OAS quality control system. It is one of the methods that OAS employs to ensure the quality of reports. These reviews provide OAS with assurance that audit reports are accurate, logical, and adequately supported. (See Chapter 30-05, *Independent Report Review*.)

- Headquarters quality assurance - Under the direction of the Director for Quality Assurance and Policy, the OAS HQ Review Team routinely performs quality reviews of audit reports and audit-related correspondence for signature by headquarters. The OAS HQ Review Team ensures that these reports and correspondence are complete and consistent with OIG and OAS policies and procedures, and meet *Government Auditing Standards.* (See OAS Audit Policy Manual Section 30-02-50*, Headquarters Review.)*

- Internal quality control reviews - These reviews provide OAS with reasonable assurance that it is complying with its quality control policies and procedures. (See Section 10-03-40, *Internal Quality Control Reviews*.)

10-03-40 INTERNAL QUALITY CONTROL REVIEWS

IQCRs are performed under the direction of the appropriate AIG to ensure that elements of quality control are being applied and the overall work of OAS meets applicable standards. Key elements of the IQCR process include:

- Overseeing quality control reviews - The AIG oversees the IQCR program. The AIG monitors the design and effectiveness of the program by evaluating quality control policies and procedures. The AIG also assigns responsibilities within the program.

- Staffing the reviews - IQCRs are conducted by API staff and are managed by the Director of Audit Planning and Implementation. Personnel assigned to these reviews are experienced professionals.

- Review cycle - Each region and the Information Technology Audits Division is reviewed annually.

Coverage and conduct of the reviews - During each review cycle one or more audit standards are reviewed. Review steps are based on the *PCIE Guide for Conducting External Quality Control Reviews of the Audit Operations of Offices of Inspector General*. The specific criteria used in these reviews are communicated to the RIG and the Director of Information Technology Audits prior to the review. These reviews provide reasonable assurance that the regions and IT division are complying with OAS's policies and

procedures and *Government Auditing Standards*. At least one audit from each region is reviewed.

Reporting results of internal reviews - At the completion of all the reviews nationwide, API summarizes the results, recommends actions needed, and forwards the overall results to the DIG and the appropriate AIG s who determine what corrective actions are necessary. API follows up on recommendations during the next review cycle.

10-03-50 FMFIA INTERNAL CONTROLS REVIEWS

As part of OIG's compliance with the FMFIA, the OIG's Office of Management and Policy identifies key functions, rates the risk involved, and plans for and conducts the evaluation of these functions.

TRAINING AND PROFESSIONAL DEVELOPMENT

10-04-00 PURPOSE

This chapter establishes policies and procedures for training and professional development in OAS. The purpose of training and professional development is to continuously develop and enhance the knowledge and skills needed by OAS employees to produce quality audit products.

10-04-10 STANDARDS

The standards for training and professional development are found in Chapter 3 of the *Government Auditing Standards*. Further guidance to assist audit organizations and individual auditors in implementing these standards is found in the Government Accountability Office (GAO) issued Guidance on GAGAS Requirements for Continuing Professional Education.

The standards place responsibility on the audit organization to ensure that staff assigned to perform the audit collectively possess adequate professional competence for the tasks required. In addition, the audit organization should have quality control procedures to help ensure that auditors meet established minimum continuing professional education (CPE) requirements. The organization should maintain documentation of education and training completed.

Individual auditors are primarily responsible for improving their own competencies and meeting CPE requirements. Internal specialists who perform as part of the audit team should also comply with *Government Auditing Standards*, including the CPE requirements.

10-04-20 POLICY

It is OAS policy that all OAS audits be conducted by staff who collectively possess adequate professional competence for the tasks required.

To facilitate this, OAS should maintain an effective training program and encourage and promote professional development. All auditors should comply with the minimum CPE requirements of the *Government Auditing Standards* and compliance with these requirements should be documented in the OIG Training Information System (OTIS). While the standards prescribe minimum CPE requirements, OAS encourages training to the extent needed to develop qualified staff in a rapidly changing auditing environment.

OAS internal specialists who perform as part of the audit team (e.g., computer specialists and program analysts) should comply with *Government Auditing Standards*, including the CPE requirements. Administrative staff, audit visual specialists, writer editors, and other staff not performing as part of the audit team are not required to meet minimum CPE

requirements, but should be qualified to perform their assigned tasks and should receive training that will maintain or enhance their competency.

10-04-30 TRAINING PROGRAM

The OAS training program should continuously develop and enhance the knowledge and skills needed by OAS employees to produce quality audit products. In addition, it should help ensure that OAS audits are conducted by staff that collectively have the knowledge and skills necessary to conduct the audit and a thorough knowledge of the government environment and government auditing relative to the nature of the audit being conducted.

Qualifications for staff members conducting audits include:

- Knowledge of *Government Auditing Standards* applicable to the type of work they are assigned and the education, skills and experience to apply such knowledge to the work being performed.
- General knowledge of the environment in which the audited entity operates and the subject matter under review.
- Skills to communicate clearly and effectively, both orally and in writing.
- Skills appropriate for the work being performed (e.g., statistical sampling and information technology skills).

The appropriate AIG is responsible for providing oversight and direction of the OAS training program, including: establishing training policies and procedures, determining appropriate roles and responsibilities for training, identifying overall OAS training needs; developing cost-effective strategies for meeting OAS training needs and CPE requirements; identifying potential sources of training; and monitoring and evaluating training programs within all OAS offices. The OAS National Training Coordinator has primary responsibility for carrying out these activities on a day-to-day basis.

The AIG and RIG have primary responsibility for ensuring that the staff under their direction receive needed training and meet the minimum CPE requirements of the *Government Auditing Standards*. Each AIG and RIG will appoint a Training Coordinator at the GS-14 level to assist in carrying out these responsibilities. If deemed necessary, and with the concurrence of the appropriate AIG, the AIG and RIG may appoint the Training Coordinator at the GS-13 level. The responsibilities of Training Coordinators should include:

- Identifying the overall training and professional development needs and CPE requirements of OAS staff in their respective offices.
- Planning, coordinating, and monitoring training activities within their respective offices to meet the identified training needs and CPE requirements.
- Documenting training activities in the OTIS database.

AIGs and RIGs are responsible for providing information on training plans and activities to the AIG for AMP and the National Training Coordinator, as requested.

Individual staff members are responsible for:

- Identifying training and professional development needs.
- Seeking opportunities for training and professional development.
- Successfully completing all training and professional development activities.
- Obtaining documentation of CPE hours earned and reporting training and professional development activities to the Training Coordinator.
- Monitoring their progress toward meeting the CPE requirements.

Subject to the availability of funds, OAS will pay for approved training courses including tuition, fees, books, and required course material. Pursuant to 5 USC 4107(a) and 5 CFR 410.308, OAS will not authorize training for an employee to obtain an academic degree. However, OAS may approve academic training to develop knowledge, skills, and abilities directly related to OAS auditing on a course-by-course basis.

10-04-40 CONTINUING PROFESSIONAL EDUCATION REQUIREMENTS

All OAS auditors (GS/ES-511 series) should meet the CPE requirements of the *Government Auditing Standards*. To satisfy these CPE requirements, OAS auditors should complete, every 2 years, at least 80 hours of continuing education that directly enhances the auditor's professional proficiency to perform audits.

At least 20 hours should be completed in any 1-year of the 2-year period, and 24 of the 80 hours should be government-related education and training (i.e., government auditing, the government environment, the specific or unique environment in which the audited entity operates), as further defined in *Guidance on GAGAS Requirements for Continuing Professional Education*. Each 2-year period begins on October 1 of even numbered years.

On a case-by-case basis, the appropriate AIG may grant waivers of the CPE requirements for auditors whose responsibilities do not involve planning, directing, conducting or reporting on government audits, or who cannot fulfill the requirements for reasons such as ill health, maternity leave, or military service.

The AIG, RIG, and individual auditors have a joint responsibility for ensuring compliance with the minimum CPE requirements. Each Training Coordinator should monitor and document compliance with the CPE requirements.

The AIG and RIG will report to the appropriate AIG by October 15 of each year the status of all auditors' compliance with the CPE requirements for the previous year or 2-year period, as appropriate. If any auditor is deficient in meeting the CPE requirements, the AIG and RIG should explain the reason for the deficiency and indicate what actions will be taken to correct the deficiency. Auditors hired after the beginning of the 2-year CPE period should complete a prorated number of CPE hours. (See prorating formulas in *Guidance on GAGAS Requirements for Continuing Professional Education*.)

Any auditor who does not complete the required number of CPE hours in a 2-year period will have 2 months to make up the deficiency. CPE hours earned toward the deficiency may not be counted toward requirements for the next 2-year period. Auditors who have not satisfied the CPE requirements after the 2-month grace period should not participate

in audits done in compliance with the *Government Auditing Standards* until the CPE requirements are met.

The AIG, RIG, and Training Coordinators are authorized to determine whether specific programs qualify as CPE and the number of CPE hours to be awarded. The National Training Coordinator may be consulted in making these determinations. The criteria to be used in making these determinations include the *Guidance on GAGAS Requirements for Continuing Professional Education*.

For example, tax courses would generally not be related to audits performed under *Government Auditing Standards*, and therefore would not qualify for CPE. However, if the taxation topic relates to a specific audit objective, the audit organization should clearly document the rationale for including such training as part of the *Government Auditing Standards* CPE requirements.

The CPE levels described in this section are minimum requirements. OAS encourages training to the extent needed to continuously develop and enhance the knowledge and skills of our staff in a rapidly changing auditing environment.

10-04-50 CERTIFICATION AND PROFESSIONAL DEVELOPMENT

OAS professional staff are strongly encouraged to:

- Participate in professional activities and organizations.
- Keep abreast of current professional trends and developments.
- Pursue professional development through outside study, including obtaining advanced degrees in such areas as economics, public administration, accounting, finance, systems analysis, statistics, computer science, and business administration.
- Obtain professional certifications, such as the Certified Public Accountant (CPA), Certified Government Financial Manager (CGFM), Certified Fraud Examiner (CFE), Certified Internal Auditor (CIA), and Certified Information Systems Auditor (CISA) designations.

Certification is a mark of professional excellence and stature for auditors and OAS. The intensive study required to prepare auditors for professional examinations also enhances their knowledge and skills needed to better perform their duties.

10-04-50-01 Reimbursement for Review Courses

Subject to the availability of funds, OAS will pay for approved review courses to prepare OAS staff to take examinations required for professional certifications. Eligible costs include tuition, fees, books, and required course material. Employees will not be reimbursed for travel, transportation, or subsistence in connection with these courses. Review courses must be completed outside of normal work hours.

In order to be reimbursed for a review course an employee should:

- Have completed 3 months of current, continuous service.
- Be performing at or above the performance level of fully successful.

- Choose a review course offered by an accredited college or university, or a recognized commercial entity or professional association.

- Agree to sit for the next scheduled examination after completing the course.

Pursuant to various Comptroller General Opinions, OAS may not pay or reimburse an employee for the cost of examinations, licenses, or certifications, including travel or per diem expenses.

10-04-50-02 Administrative Leave

Administrative leave will be used to assist OAS employees in taking examinations that are required for professional certification.

Administrative leave not exceeding the length of an examination will be approved to allow an employee to sit for the examination. In addition, on the first sitting, administrative leave not exceeding twice the time scheduled for each section scheduled to be taken will be approved immediately prior to the examination for final preparation. For example, 42 hours administrative leave will be approved for an individual sitting for all four parts of the CPA examination for the first time (14 hours to sit for the examination and 28 hours study time).

Likewise, if an auditor sits for the first time for the:

- Auditing and Attestation section, the auditor would get 4 hours of administrative time to take the exam and 8 hours of administrative time to study for that section.

- Financial Accounting and Reporting section, the auditor would get 4 hours of administrative time to take the exam and 8 hours of administrative time to study for that section.

- Regulation section, the auditor would get 3 hours of administrative time to take the exam and 6 hours of administrative time to study for that section.

- Business Environment section, the auditor would get 3 hours of administrative time to take the exam and 6 hours of administrative time to study for that section.

Approval of administrative leave for preparation on subsequent sittings for the same examination will be at the discretion of the leave approving official.

10-04-60 OIG TRAINING INFORMATION SYSTEM

OTIS is a database maintained by each OAS office to monitor and document the training and professional development of OAS staff, as well as conformity by audit staff with the CPE requirements of the *Government Auditing Standards*. The Training Coordinator in each OAS office is responsible for maintaining OTIS.

CONTRACTING FOR AUDIT SERVICES

10-05-00 PURPOSE

This chapter establishes policies and procedures covering the roles of OAS staff in contracting for audit services performed by independent public accountants. This chapter does not apply to using the work of others during the conduct of a performance audit (which is discussed in Chapter 20-05, *Using the Work of Others*).

10-05-10 STANDARDS

Chapter 3 of *Government Auditing Standards* states that in all matters related to audit work, the audit organization and individual auditor, whether Government or public, must be free from personal, external, and organizational impairments to independence. When procuring audit services, organizations should assess the auditor's ability to perform the work and report the results impartially.

10-05-20 BACKGROUND AND OTHER REQUIREMENTS

OAS has responsibility for the technical monitoring of task order contracts for audit services awarded by the HHS Program Support Center (PSC), which reports to the Office of the Assistant Secretary for Administration and Management (ASAM). PSC, with input from OAS, awards competitive task order contracts for audit services.

HHS Operating Divisions (OPDIVs) may also award task orders against the audit services contracts when OAS resources are not available. Each task order must be within the scope of the basic contract and clearly describe the audit services to be performed. In addition, orders must be placed during the period of performance and the aggregate amount of all task orders must be within the maximum dollar value of the contract.

When assisting PSC with contracting for audit services, OAS is guided by the following:

- The HHS Contracting Officer's Representative Handbook for Federal Acquisition Certification, issued in July 2014 by ASFR.
- The HHS Acquisition Workforce Program Guide, issued in July 2014 by ASFR.
- A Guide to Federal Agencies' Procurement of Audit Services from Independent Public Accountants, issued in April 1991 by the Government Accountability Office (GAO).
- A Guide for Review of Independent Public Accountant Work, issued in December 1988 by GAO.

- Section 650, Using the Work of Others, of the Financial Audit Manual, issued in April 2008 by GAO.

Two roles are essential in a contract to procure audit services: a contracting officer and a contracting officer's representative (COR).

Per FAR 1.602, "contracting officers have authority to enter into, administer, or terminate contracts, and are responsible for ensuring performance of all necessary actions for effective contracting, ensuring compliance with the terms of the contract, and safeguarding the interests of the United States in its contractual relationships." Generally the contracting officer function is performed within PSC.

The main function of the COR is to ensure that contractors perform in accordance with the requirements (or terms) of the contract. The COR accomplishes this by providing support to and serving as the technical representative of the contracting officer. An OAS employee serves as the COR. Since OAS will generally transmit the report to the auditee and express negative assurance in the transmittal (see section 10-05-50-03, *Completing the Assignment*, for more information) it is important that OAS performs adequate oversight to assure that the report meets appropriate *Government Auditing Standards*.

To become a COR, an OAS employee must obtain the appropriate certification. There are three levels of certification with varying educational requirements. Additional information about these requirements can be found on the HHS intranet. Please check with the HHS OIG Acquisition Career Manager for current requirements.

In some circumstances, other OAS staff with more technical experience with, or knowledge of, the contracted audit services may assist the COR in monitoring the work being performed, such staff are referred to as task monitors. Task monitor responsibilities are shared by the OAS program division and region for OAS audit service task orders and for those requested by HHS OPDIVs. Task monitor responsibilities are also shared by the OAS program division and region for task orders requested by HHS OPDIVs.

The COR for a task order awarded by an OPDIV would be an employee of the OPDIV that awarded it.

The primary regulations governing the Federal procurement process are the Federal Acquisition Regulation (FAR) and the Health and Human Services Acquisition Regulation (HHSAR). The FAR is the primary regulation for use by all Federal agencies when supplies and services are acquired with appropriated funds. For HHS, the HHSAR supplements the FAR. It contains all formal departmental policies and procedures governing the acquisition process and explains the controlling relationships between HHS contracting officers and contractors.

10-05-30 POLICY

It is OAS policy to assist the contracting officer in the preparation of the technical aspects of the contract, and effectively monitor contractor performance for each contracted audit assignment. These duties require an active role by assigned OAS staff in both the preaward and post award phases of the contracting process. It is important that OAS take an active role throughout the contracting process consistent with the level of responsibility OAS decides to take for the contractors work as discussed in the GAO Financial Audit Manual, Section 650.09. OAS generally determines whether the contracted report is of professional quality and meets applicable *Government Auditing Standards*.

10-05-40 PREAWARD RESPONSIBILITIES

Before awarding an OAS task order for audit services, the COR provides technical support to the contracting officer in preparing the performance work statement (PWS) and Government cost estimate.

For audit services requested by an OPDIV, OAS will provide technical assistance to the requesting OPDIVs in the preparation of a PWS. Usually this will involve only the appropriate OAS headquarters division. However, OAS regional staff may be involved; for example, when work is requested by regional program staff.

OAS is responsible for approving the PWS and forwarding it to PSC's contracting office for the development and award of a task order. Since OAS task orders are usually firm fixed price, it is important to ensure that all parties agree on the PWS before it is submitted to the contracting officer.

10-05-40-01 Performance Work Statement

A PWS is type of requirements document that describes the tasks to be performed by the contractor in terms of desired outcomes or results. The contractor remains responsible for achieving the required results, based on its own proposed technical and management approach; the specific step-by-step audit approach is not dictated by OAS. The guidance at FAR 37.602 requires agencies, to the maximum extent practicable, to describe the work in terms of the required results rather than either "how" the work must be done or the number of hours to be provided, and to enable work performance to be assessed against measurable performance standards.

Although there is no standard template or outline for a PWS, the document generally covers the following elements:

ELEMENT/DESCRIPTION

General Information – Contains a broad overview of the PWS, including a description of the scope of the work and contract requirements that relate to the overall management of the contract. This element should also include the COR's information, any security requirements, or training required for contractor staff.

Definitions – Defines terms and phrases used in the PWS that are unique to the particular requirements.

Government-Furnished Property and Services – Describes any property or services that OAS will provide to the contractor for use in performing the required services, i.e. office space or use of computers.

Contractor-Furnished Items and Services – Relays to the contractor that outside of items or services specifically identified in the previous section, the contractor must furnish everything needed to perform the audit according to all contracted terms.

Specific Tasks – This is the bulk of the document. Describes each task the contractor is to perform, and cites relevant technical publications or references.

Technical Exhibits – Includes a list of deliverables or report due dates if applicable, a description of how the contractor's performance will be monitored and evaluated (i.e., it indicates whether all deliverables will be reviewed by the OAS team overseeing the contract, if comments will be provided by OAS, and the expected timeframe for the contractor to respond to the comments).

NOTES

1. For audit services requested by an OPDIV, it is important that the OPDIV staff agree on the scope.

2. Deliverables are products that the contractor will present on a specified date or timetable. An example of a deliverable is a plan implementation schedule which lists the milestone dates for the contracted audit work. Milestone dates may include the entrance conference date, field work completion date, and proposed dates that the draft and final report will be submitted to OAS.

10-05-40-02 Other Preaward Responsibilities

In addition to the PWS needed for the task order, OAS staff prepare the government cost estimate. This estimate contains the level of effort needed for each category of staff (e.g., partner, manager, and staff auditor), and the required travel and per diem costs.

OAS should furnish the contracting officer an estimated period of performance for the proposed contract. This may not be necessary if the contract period is evident from the milestone dates in the schedule of deliverables. The assigned OAS staff should advise the contracting officer to include specific contractual provisions to allow OAS to: provide technical oversight, have access to the audit documentation, and review the draft and final reports before they are finalized. In some audit procurements, it may be helpful to have the contract require that the contractor submit progress reports on the audit.

10-05-50 POST AWARD RESPONSIBILITIES

The OAS COR generally performs most of the oversight functions from contract monitoring to issuance of the contracted report. At the start of each task order assignment, the COR should discuss and clarify their respective duties with the contracting officer.

OAS is to determine the degree of responsibility it plans to take for the contractors work and ensures that the contractor completes the audit work within the time and financial requirements of the contract, and delivers a high quality report that conforms with applicable *Government Auditing Standards*. If problems arise that could affect contractual provisions in any manner, it is the duty of the COR to notify the contracting officer.

Post award responsibilities include commencing work on the contract, contract monitoring, and completing the assignment. These responsibilities are described in more detail below.

10-05-50-01 Commencing Work on the Contract

Generally, OAS and (as appropriate) OPDIV staff attend the entrance conference with the contractor and auditee. This forum can be used to explain to the auditee the relationship between the contractor and OAS. OAS should also participate in other key meetings with the contractor and the auditee.

As work on the contract progresses, it is the OAS COR's responsibility to keep the contracting officer informed of any problems that arise that could affect compliance with the terms and conditions of the contract. The COR should attempt to resolve any problems that may result in reduced work quality, missed deadlines, or increased costs to the Federal Government. To this end, OAS should provide technical direction to the contracted audit firm as necessary to ensure a quality product.

10-05-50-02 Contract Monitoring

The COR is responsible for monitoring the contractor's progress after the contract is awarded. The type, intensity, and frequency of monitoring can vary depending on the circumstances.[1] Factors to be considered when determining the extent of monitoring include: the contractor's experience with the type of audit work, the complexity of the work requirements, and OAS's previous experience with the contracted audit firm.

The two major objectives in monitoring a contract are to determine the progress made toward successful completion of the requirements, and to monitor costs of the contract as the audit work progresses. As part of this process, the OAS COR should review and approve progress billings. To accomplish this, the COR must determine that the billing request matches the progress made. If the payment schedule in the contract matches specific deliverables, such as holding the entrance conference or completing the field work, the COR should determine that these events have taken place before payment is authorized.

If payment is not tied to specific deliverables, the COR must determine the progress by other means. For example, the COR can review required technical reports to determine the status of the audit work. Additional information may also be obtained from letters, phone calls, and e-mail exchanges between the contractor and the COR. Visits to the audit site or contractor's office may be necessary to review working papers and/or monitor contractor progress. Since OAS customers will rely on any resulting report, OAS is responsible for monitoring the contract as specified under the terms of the contract.

The COR should always be clear about the limitations of their role. Contract administration is the sole responsibility of the contracting officer. The contracting officer is the only person who may modify the contract or take any actions to enter or change a contractual commitment on behalf of the Federal Government. However, the COR should immediately notify the contracting officer about any information that could affect the terms and conditions of the contract.

10-05-50-03 Completing the Assignment

As the work under the contract is near completion, the COR (and OPDIV staff if appropriate) should attend the exit conference with the contractor and the auditee. This will provide OAS some indication of how the auditee will respond to any findings and may provide some insight into the time needed to complete work under the contract.

The COR or other designated OAS staff should also review the draft report submitted by the contractor before it is sent to the auditee for comments. This review should be for technical completeness, compliance with the contract terms and conditions, and

[1] The National External Audit Resources Center (NEAR) also performs quality assurance reviews of independent public accountants, on a sample basis. OAS will rely on the NEAR reviews unless circumstances warrant closer monitoring by the region.

conformity with OAS policies and procedures. When the contractor prepares the final report, it should be reviewed in a similar fashion prior to issuance.

Consistent with the GAO Financial Audit Manual, Section 650.09, the type of reporting will depend on OAS's association with the report. The types of reporting included in the GAO Financial Audit Manual are described below:

No association with the report: If OAS assumes no association with the report, the contractor will provide the report directly to the audited entity and/or other significant users.

Association with the report expressing no assurance: If OAS choses to express no assurance on the report, it will issue a transmittal memorandum or letter without reviewing the other auditors' audit documentation. In these situations, the transmittal should be clear as to the limitations of the COR who had the responsibility to monitor the contract.

Association with the report expressing negative assurance: If OAS choses to express negative assurance it will issue a transmittal memorandum or letter indicating that the auditor reviewed the other auditors' and related audit documentation, inquired of their representatives, and found no instances where the other auditors did not comply, in all material respects, with GAGAS.

The COR must obtain express approval from the DIG if it is planned that OAS will assume no association with a report or association with a report expressing no assurance.

After the COR completes their review, OAS prepares a transmittal memorandum or letter in accordance with OAS policies[2] (Chapters 30-02, *Reporting on Results of Audits* and 30-03, *Transmitting Audit Reports*), assigns a Common Identification Number, and distributes the report. The transmittal memorandum or letter should include the following information about the OAS's role in conducting the audit:

> The review was completed under a contract with the Department of Health and Human Services, Office of Inspector General.
>
> Our monitoring review disclosed no instances in which (contractor's name) did not comply, in all material respects, with Government Auditing Standards.

The transmittal letter may also include information about OAS's technical oversight of the contractor's performance.

After the contract has been completed, the contracting officer will sometimes request information on how well the contractor performed under the contract. The COR should comply with these requests.

[2] Transmittal letters for work requested by an OPDIV or external agency are prepared on a case-by-case basis, per discussion with the respective Audit Manager, Regional Inspector General, and/or the Assistant Inspector General.

AUDIT RESOLUTION AND FOLLOW-UP

10-06-00 PURPOSE

This chapter establishes policies and procedures for the resolution of recommendations resulting from work performed by OAS, the resolution of recommendations from non-federal audits processed by the National External Audit Resource Center (NEAR), and the followup of audit recommendations as required by the Office of Management and Budget (OMB) Circular A-50.

OAS maintains information on the status of resolution of recommendations related to Federal and non-Federal reports. The resolution process begins when the results of work are reported to management, and is completed only with the receipt and acceptance of the final management decision, i.e., management's decision on the recommendations included in the final report.

10-06-10 STANDARDS

Standards for audit followup and resolution are found in The Inspector General Act of 1978 (Public Law 95-452), as amended, and OMB Circular A-50, Audit Followup.

10-06-20 POLICY

It is OAS policy to monitor the Department's resolution of OAS recommendations by:

- Maintaining a management information system to track OAS recommendations until final decisions are made on the amount of funds to be recovered, cost savings, and the actions to be taken by auditees to correct deficiencies.
- Evaluating OIG clearance documents (OCD) and ensuring that OCIG is consulted on resolutions, when appropriate.
- Performing follow-up audits and other activities on selected reports to determine whether auditees have implemented corrective measures and what steps action officials took to ensure that auditees made needed improvements.

10-06-30 THE AUDIT PROCESS

The success of audit resolution depends on the quality of the audit work and audit recommendations.

Communications with program officials, established during the planning phase and maintained throughout the audit, will assist the audit team in developing recommendations that management will agree to take action on. Recommendations that are supported by fully developed findings, and address the cause of the problem will allow the program officials to take action to resolve the cause. When possible, the audit team should develop recommendations that address the root cause and are specific.

10-06-40 THE WEB AUDIT INFORMATION MANAGEMENT SYSTEM AND OAS STEWARDSHIP REPORT

The Web Audit Information Management System (WebAIMS) provides information on various phases of OAS operations. It is maintained by the Office of Audit Planning and Implementation (API). Included in the output produced by WebAIMS is a series of lists collectively called the Stewardship Report. The Stewardship Report provides detailed information on OAS reports issued during a semiannual period, all recommendations that are outstanding as of the date of the report, and management decisions reported by operating divisions (OPDIV) during the period to resolve recommendations. Monthly Stewardship Reports are provided to the OPDIVS to track recommendations.

10-06-50 OIG CLEARANCE DOCUMENT

Management reports its decisions and actions taken on OAS recommendations on the OCD. OAS uses the OCD as the source document to clear recommendations from the Stewardship Report. An original OCD is prepared to report management decisions taken on all monetary and non-monetary OAS recommendations, including any monetary recoveries made at the time of the management decision. Management reports its concurrence or non-concurrence on each recommendation in the OCD. Note: OAS's monitoring and tracking responsibility ends with the management decision (as reported on the OCD).

10-06-60 AUDIT RESOLUTION RESPONSIBILITIES

Resolution responsibilities are shared by the OPDIVs and OIG. The OPDIVs are responsible for preparing the OCD that explains management's decisions on recommendations made in final OIG reports. For OAS reports, API ensures that the appropriate OAS official receives a copy of the OCD.

10-06-60-01 OPDIVs

The OPDIVs are required to prepare an OCD explaining management decisions on recommendations made in final OAS reports. The OPDIV's audit liaison official at the appropriate headquarters or regional level is responsible for ensuring that all OCDs contain the proper information and are properly distributed, including to the appropriate Finance Officer, when applicable.

Additional information about the OPDIV's specific responsibilities for resolution of OIG recommendations is contained in Chapter 1-105, *Resolution of Audit Findings*, of the HHS Grants Administration Manual; Chapter 8-30, *Conflict Resolution Mechanism for Inspector General Reports*, of the HHS General Administration Manual; Grants Policy Directive 4.01, Part 4, Section 01, *Audits*; *Grants Policy Directive 4.02, Part 4, Section 2, Debt Collection and Closeout;* and Chapter 10-41, *Credit and Debt Management*, of the Departmental Accounting Manual.

10-06-60-02 Audit Planning and Implementation

The OPDIVs submit OCDs to API. API evaluates the actions shown by OPDIVs on the OCDs to determine if the actions are fully responsive to the recommendations in WebAIMS. If API cannot determine if an action is appropriate, input from OAS headquarters and regional offices having responsibility for the recommendations will be obtained. When necessary, API will obtain further information from the OPDIV. All nonconcurrences over $100,000 are sent to the appropriate OAS Division and/or regional office for comment. API maintains electronic files of OCDs and ensures that the appropriate OAS official receives a copy of the OCD upon request.

If the OCD is accepted, API will clear the recommendations in WebAIMS. If the OCD is not accepted, API will return it to the OPDIV's audit liaison and cite the reason the OCD cannot be accepted. API is responsible for maintaining WebAIMS and processing OCDs timely. Since prompt resolution of audit recommendations is crucial to the Department's stewardship responsibility, API will notify the DIG of any delays in submission of OCDs.

10-06-60-03 Assistant and Regional Inspectors General for Audit Services

The AIG or the RIG is responsible for ensuring that annotated copies of all OAS reports are provided to the audit liaison, action official(s), and API. Annotated audit reports include the corresponding recommendation codes that have been entered into WebAIMS by the region or division issuing the report. Chapter 30-04, *Distribution of HHS - Produced Audit Reports*, subsection 30-04-110 provides guidance for annotating audit reports. Additional guidance can be found in the policy memo Guidance on using action codes when coding audit recommendations. Annotated reports are used by the audit liaisons and action officials to match the recommendations in the report to the monthly OAS Stewardship Report and by API to clear recommendations.

10-06-70 AMENDMENTS AND APPEALS

Management decisions and actions reported on OCDs are generally final. However, cases arise in which an auditee appeals a decision by an OPDIV and an administrative appeal is granted. When this occurs and the appeal decision changes what the OPDIV reported in the original OCD, the OPDIV is required to submit an amended OCD for those items that have been changed. The amended OCD should state the change and how it affects the original OCD.

The Departmental Appeals Board (DAB), or other such office responsible for rendering a decision on an appeal, will notify the appropriate audit liaison office of its decision. The audit liaison must, in turn, notify the appropriate finance office and OIG when an appeal is completed and a decision rendered. A copy of the decision should be attached to the amended OCD.

On occasion, an auditee may appeal a DAB decision which may result in further amendments to the OCD. In addition, original management decisions may be amended for reasons other than a DAB decision. In those instances, an amended OCD is also required.

10-06-80 FOLLOW-UP PROCEDURES

Follow-up audits allow OAS to determine, for selected audits, whether:

- Recommended actions were implemented or are in the process of being implemented.
- Actions have led to, or will lead to, resolution of the problem.
- The OPDIV's procedures for completing final action on audit reports meet requirements.
- The OPDIV's documentation of final action taken in response to OAS recommendations is adequate and properly reported to the Department's follow-up official and, when applicable, included in the Department's semiannual report to Congress.

10-06-80-01 Audit Planning and Implementation

API is responsible for developing and implementing audit follow-up procedures within OAS. API monitors the status of OAS recommendations to the point of management decision. After the OPDIV makes the management decision for stewardship reporting purposes, API, in consultation with the appropriate AIG and RIG, will recommend certain reports for follow-up. The selection is made principally from reports with significant findings where the OPDIV has accepted OAS recommendations. On occasion, API may select a GAO report for follow-up.

The Assistant Secretary for Financial Resources (ASFR) is the Department's follow-up official, as designated under OMB Circular A-50. As the audit follow-up official, ASFR ensures that systems of audit follow-up are documented and in place, that timely responses are made to all audit reports, and disagreements are resolved. API solicits input from ASFR before selecting reports for followup, as well as from the AIG and RIG. API will specify the number and approve selections of follow-up audits for each division and region.

10-06-90 REPORTING

Follow-up audit reports will be prepared and distributed in accordance with OAS Policy. Chapter 30-02, *Reporting on Results of Audits,* and Chapter 30-04, *Distribution of HHS Produced Audit Reports,* provide OAS policy on preparing and distributing audit reports.

OAS may issue a report for each follow-up audit performed or a single, consolidated report on several follow-up audits of the same OPDIV, if the action official is the same.

The report should include a statement that the objective of the audit was to follow up on findings and recommendations identified in a previous audit. Additionally, the report will generally include a summary of each finding and recommendation in the original report, the auditee's position and the OPDIV's position (if the OPDIV is not the auditee), the actions taken, and the current status at the time of the follow-up audit.

Generally, follow-up reports will not be as lengthy or detailed as the original report. However, the reader of the report should be able to obtain a complete understanding of the issues presented from the follow-up report.

10-06-100 CONFLICT RESOLUTION PROCESS FOR OIG REPORTS

The conflict resolution process used to settle disagreements between an OPDIV and OIG over an OIG report begins on the date the report is issued and ends no later than 6 months after the issue date, as prescribed in OMB Circular A-50, Audit Followup. The process is intended to encourage settlement at the lowest organizational level, nearest the program in question, but allows for escalation of the conflict through the ASFR to the Deputy Secretary, if necessary. The Deputy Secretary makes the final decision.

The DIG, after consulting with the appropriate AIG/RIG, will initiate the conflict resolution process on behalf of OAS.

The conflict resolution process is described at Chapter 8-30, *Conflict Resolution Mechanism for Inspector General Reports*, of the HHS General Administration Manual.

INDEPENDENCE

10-07-00 PURPOSE

This chapter establishes OAS policies and procedures relative to independence. If OAS and its employees are to be effective, they must be independent so that their opinions, findings, conclusions, judgments, and recommendations will be impartial, and viewed as impartial by reasonable and informed third parties.

10-07-10 STANDARDS

Chapter 3 of the *Government Auditing Standards* contains the standard for independence. This standard places responsibility on each auditor and the audit organization to maintain independence. In all matters relating to the audit work, the audit organization and the individual auditors, whether government or public, must be independent.

10-07-20 POLICY

It is OAS policy that OAS and the individual auditors participating on an audit assignment maintain independence so their opinions, findings, conclusions, judgments, and recommendations will be impartial and will be viewed as impartial by reasonable and informed third parties. Auditors should avoid situations that could lead reasonable and informed third parties to conclude that the auditors are not independent and, thus, are not capable of exercising objective and impartial judgment on all issues associated with conducting the audit and reporting on the work.

It is OAS policy that auditors must consider not only the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, but also whether there are any circumstances that would cause a reasonable and informed third party, having knowledge of relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of OAS or a member of the audit team had been compromised. All situations deserve consideration because it is essential not only that auditors are independent and impartial, but also that reasonable and informed third parties consider them so.

Except during the performance of nonaudit services, auditors should be independent from the audited entity during any period of time that falls within the period covered by the subject matter of the audit and during the period of the audit, which is from the start of the planning phase of the audit to the date the final report is issued.

10-07-30 CONCEPTUAL FRAMEWORK APPROACH TO INDEPENDENCE

Government Auditing Standards establishes a conceptual framework that auditors use to identify, evaluate, and apply safeguards to address threats to independence.

10-07-30-01 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, and on specific safeguards applied to eliminate the threat or reduce it to an acceptable level. 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. OAS auditors should evaluate the following broad categories of threats to independence when threats are being identified and evaluated:

- Self-Interest Threat – The threat that that a financial or other interest will inappropriately influence an auditor's judgment or behavior.

- 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 the audit.

- 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.

- 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.

- Undue Influence Threat – The threat that external influences or pressures will impact an auditor's ability to make independent and objective judgments.

- 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 the audit.

- 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.

All OAS team members, including specialists, who are in any way involved in an audit must be free from threats to independence. Members of the audit team are responsible for notifying their supervisor if they have any threats to independence. Supervisors are responsible for taking appropriate corrective action when team members have threats to independence relating to an audit assignment.

When a threat to independence is identified prior to or during the audit, the threat needs to be resolved in a timely manner. When the threat to independence is applicable only to an individual auditor on a particular audit, the supervisor may be able to eliminate the threat. The supervisor should discuss the threat to independence with the auditor and ways to eliminate it. If the threat to independence cannot be eliminated, the auditor should be removed from the audit assignment.

If a threat to independence is identified after the audit report is issued, OAS should evaluate the threat's impact on the audit and on compliance with *Government Auditing Standards*. If OAS determines that the newly identified threat had an impact on the audit that would have resulted in the audit report being different from the report issued had the auditors been aware of it, it 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 audts, and other known users, so that they do not continue to rely on the findings or conclusions that were impacted by the threat to independence. If the report was posted to the HHS OIG website, OAS should remove the report and post a public notification that the report was removed. OAS 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 of findings or conclusions.

All non-administrative employees will certify their independence on *Annual Independence Certification Form.* They should complete this certification before the start of each FY and should provide a copy to their supervisor. New employees should complete the form within two weeks of starting employment with OAS.

10-07-30-02 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 following are examples of safeguards that may be effective under certain circumstances:

- Consulting an independent third party, such as a professional organization, a professional regulatory body, or another auditor.
- Involving another audit organization to perform or reperform part of the audit.
- Having a professional staff member who was not a member of the audit team review the work performed.
- Removing an individual from an audit team when that individual's financial or other interests or relationships pose a threat to independence.

OAS team members 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. Team members should evaluate threats both individually and in aggregate because threats can have a cumulative effect on an auditor's independence. Members of the audit team 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.

In cases where threats to independence are not at an acceptable level, thereby requiring the application of safeguards, OAS team members 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, OAS should decline to perform a prospective audit or terminate the audit in progress.

Threats to independence should be disclosed in accordance with Chapter 30-02, *Reporting on Results of Audits*, Section 30-02-50-11, *Objectives, Scope, and Methodology*.

10-07-30-03 OIG Independence

The Inspector General Act of 1978 (Public Law 95-452), as amended (the Act), established the Offices of Inspector General as independent and objective units. The Act provides for an IG at each agency who shall generally be appointed by the President, by and with the advice and consent of the Senate, without regard to political affiliation, and solely on the basis of integrity and ability. The HHS IG is appointed by the President and reports to and is under the general supervision of the Secretary of HHS.

The Secretary shall not prevent or prohibit the IG from initiating, carrying out, or completing any audit or investigation. The purpose of the Act is to:

- Require the OIG to conduct and supervise audits and investigations relating to programs and operations.
- Promote economy, efficiency, and effectiveness and prevent and detect fraud and abuse in those programs and operations.
- Provide a means for keeping the Secretary of HHS and the Congress fully and currently informed about problems and deficiencies, necessity for, and progress of corrective action.

The Act gives the IG independence by providing for direct reporting to Congress and protection against removal. Within HHS, the Secretary cannot remove the IG. The IG may only be removed from the office by the President, who shall communicate the reasons for any such removal to both Houses of Congress. Moreover, the Act provides IGs with strong independent authority to obtain information through subpoenas and other means. The Act further requires IGs to inform the Attorney General of suspected violations of Federal criminal law, thereby eliminating the ability of agency officials to prevent or delay furnishing such information.

10-07-40 NONAUDIT SERVICES

OAS may at times provide professional services, other than audits, which are sometimes referred to as nonaudit services or consulting services. Providing such nonaudit services may create threats to OAS's independence.

Before OAS agrees to perform a nonaudit service to an audited entity, OAS should determine whether providing such a service would create a threat to independence, either by itself or in aggregate with other nonaudit services performed, with respect to any

audit it performs. A critical component of this determination is consideration of management's ability to effectively oversee the nonaudit service to be performed. OAS should document consideration of management's ability to effectively oversee nonaudit services to be performed.

OAS may be required to perform a nonaudit service that could impair its independence with respect to a required audit. If OAS cannot, as a consequence of constitutional or statutory requirements over which the auditor has no control. implement safeguards to reduce the resulting threat to an acceptable level, or decline to perform or terminate the nonaudit service that is incompatible with audit responsibilities, OAS should disclose the nature of the threat that could not be eliminated or reduced to an acceptable level and modify the GAGAS compliance statement accordingly.

OAS may be able to provide nonaudit services without impairing independence if (1) the nonaudit services are not expressly prohibited, (2) OAS has determined that the requirements for performing nonaudit services have been met, and (3) any significant threats to independence have been eliminated or reduced to an acceptable level through the application of safeguards. For performance audits and agreed-upon procedures engagements, nonaudit services that are otherwise prohibited by *Government Auditing Standards* may be provided when such services do not relate to the specific subject matter of the of the engagement. For financial statement audits and examination or review engagements, a nonaudit service performed during the period covered by the financial statements may not impair an auditor's independence with respect to those financial statements provided that the following conditions exist: the nonaudit service was provided prior to the period of the professional engagement; the nonaudit service related only to periods prior to the period covered by the financial statements; and the financial statements for the period to which the nonaudit service did relate were audited by another auditor.

10-07-50 DISCLOSURES

OAS staff are required to submit disclosure statements (HHS Form 520 Request for Approval of Outside Activities) regarding their outside activities and certain employees must also submit confidential financial disclosure statements (OGE Form 450 Confidential Financial Disclosure Report). These requirements assist in establishing whether an employee has a threat to independence.

The Standards of Ethical Conduct for Employees of the Executive Branch, issued by the U.S. Office of Government Ethics (OGE), provide general principles that apply to every Government employee. These principles address:

- Gifts from outside sources.
- Gifts between employees.
- Conflicting financial interests.
- Impartiality in performing official duties.
- Seeking other employment.
- Misuse of position.
- Outside activities.

HHS has issued supplemental standards that provide additional guidance to its employees. Both the OGE standards and HHS supplemental standards can be accessed at the OGE website.

Although restrictions exist, OAS staff generally may obtain outside employment that does not conflict with their government duties. All OAS staff are required to submit HHS Form

520, Request for Approval of Outside Activity, prior to participating, either for compensation or as a volunteer, in the following non-official duty activities:

- Providing consulting or professional services.
- Teaching, speaking, writing, or editing that relates to the employee's official duties.
- Serving as an officer, director, or board member of a nonfederal entity or as a member of an advisory board or commission (unless the service is provided without compensation to a political, religious, social, fraternal, or recreational organization and the position held does not require the provision of professional services). Therefore, approval is not required for such unpaid positions as serving on the board of a condominium association and serving as an officer of a parent teacher association.

OAS staff who use HHS Form 520 to apply for approval of their outside activities must receive a copy of a notice explaining the standards of conduct regarding outside employment and activities and cautioning employees that: "Approval of an HHS Form 520 does not release you from a continuing legal obligation to disqualify yourself from official assignments affecting your outside employer." OIG staff must submit their completed HHS Form 520 to their supervisor, who serves as the recommending official. Final approval is made by the respective AIG or RIG. OAS staff should not participate in the outside activity until final approval has been granted. The OIG requirements for the submission of HHS Form 520 are contained in Chapter 3-05 of the OIG Administrative Manual.

Additional disclosure requirements are mandated for GS-14 and GS-15 staff. The policy on confidential financial disclosure reporting is contained in Chapter 3-20 of the OIG Administrative Manual. It requires employees to submit OGE Form 450, Confidential Financial Disclosure Report, on an annual basis. This form is available in electronic format at the OGE website.

In addition, Chapter 7-00 of the OIG Administrative Manual contains policies relating to requests for staff to speak to outside groups as part of their official duties.

10-07-60 INDEPENDENCE OF OTHER GOVERNMENT AUDITORS

In the course of performing its work, the audit team may want to use the work of other government auditors. To determine if the team can use the work of other government auditors, the team must consider the independence of the government audit organization.[1]

A government audit organization's ability to perform the work and report the results impartially can be affected by its place within government and the structure of the government entity that the audit organization is assigned to audit. OAS will determine if an audit organization is free from organizational impairments to independence whether reporting internally to management within the audited entity, or externally to third parties outside the audited entity.

[1] This is one of the factors that should be considered. Other factors to consider are discussed in Chapter 20-05, *Using the Work of Others*.

Reporting Internally

A Federal, state, or local government audit organization, or an audit organization within another government entity, such as a public college, university, or hospital, may be subject to administrative direction from persons involved in the government management process. Under these circumstances, the audit organization may be required to report internally to management. In accordance with *Government Auditing Standards*, internal auditors who work under the direction of the audited entity's management are considered independent for the purposes of reporting internally if the head of the audit organization meets all of the following criteria:

- Accountable to the head or deputy head of the government entity or to those charged with governance.
- Reports the audit results to the head or deputy head of the government entity and to those charged with governance.
- Located organizationally outside the staff or line-management function of the unit under audit.
- Has access to those charged with governance.
- Sufficiently removed from political pressures to conduct audits and report findings, opinions, and conclusions objectively without fear of political reprisal.

The audit organization's independence is enhanced when it also reports regularly to the entity's independent audit committee and/or to the appropriate government oversight body.

Auditors should also be sufficiently removed from political pressures to ensure that they can conduct their audits objectively and report their findings, opinions, and conclusions objectively without fear of political repercussion. Whenever feasible, auditors should be under a personnel system in which compensation, training, job tenure, and advancement are based on merit.

Reporting Externally

When reporting externally, audit organizations that are structurally located within government entitites are often subject to constitutional or statutory safeguards that mitigate the effects of structural threats to independence. For external audit organizations, such safeguards may include government structures under which a government audit organization is:

- At a level of government other than the one of which the audited entity is part, for example federal auditors auditing a State government program.
- Placed within a different branch of government from that of the audited entity, for example, legislative auditors auditing an executive branch program.

Safeguards other than those described above may mitigate threats resulting from governmental structures. For external auditors or auditors who report both externally and internally, structural threats may be mitigated if the head of an audit organization meets any of the following criteria in accordance with constitutional or statutory requirements:

- Directly elected by voters of the jurisdiction being audited.

- Elected or appointed by a legislative body, subject to removal by a legislative body, and reports the results of audits to and is accountable to a legislative body.

- Appointed by someone other than a legislative body, so long as the appointment is confirmed by a legislative body and removal from the position is subject to oversight or approval by a legislative body, and reports the results of audits to and is accountable to a legislative body.

- Appointed by, accountable to, reports to, and can only be removed by a statutorily created governing body, the majority of whose members are independently elected or appointed and outside the organization being audited.

OAS auditors considering independence issues should refer to Chapter 3 of the *Government Auditing Standards* for detailed guidance.

Part II

Auditing Chapters

PLANNING AUDIT ASSIGNMENTS

20-01-00 PURPOSE

This chapter establishes policies and procedures for planning audit assignments. Careful planning of each audit assignment is essential.

20-01-10 STANDARDS

The standards for planning audits are found in Chapters 4 and 6 of the *Government Auditing Standards*. Government Auditing Standards require that auditors plan the audit to reduce audit risk to an appropriate level for the auditors to provide reasonable assurance that the evidence is sufficient and appropriate to support the auditors' findings and conclusions. Chapter 6 provides extensive guidance for planning performance audits.

20-01-20 POLICY

It is OAS policy for auditors to use professional judgment to plan each audit assignment. Specifically, for each audit the team should:

- Prepare sufficient audit documentation, including an audit plan, to enable an experienced auditor[1] having no previous connection to the audit to understand from the audit documentation that the audit has been adequately planned and documented.
- Use a teamwork approach to plan audits.
- Conduct a team meeting when planning the audit to establish and agree upon a manageable number of clear audit objectives that can be completed in a timely fashion.
- Prepare a TeamMate Current Issue, also known as an Objective Attributes Recap Sheet (OARS) for each audit objective. One of the primary purposes of the TeamMate Current Issue is to focus the audit team on the attributes needed to accomplish each audit objective during planning and each subsequent phase of the audit. Because most special audits, as discussed in Chapter 20-04, Special Audits, are low-risk and the audit results are needed in a short time frame, use of TeamMate Current Issues is optional..

[1] An experienced auditor means an individual who possesses the competencies and skills that would have enabled him or her to perform the performance audit. These competencies and skills include an understanding of (a) the performance audit processes (b) GAGAS and applicable legal and regulatory requirements, (c) the subject matter associated with achieving the audit objectives, and (d) issues related to the audited entity's environment.

20-01-30 THE AUDIT PROCESS

The Audit Process handbook discusses the four phases of an audit. The first phase, planning, focuses on all the activities needed to produce the ultimate product, the audit report. Although planning is done throughout the assignment, it is most concentrated in the planning phase of the audit process.

20-01-30-01 Selection of an Assignment

The OIG publishes an annual work plan that details the specific assignments that it expects to undertake. These assignments come from a variety of sources including: leads developed from current assignments, effort spent on work plan budgeted research and development projects, and requests from program officials or members of Congress. Assignments are selected for the work plan based upon significance and a risk assessment of the Department's program activities and functions. In considering significance and risk some of the factors are:

- Statutory and regulatory requirements.
- The vulnerability to fraud and abuse within a program based upon an assessment of internal control, management information systems, and the risk of financial gain by program users, beneficiaries, providers, contractors, grantees, or others.
- The needs of users including management, governmental officials, the Congress and others who have an ability to influence the conduct of the program. An awareness of these needs can help the audit team understand the way a program operates the way it does.
- Newness, visibility, or sensitivity for the organization, program activity or function.
- Current and potential dollar magnitude.
- Extent of Federal participation in terms of resources or regulatory authority.
- The results of past and current oversight activities from within and outside the OIG.
- The availability of resources.

OAS collaborates with other OIG components to ensure effective, non-duplicative coverage of the Department's programs and activities in the development of the OIG Work Plan.

Assignment planning should ensure that the factors that resulted in the selection of the issue in the work plan are adequately covered by the scope of the audit. The determination that the specific assignment being planned is the best use of audit resources is generally made in the initial phases of the audit process.

20-01-30-02 Phase I - Planning

After a decision is made to commit audit resources to an issue or concern, initial team discussions are conducted to convert issues described in the OIG Work Plan into clear audit objectives.

An initial meeting of team members should be held either in person or by use of electronic media. As the team makes preliminary decisions on audit objectives, each

objective should be recorded on a separate TeamMate Current Issue. The TeamMate Current Issue should be modified and updated as objectives are refined and attributes developed throughout the audit. All planning efforts should focus on the final product - the audit report.

At this meeting, team members should discuss and make preliminary decisions about scope and methodology with the understanding that these decisions can be refined and modified throughout the audit.

The scope is the boundary of the audit and is directly tied to the audit objectives. The scope of the audit can be defined by the program, or an aspect of a program to be audited, the period of time reviewed and/or the locations that will be included.

The methodology is the audit procedures performed to accomplish the audit objectives. The audit team should design the methodology to obtain sufficient, appropriate evidence to address the audit objectives, reduce audit risk to an acceptable level, and provide reasonable assurance that the evidence is sufficient and appropriate to support the auditors' findings and conclusions.

In addition to establishing the audit objective(s), scope and methodology, the audit team should assess audit risk and significance within the context of the audit objective by focusing on the following:

- Obtaining an understanding of the program to be audited and the needs of potential users of the audit report.
- Identifying the criteria needed to evaluate matters subject to audit.
- Obtaining an understanding of internal controls related to the scope and objective(s) of the audit.
- Assessing and discussing the risks of fraud, including factors such as incentives or pressures to commit fraud, the opportunity for fraud to occur and the rationalizations or attitudes that could allow individuals to commit fraud.
- Identifying the potential sources of data that could be used as audit evidence.
- Considering the results of previous audits and attestation engagements that could affect the planned audit objectives.
- Considering whether the work of other auditors and/or specialists may be used to satisfy some of the audit objectives.
- Providing appropriate and sufficient staff and other resources to perform the audit in a timely manner.
- Communicating general information concerning the planning and performance of the audit to management officials responsible for the program being audited, those charged with governance and others as applicable.
- Preparing an audit plan.

Additional information on these items is contained in Chapter 6 of *Government Auditing Standards*.

20-01-40 PLANNING CONSIDERATIONS

Four items of particular importance in planning an audit are discussed below.

20-01-40-01 Understanding the Program

The audit team should gain an understanding of the program. To accomplish this, the audit team should review and identify the criteria to be used in the audit. Criteria are generally set forth in laws, regulations, guidelines and/or State plans.

At this time, the audit team generally should obtain the advice of OCIG. If the criteria are conflicting or unclear, the audit team must seek guidance from the OCIG at the earliest point in the audit process. During the planning phase the criteria should be written on each TeamMate Current Issue.

Knowledge of the laws, regulations and guidelines under which a program operates is an excellent starting point to understanding how the program is supposed to work. In addition, in determining audit objectives, knowledge of a program's purpose and goals, efforts, operations, outputs and outcomes is very useful.

The purpose of a program is the legislative result that is intended or desired and is not always expressly stated. Goals quantify the level of performance intended or desired and are generally set by management. Efforts are the amount of money, materials, personnel and other resources that are put into a program. Outputs are the quantity of goods and/or services provided by a program. Outcomes are accomplishments or results that occur, to some extent, because of the services provided. Although complete knowledge of all of these items may not be necessary for all audits, an audit team that has a good understanding of these aspects of a particular program will more likely have clear, understandable and achievable audit objectives.

To increase its understanding of the program, the audit team should meet or confer with the appropriate program officials. This meeting can help the audit team gain a better understanding of how the program actually operates. In addition, program officials can sometimes provide insight on recent changes to the program criteria. Program officials may be familiar with the auditee and have information as to how the program is implemented by other auditees.

20-01-40-02 Written Audit Plan

Each audit performed by OAS must include a written audit plan. A written audit plan includes, but is not limited to, an audit program and documentation about the key decisions that the audit team makes on audit scope, methodology and objectives.

The contents of the written audit plan should be contained in one document and should be updated to include any significant changes.

Chapter 6 of *Government Auditing Standards* and Chapter 20-06-80 provide additional guidance on the contents of written audit plans.

20-01-40-03 Audit Risk

Audit risk is the possibility that an audit teams' findings, conclusions, recommendations, or assurance may be improper or incomplete, as a result of factors such as evidence that is not sufficient and/or appropriate, an inadequate audit process, or intentional omissions or misleading information due to misrepresentation or fraud.

The assessment of audit risk involves both qualitative and quantitative considerations. Factors such as the time frames, complexity, or sensitivity of the work; size of the program in terms of dollar amounts and number of citizens served; adequacy of the audited entity's systems and processes to detect inconsistencies, significant errors, or fraud; and auditors' access to records, also impact audit risk. Audit risk includes the risk that the audit team will not detect a mistake, inconsistency, significant error, or fraud in the evidence supporting the audit.

Audit risk can be reduced by taking actions such as increasing the scope of work; adding specialists, additional reviewers, and other resources to the audit team; changing the methodology to obtain additional evidence, higher quality evidence, or alternative forms of corroborating evidence; or aligning the findings and conclusions to reflect the evidence obtained.

20-01-40-04 Requesting OI Clearance

When starting audits, auditors should request OI clearance to ensure that the auditee is not under OI investigation. Auditors should send their clearance requests through the OAS liaison within the applicable OAS Division. All clearance requests will be coordinated through OI headquarters. The process for requesting OI clearance is available on the OAS Intranet.

OI clearance is not required for audits of State agencies or reimbursable audits. However, if an audit of a State agency involves the review of a specific provider, the audit team should obtain OI clearance for that provider.

20-01-50 AUDIT START NOTICES

Audit start notices, addressed to the audit liaison of the OPDIV and signed by the appropriate AIG, should be prepared for all new assignments that will have reports addressed to OPDIV headquarters officials. In addition to notifying the OPDIV, the notice will be distributed to other components within the OIG (OI, OEI, OCIG, and OMP), and to the OAS DIG, AIGs, and RIGs.

The audit start notice should help minimize duplication of effort when more than one OIG component is looking at the same general area. Audit start notices should be sent out during the planning phase of the audit. If significant on-site fieldwork is contemplated during the planning phase, the audit start notice should precede that on-site fieldwork.

The RIG of a lead region should submit an audit start notice addressed to the OPDIV head to the appropriate AIG before starting an assignment. The AIG should prepare audit start notices for assignments conducted solely by headquarters staff. The AIG, as signatory of all audit start notices, should distribute copies within OIG as well as to appropriate OPDIV officials.

The audit start notice should contain a brief description of the assignment and a brief statement of the audit objective(s). The participating regions and division should also be identified. Sufficient background and general description of the work should be provided

in order to be understood by a reader not familiar with the program or auditee(s). The audit start notice should identify the audit sites, the method for securely transmitting audit information to OAS over the Internet, the regional and divisional audit managers, and their phone numbers and email addresses.

The audit start notice should be maintained in the TeamMate file.

A template for preparing audit start notice is available on OAS's Intranet.

20-01-60 AUDIT NOTIFICATION LETTERS

The RIG/AIG should send an audit notification letter to an auditee before starting an assignment to confirm audit arrangements. The letter serves as the official notification to the auditee of our intention to perform an audit of its organization. The letter briefly describes the audit objective(s), identifies the individuals within OAS and the auditee organization that made the arrangements, and the method for securely transmitting audit information to OAS over the Internet. The letter describes the OIG's authority for performing the audit. The letter also identifies the audit manager and senior auditor assigned to the audit and includes their phone numbers and email addresses. This letter can also be used to request specific documentation or information that will be needed for the audit. Examples of audit notifications letters can be found on the OIG Intranet.

The audit notification letter should be maintained in the TeamMate file.

Templates for preparing audit notification letters are available on OAS's Intranet.

STATISTICAL SAMPLING AND MATHEMATICAL CALCULATION ESTIMATION TECHNIQUES IN AUDITING

20-02-00 PURPOSE

This chapter establishes OAS policies and procedures on estimation techniques for statistical sampling and mathematical calculation which uses existing information or data that does not involve OAS sampling.

20-02-10 STANDARDS

Chapter 6 and Appendix I of *Government Auditing Standards* discuss the use of sampling to obtain sufficient, appropriate evidence. Chapter 7 discusses reporting requirements when sampling significantly supports the audit findings, conclusions, or recommendations.

20-02-20 POLICY

It is OAS policy that estimates used in audit reports are either derived from statistical sampling results or from mathematical calculations that do not involve OAS sampling, such as analysis of existing information or data.

Statistical sampling, or probability sampling is the process of examining or measuring a smaller group of items, called a sample, to make estimates about a larger group of items, called a sampling frame. It involves selecting the sample based on the theory of probability. At any stage in selecting the sample units, the probability of selecting any set of sample units should be known. Statistical sampling is the only general method known that can provide a measure of precision of the estimate.

It is OAS policy that auditors use the statistical estimators that follow:

- For monetary recovery, use the difference estimator and recommend recovery at the lower limit of the 90 percent two-sided confidence interval. The difference estimator uses the difference between the value the auditor determined for the sample unit and the corresponding amount appearing in the auditee's records to estimate the difference amount for the sampling frame.

- For estimates other than for monetary recovery, such as Funds Put To Better Use (FPBU), use the appropriate estimator; and report the point estimate.

- For rate-setting audits, use the appropriate estimator and recommend the point estimate.

- For audits where the point estimate is included in the body of the report and is materially different from the lower limit, report the lower limit alongside the point estimate. Auditors should use their professional judgmental when assessing the materiality of the difference.

Statistical sampling is discussed in sections 20-02-50, *Statistical Sampling*, 20-02-60,*Stratified Random Sampling*, 20-02-70, and *Multistage Sampling*.

This list of methods presented within this chapter is not exhaustive. Alternate methods may be applied given a policy waiver as discussed in section 20-02-110.

It is OAS policy that, depending on the objectives of the audit, it may be appropriate to develop estimates that are derived from mathematical calculations that do not involve statistical sampling. These estimates are discussed in section 20-02-90, *Estimates Involving Mathematical Calculations*.

It is OAS policy that, depending on the objectives of the audit, it may be appropriate to use statistical sampling for purposes other than estimation(e.g., to evaluate internal controls) if the OAS statistician is consulted during development of the sample plan.

Judgmental sampling (also referred to as nonstatistical sampling) is the selection of a sample by a method not based on the theory of probability. It is OAS policy that estimates must not be made from a sample that was not selected statistically. The use and limitations of judgmental sampling are discussed in sections 20-02-100, *Judgmental Sampling*.

20-02-30 THE AUDIT PROCESS

Below are the estimation activities involving statistical sampling and the use of mathematical calculations that take place in each of the four phases of the audit process.

20-02-30-01 Phase 1 - Planning

In Phase 1 of the audit process, preliminary decisions are made about audit objectives, scope, and methodology, and the appropriate criteria are developed.

During this phase, a decision should be made whether an estimate might be used in the audit. If so, the designated regional or divisional statistical specialist should be included on the team as a technical consultant. Preliminary decisions can be made about the estimates, and the preliminary audit objective can be agreed upon. The criteria developed in this phase are used in developing the *Characteristics to Be Measured* section of the sampling plan.

20-02-30-02 Phase 2 - Survey

For estimation purposes, Phase 2 is probably the most critical phase of the audit. The necessary steps are performed in this phase to enable the audit team to make decisions concerning the nature, timing and extent of detailed audit work, including the development of estimates.

During this phase, the statistical sampling or mathematical calculation plan should be completed by the audit team, in consultation with the statistical specialist. These plans

should be developed along with the audit program, and should be approved before data collection and analysis begins. The audit manager and the statistical specialist should sign the plan for the audit team. If the plan is for a multi-region audit for which another region is the lead region, the lead region audit manager should also sign the plan.

Plans should be forwarded for approval by the OAS statistician:

- If the report is expected to be signed by the IG, DIG, or AIG (if there is any question about the signature level, the plan should be forwarded to the OAS statistician for approval).
- If the plan is part of a multi-region audit.
- If the plan uses discovery sampling.

Depending upon the audit circumstances, a plan connected with a RIG-signed report may be sent to the OAS statistician for technical assistance and/or approval.

Approved plans should be documented in the TeamMate file.

20-02-30-03 Phase 3 - Data Collection and Analysis

During Phase 3, the statistical sample is selected, reviewed, and analyzed. In addition, estimates based on existing information or data that does not involve OAS sampling are calculated. Significant modifications to the plan should be documented and the modified plan should be signed as discussed in the prior section.

If, in the review of the sample during the data collection and analysis phase, the audit team determines that the report will meet the threshold for IG, DIG or AIG signature, the team must notify the statistical specialist and forward the plan to the OAS statistician immediately. Plans should not be sent to the statistician for first the time during the drafting of the report.

The statistical specialist should be involved in the selection of random numbers, and in the interpretation of the statistical sample estimate or the mathematical calculation estimate.

20-02-30-04 Phase 4 - Reporting

During Phase 4, the statistical specialist should examine and approve the manner in which estimates have been developed and presented in the report. See Chapter 30-05, *Independent Report Review*, Section 30-05-40, *Independent Report Reviewer's Responsibilities*.

The manner in which the estimates are presented in the report depends on the nature and objective of the audit. See Section 20-02-30-04B, *Reports*.

20-02-30-04-A Audit Documentation

The audit documentation supporting reported estimates should contain enough detail so the sample selection, results, and estimates, or the mathematical calculations, results, and estimates can be reconstructed. At a minimum, the following should be included:

- Approved sampling or mathematical calculation plan and approved modifications.

- For statistical samples, documentation of the output from OAS Statistical Software - Random Number Generators, and output from OAS Statistical Software and copies of the data files processed by the programs.

- For estimates that are derived from mathematical calculations that do not involve OAS statistical sampling, the information or data used in the calculations.

- Evaluation of results.

20-02-30-04-B Reports

If statistical sampling is used, the methodology appendix should explain the relationship between the target population and what was reviewed and clearly describe the sample design. If the sample design is too technical or lengthy, it should be included as a separate appendix.

It may be appropriate to describe details of the sample design in the finding if the information is integral to the finding. When the description of the sample design does not add to the persuasiveness of a finding, but is necessary to explain how the data was accumulated and analyzed, it is appropriate to use an appendix. In some instances, a report may need a reasonably detailed description in the finding and in an appendix.

The report should also provide perspective on the extent and significance of reported findings, such as the frequency of occurrence relative to the number of cases or transactions tested and the relationship of the findings to the entity's operations. If the sample included evidence that helped identify the cause of a finding or included other relevant evidence, the description of the sample results should be explained in more detail in the finding. Except as necessary to make convincing presentations, detailed supporting data need not be included in the finding.

20-02-30-04-C Supplementary Estimation Documentation

When a report is sent to the OAS headquarters review team, supplementary estimation documentation should be submitted. The supplementary documentation provides the minimal documentation necessary to aid in an efficient and effective review of the report. The supplementary documentation should contain enough information so the scope and methodology can be checked.

The following supplementary documentation should be submitted with the report:

- The approved sampling plan or mathematical calculation plan and approved modifications to the plan.

- Explanation of the estimation methodology and estimates if the explanation is not provided in the report or in the sampling plan or the mathematical calculation plan.

- For statistical estimates, output from the OAS statistical software and copies of the data files processed by the programs.

- For statistical estimates, information about the sampling frame and the sample units should be provided. The format depends on the sample design. The required information will usually be contained in the report or will be input to or output from the OAS Statistical Software. If another type of variable has been reviewed, the variable of interest should be reported. If the sample is an attribute sample, characteristics other than dollar amounts may be relevant.

- For statistical estimates, the following information should be included in the report or in the supplementary documentation when dollar amounts have been reviewed:[1]

  - For simple random samples: the number in the sampling frame, the sample size, number of errors, and the dollar value of errors. When appropriate, include the dollar value of the sampling frame and the dollar value of the sample.

  - For stratified random samples: the number in the sampling frame, a description of strata, the number per stratum, the sample size per stratum, the number of errors per stratum, and the dollar value of errors per stratum. When appropriate, include the dollar value of the sampling frame and the dollar value of sample per stratum.

  - For multistage samples: a description of stages, the number of primary units, the number of transactions or units sampled from at each stage, the number of transactions or units selected at each stage, and the number of errors and dollar values of errors. When appropriate, include the dollar value of the sampling frame and the dollar value of the transactions reviewed.

  - For other sample designs, sufficient detail so the methodology can be checked.

Supplementary documentation need not be submitted to the headquarters review team with final reports unless estimates have been changed or added to the report since the draft. If the review team did not review the draft report with supplementary documentation, supplementary documentation should be submitted with the final report.

20-02-30-04-D Reporting Composite Figures

Sometimes it is necessary to use findings from several audits and construct a composite figure for reporting purposes. Audit findings that were stated in terms of the lower limit should not be combined with other audit findings that were stated in terms of the point estimate since the sum would be meaningless.

From a technical point of view, the most reasonable figure to report as an estimate is the point estimate. Values for monetary recovery, which have been based on lower limits or another negotiated figure, can be reported separately.

Ordinarily there is no need to display a confidence interval for the sum of several audit findings in a consolidated management report. However, should this be necessary, the correct values for the limits of the confidence interval of the sum are not the sum of lower limits and the sum of the upper limits. A new overall confidence interval for the sum should be calculated.

20-02-40 STATISTICAL SAMPLING AND MATHEMATICAL CALCULATION PLANS

A statistical sampling plan or mathematical calculation plan is required for all audits if estimates relevant to the audit objectives are reported.

These plans document the steps involved in taking a sample or designing a mathematical calculation. The plans also guide auditors in executing the sample or performing the mathematical calculation, and aid in preparing the scope and methodology section of the

[1] If another type of variable has been reviewed, the variable of interest should be reported. If the sample is an attribute sample, characteristics other than dollar amounts may be relevant.

report. See Section 20-02-50, *Statistical Sampling*, for the format of a sampling plan, and Section 20-02-90, *Estimates Involving Mathematical Calculations*.

20-02-50 STATISTICAL SAMPLING

Statistical sampling depends on the principle of random selection. By selecting a sample randomly, personal bias and subjective considerations are eliminated from the sample. The random numbers used to select the sample and their source must be documented in the audit documentation. The details of sample selection, including the handling of missing units and use of replacement units, should also be documented in the audit documentation.

Sample estimates should be based on output from OAS approved programs. The computer output, copies of the data files processed by the computer programs, and other supporting material should be part of the audit documentation.

The employee should use *SD-9, Sampling Plan*. The elements to be included in the plan are discussed below.

20-02-50-01 Audit Objective

The audit objective to be achieved and the audit procedure, or combination of procedures, to be applied to achieve that objective should be described.

20-02-50-02 Target Population, Sample Unit, and Sampling Frame,

The target population, sample unit, and sampling frame should be identified as an initial step in designing the sample.

- The target population is the group about which information is desired.
- A sample unit is any of the designated elements that comprise the target population.
- The sampling population is the totality of the sample units from which the sample will be selected. The physical or electronic listing of the sampling population is known as the sampling frame. The auditor should determine and document how the target population differs from the sampling frame and what affect that will have on conclusions drawn from the audit.

20-02-50-03 Survey Information

Information gathered during the survey that is relevant to the sample should be described. This may include the results of risk analysis and an internal control assessment, coordination with other auditors and specialists, an analytical review and transaction testing of the controls, and any appropriate background information. This information can help support the conclusion that statistical sampling is necessary to conduct the audit more efficiently.

Criteria, which is generally identified during the planning phase, should be described in the Characteristics to be Measured section, and not in the Survey Information section.

20-02-50-04 Sample Design

The type of sample design to be used must be identified. The most common designs used are simple random sampling, stratified random sampling, and multistage sampling. Details about the strata, stages, and clusters should be included, if appropriate.

20-02-50-05 Sample Size

The sample size is critical for the efficient conduct of the audit. Exhibit A summarizes the minimum sample size requirements for the most common sample designs.

For simple random sampling, the minimum sample size is 100 sample units. Use of larger sample sizes usually has the advantage of yielding estimates with better precision without affecting the point estimate. Better precision results in a larger lower limit for the confidence interval of the estimate. The lower limit is used as the amount recommended for monetary recovery.

For stratified random sampling, the minimum sample size is 100 randomly selected sample units with a minimum of 30 sample units per random stratum.

There are various methods for allocating sample units among the strata including proportional allocation and optimal allocation. The sample sizes for the strata do not have to be identical or multiples of each other.

For multistage sampling, at least 8 primary sample units should be selected with a sample of at least 30 transactions for each primary sample unit

Larger sample sizes or strata should be considered when a minimum number of units with the characteristics of interest is required for estimation. See section 20-02-80, *Minimum Number of Units With the Characteristic of Interest*, for information on when a minimum number of units with the characteristics of interest is required.

Discovery and acceptance sampling can be used to verify a high error rate in a sampling population. The minimum sample size for discovery sampling is 30 units. If 30 units are randomly selected and all are determined to be in error, we are 95 percent confident the error rate in the sampling frame is at least 90 percent. If more reliance than 95 percent confidence and 90 percent error rate is needed, a larger sample size is needed.

20-02-50-06 Source of Random Numbers and Method of Selecting Sample Units

The source for the random numbers used to select sample units should be shown in the sampling plan. The OAS Statistical Sampling Software is the required source of random numbers. The random numbers used for selecting the sample must be documented. The method for selecting the sample units should be explained.

20-02-50-07 Characteristics to Be Measured

The purpose of a sample is to determine the extent of a characteristic or combination of characteristics existing in a given sampling frame. It is important to be specific in defining what is to be measured and to include the definition in the sampling plan. For example, a sample may be taken to estimate the value of overpayments due to duplicate payments. The characteristics under consideration are the conditions that should exist for a sample unit to be a duplicate. The amount of the duplicate payment is the measurement of the overpayment.

The criteria developed in the survey phase are used in developing the characteristics to be measured.

20-02-50-08 Treatment of Missing Sample Units

Often sample units cannot be located. How missing sample units are handled depends on the objectives of the audit and characteristics being analyzed. The sampling plan should include a discussion of (1) how missing sample units are to be handled and (2) the rationale.

20-02-50-09 Estimation Methodology

The objective of the audit and the sample design affect the estimation methodology and the estimates calculated. Sampling for attributes is used to estimate the rate or proportion of a characteristic or group of characteristics in a sampling frame. Variables sampling is used to estimate quantitative characteristics, usually dollar amounts, in a sampling frame. The same sample can be used to calculate both variable and attribute estimates.

The plan should include a description of what estimates are to be reported, the rationale for using the estimate, and how the estimate will be calculated. For monetary recovery, use the difference estimator and recommend recovery at the lower limit of the 90 percent two-sided confidence interval. For estimates of FPBU, use the appropriate estimator and report the point estimate. Report the precision or the 90 percent confidence interval for all statistical estimates. For rate-setting audits, use the appropriate estimator and recommend the point estimate.

20-02-50-10 Other Evidence

Although sample results should stand on their own in terms of validity, sample results may be combined with other evidence in arriving at specific audit conclusions. Audit teams should indicate what other substantiating or corroborating evidence will be developed.

When audit evidence collected and analyzed is sufficient and appropriate to reach a persuasive and compelling conclusion that a condition has a very high error rate, discovery sampling may be used as additional supporting evidence for the finding.

20-02-50-11 Description of How Results Will Be Reported

The auditor should be able to envision how the results of the sample should be used and reported. Describe how the results will be reported in enough detail to clearly indicate what estimates will be reported.

20-02-50-12 Sources of Data and Assessment Made on Data Reliability

- Sources of Data - Identify the sources of data to be used, e.g., National Claims History, or OIG Data Warehouse. These sources are available on the completed form SD-22, *Assessing the Reliability of Computer-Processed Data, Source of Data* Section.

- Validation of Data Sources - Briefly describe the data validation work performed by the team. This information is available on the completed form SD-22, *Assessment* Section.

20-02-60 STRATIFED RANDOM SAMPLING

One method commonly used to improve sampling efficiency is to stratify the sampling frame. A stratification plan performed for convenience need not be a statistically efficient plan. An example of stratification for convenience is stratification by OIG regions. The audit manager should be aware of the impact of a sample designed for convenience compared to a more efficient design; such a stratification plan may require a larger overall sample to ensure that a minimum number of items with the characteristics of interest is obtained in each stratum.

For stratified random sampling, the minimum sample size is 100 sample units with a minimum of 30 sample units per random stratum – at least 100 of the sample units should be randomly selected. If a certainty stratum is used, it should be added to the randomly selected sample of 100 or more sampling units.

There are various methods for allocating sample units among the strata including proportional allocation and optimal allocation. The sample sizes for the strata do not have to be identical or multiples of each other.

20-02-70 MULTISTAGE SAMPLING

Multistage sampling can reduce the expense of reviewing transactions by reducing the number of locations that are visited by the auditors. Multistage sampling involves breaking the sampling population into subgroups called primary sample units. In the first stage of the sample design, a statistical sample is taken of the primary sample units. In subsequent stages, statistical subsamples are selected from the preceding sample unit.

For a two-stage sample, at least 8 primary sample units should be selected with a sample of at least 30 transactions from each primary unit.
When using multistage designs, use as few stages as possible. Statistical specialists must be consulted in designing the sample, selecting the sample, and analyzing the results.

An example of a multistage sampling application is an audit centering on a state's administration of Medicaid funds with the objective to estimate unallowable costs incurred in nursing homes. Nursing homes would be the primary sample units. Since it is impractical to review all nursing homes within a state, the auditor selects a statistical sample of at least eight nursing homes within the state. Patients within the selected nursing homes are statistically sampled and reviewed as the secondary sample units. Since the samples of nursing homes and patients were selected statistically, estimates for FPBU may be made for all nursing homes within the state.

Variability among sample units can greatly affect the precision of multistage estimates. Multistage sampling should only be used if no other sampling technique is practical.

20-02-80 MINIMUM NUMBER OF UNITS WITH THE CHARACTERISTIC OF INTEREST

There is no minimum number of units with the characteristic of interest required to make an estimate if the following conditions are met:[2]

- The lower limit of the estimate is positive.

[2] In addition, when appraising the data from a simple random sample, there is no minimum number of sample units with the characteristic of interest required for an attribute appraisal.

- The upper limit of the estimate is not intended to materially support the findings, conclusions, or recommendations.

- There are no negative error values in the sample.

If these conditions are not met, the following minimum error counts are required to calculate an estimate without the approval of the OAS statistician:

- For all sampling designs, a minimum of three percent of the sample units must have the characteristic of interest in the final anaylsis.

- As an additional requirement for stratified random sampling, a minimum of two sample units in each stratum must have the characteristic of interest in the final analysis.

20-02-90 ESTIMATES INVOLVING MATHEMATICAL CALCULATIONS

Depending on the objectives of the audit, it may be appropriate to develop estimates that are derived from mathematical calculations that do not involve OAS sampling. See *Government Auditing Standards* Chapter 6 for guidance on using the work of others.

If estimates are calculated using data or information other than OAS sample results, a mathematical calculation plan is required. The employee should use *SD-10 Mathematical Calculation Plan*.

The elements to be included in the mathematical calculation plan are:

- Audit Objective - The audit objective to be achieved and the audit procedure, or combination of procedures, to be applied to achieve that objective will be described.

- Description of Estimates to Be Calculated - Give a brief narrative of the estimate to be calculated, e.g., “The audit will include an estimate of the number of widget builders in the United States in 2009.”

- Estimation Methodology - Briefly describe the mathematics that will be used in the estimate, e.g., “The total number of employees in the widget industry in 2009 was 42,000. Nineteen percent of the industry are builders. The number of builders is calculated by multiplying 42,000 by 19 percent.”

- Sources of Data - State the sources of data to be used in the estimation, e.g., “The Bureau of the Census Statistical Abstract of the United States for 2010 showed the number of widget workers for 2006. Bureau of Census documentation is attached. The National Widget Association (NWA) maintains statistics on the industry and provided us with their annual publication for 2009. The publication indicated the percentage of workers by job classification. NWA documentation is attached.

- Validation of Data Sources - Briefly describe the data validation work performed by the team. Reports generated by nationally known organizations, such as the Bureau of the Census, may be accepted at face value. Reports generated by the auditee require additional validation work by the team. The role of the estimate in the report dictates the extent of validation. An estimate for background purposes requires less validation than a significant estimate used to recommend a legislative change. For example, the plan might state, “Other statistical data in the NWA publication were

validated by comparison to the Bureau of the Census data. The data reconciled and therefore we are reasonably assured that the date is reliable."

- Reasons for Using Data - Describe why the estimate is needed in the report and why statistical sampling was not used to develop the estimate.

20-02-100 JUDGMENTAL SAMPLING

Judgmental sampling involves the use of an auditor's judgment in the selection of sample units (generally these will be transactions such as claims, invoices, beneficiaries, or recipients) and removes the element of randomness from the sampling plan. The major disadvantage of judgmental sampling is that a judgmental sample is not necessarily representative of the sampling population and the results of a judgmental sample cannot be used to make estimates about the sampling population. Also, judgmental sampling cannot be a basis for recommending FPBU or cost recoveries beyond those items identified in the judgmental sample.

Statistical sampling methods are preferable because they are more likely to result in obtaining sufficient, competent evidence in a more efficient manner. However, under certain conditions it may be appropriate to use judgmental sampling.

A judgmental sample may be used as evidence to convince management that a problem exists. Additional substantiating information is always needed to support the findings (e.g., assessment of controls). Collectively, these results should provide the auditor with sufficient and appropriate audit evidence. However, the auditor must not imply in the report an evaluation or opinion on all units in the sampling population (such as rate of noncompliance or amount of unauthorized expenditures).

When a judgmental sample is used as evidence to convince management that a problem exists, at least 30 units should be reviewed.

A sampling plan is not needed for a judgmental sample. However, a description of the judgmental sample design and the method for selecting the sample units should be documented in the TeamMate file. A description of the sample should be included in the methodology section of the audit report.

20-02-110 POLICY EXCEPTIONS

Any proposed deviation from this policy should be approved by the OAS statistician. Requests for any deviations should include either a valid statistical justification for not following the policy in the given situation or a detailed statement explaining why the existing policy could not be followed. All exceptions should be approved in writing before the exception is applied and should be documented in the TeamMate file of the applicable audit.

Exhibit 6-20-02-A

Minimum Sample Sizes

Sample Design	Minimum Sample Sizes
Simple Random Sampling	Minimum: 100 sample units
Stratified Random Sampling	Minimum: 100 randomly selected sample units with minimum of 30 sample units per random stratum
Multistage Sampling	Minimum: 8 primary sample units with minimum of 30 transactions per primary sample unit

Large enough sample sizes should be used to assure sufficient items exist in the sample with the characteristics of interest as discussed in Section 20-02-80, *Minimum Number of Units With the Characteristic of Interest.*

INTERNAL CONTROLS

20-03-00 PURPOSE

This chapter establishes policies and procedures for reviewing internal controls established by audited organizations and for assisting the Department in meeting its responsibilities under the Federal Managers' Financial Integrity Act (FMFIA) (Public Law 97-255) as implemented by the Office of Management and Budget (OMB) Circular A-123, Management Accountability and Control, and OMB Circular A-127, Financial Management Systems.

20-03-10 STANDARDS

Government Auditing Standards provide the following guidance for conducting internal control assessments.

Auditors should obtain an understanding of internal control significant to the audit objectives and assess whether specific internal control procedures have been properly designed and implemented.

Chapter 6 of *Government Auditing Standards* classifies and describes three areas of internal control to assist auditors in understanding the controls and to determine the significance of such controls to the audit objectives. These classifications include: the effectiveness and efficiency of program operations; relevance and reliability of information; and compliance with applicable laws, regulations, and provisions of contracts or grant agreements.

In addition to *Government Auditing Standards*, OMB Circular A-123 provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting management controls.

20-03-20 POLICY

It is OAS policy to obtain an understanding of internal control as it relates to the specific audit objectives. The audit team should consider whether specific internal control procedures have been properly designed and implemented.

20-03-30 THE AUDIT PROCESS

In the audit process, setting clear, specific audit objectives will help the auditor understand internal controls and determine the significance of these controls to the audit objectives. Throughout the audit process, the audit team should exercise professional skepticism. Professional skepticism is an attitude that includes a questioning mind and a critical assessment of audit evidence.

During the planning phase, the team establishes audit objectives and considers the internal controls that may be significant to the audit objectives and the scope of the audit.

This may be accomplished by meeting with program officials to discuss information on the program and identifying potential problem areas. The team should also review policies and procedures relating to the effectiveness and efficiency of program operations, validity and reliability of data, compliance with applicable laws and regulations and provisions of contracts or grant agreements that may be significant to the audit objectives.

During this phase, the audit team should also consider work performed by other auditors or reviewers to determine the reliance which the audit team can place on internal controls. The audit team should make maximum use of audits of internal controls made by other auditors. (See Chapter 20-05, *Using the Work of Others*.)

Information gathered during this phase will alert the audit team to potential risk factors which could affect the audit approach. The team will make preliminary decisions about the relevance of internal controls to the audit objectives and the effectiveness of these controls.

During the survey phase, the audit team should gain an understanding of the internal controls that are significant within the context of the audit objectives. For internal controls that are significant within the context of the audit objectives, auditors should assess whether internal controls have been properly designed and implemented. The team should identify areas of potential audit risk and design audit work to minimize such risk.

By analyzing the audit risk and performing internal control assessments, the team will refine the audit objectives so that the audit resources will focus on those areas of highest risk. During the survey phase, the audit team will determine the effectiveness of internal controls. The team should also review the resolution of recommendations from prior audits to identify possible internal control weaknesses.

The audit team should include in the audit documentation steps taken to assess internal controls, relevance of internal controls to the audit objectives, and the basis for any modification made to the objectives.

During the data collection and analysis phase, the audit team should use the survey results to determine the amount of testing needed. If internal controls are found not to be effective, the data collection and analysis phase should include tests of controls and documentation of the results and conclusions of these tests.

The audit report should include the scope of work on internal controls and any significant deficiencies found during the audit.

20-03-40 REVIEW OF INTERNAL CONTROLS OF COMPUTER-BASED SYSTEMS

Audits may include a review of internal controls of computer-based systems. A review of information systems controls is especially important when computer processed data is an important factor in the operations of the auditee and the computer processed data significantly affects the audit objectives. Information systems controls are significant to the audit objectives if auditors determine that it is necessary to evaluate the effectiveness of the controls in order to obtain sufficient, appropriate evidence. When information systems controls are determined to be significant to the audit objectives, auditors should evaluate the design and operating effectiveness of such controls. Auditors should obtain a sufficient understanding of information systems controls necessary to assess audit risk and plan the audit within the context of the audit objectives.

When computer-processed data is significant to the auditor's findings and conclusions, auditors need to satisfy themselves that the data is complete and accurate (valid and

reliable). This is important regardless of whether the data is provided to the auditor or the auditor independently extracts it. Auditors must perform a data reliability assessment for all computer-processed data that support findings, conclusions, or recommendations. The assessment should be conducted early in the audit process, well before using the data in the audit. The auditors should document this assessment using Standard Document 22, *Assessing the Reliability of Computer Processed Data* (SD-22). The SD-22 is required for all audits started after April 24, 2013, in which computer-processed data, such as data for a statistical sample, support the findings and recommendations.

SPECIAL AUDITS

20-04-00 PURPOSE

This chapter establishes OAS policies and procedures for evaluating requests for special audits and for performing and reporting the results of special audits. Special audits include recipient capability audits, bid proposal audits, grant and contract closeout audits, and facilities and administrative cost audits. In addition, this chapter references sample notification letters which are available on the Intranet.

20-04-10 POLICY

In its role as financial advisor to the HHS, OAS routinely receives requests for audit services from other HHS agencies or offices and other Federal departments. Evaluation of all audit requests should be coordinated between the division and the appropriate regional office.

When evaluating requests for special audits OAS will consider the following factors in addition to any specific factors listed separately for each type of audit:

- Why is the audit being requested?
- Is an audit the appropriate tool to satisfy the request?
- What difference will the audit make/how will the results of the audit be used?
- How soon are results needed?
- Are resources available to satisfy the request in the timeframe needed?
- Is the commitment of audit resources appropriate?

The majority of requests generally involve the kinds of limited scope audits discussed in this chapter. It is not intended that each finding presented in the report always contain fully developed attributes. In addition, because most special audits are low-risk and the audit results are needed in a short time frame, use of TeamMate Current Issues, also known as OARS (Objective Attributes Recap Sheet) is left up to the judgment of the audit team.

20-04-20 BACKGROUND

The purpose of Recipient Capability Audits, Bid Proposal Audits, and Grant and Contract Closeout Audits is to provide the awarding office with:

- An assessment of the recipients' general capability to satisfactorily manage and account for HHS funds.

- Information to assist in negotiating a contract.

- Information to assist in closing out a contract.

The purpose of Facilities and Administrative Cost Audits is to provide the:

- HHS, Program Support Center, Division of Cost Allocation (DCA) assistance on specific facilities and administrative cost issues at non-Federal entities (States, local governments, and non-profit organizations).

- HHS, Public Health Service (PHS) Agencies assistance on specific facilities and administrative cost issues at for-profit organizations and educational institutions and other nonfederal entities.

20-04-30 RECIPIENT CAPABILITY AUDITS

The Department has established a program of early assessment of new organizations having little or no experience managing Federal funds. Such assessments, known in OAS as Recipient Capability Audits, should be made either prior to or shortly after award of the grant or contract. Evaluating recipient capability is primarily a management function; however, an agency may periodically request that we perform a Recipient Capability Audit on their behalf.

Requests for Recipient Capability Audits should be directed to the appropriate AIG. When evaluating a request for a Recipient Capability Audit the OAS will consider the nature of any concerns raised by the requesting official in addition to the factors listed in Section 20-04-10. OAS will generally perform Recipient Capability Audits of organizations that are new recipients of Federal funds.

20-04-30-01 Audit Objectives

Recipient Capability Audits determine the adequacy of an organization's accounting and administrative systems and their financial capabilities to satisfactorily manage and account for Federal funds. The objectives of Recipient Capability Audits usually include a determination of whether the organization:

- Is financially capable of performing as a responsible contractor or grantee.

- Maintains adequate:

    - Systems and internal controls relating to accounting, budgeting, personnel, procurement, and property control to administer federally-funded projects.
    - Financial management reporting systems to provide accurate, current, and complete disclosure of the financial results of each award.
    - Monitoring and evaluation systems for both financial and program performance activities.

It should be noted that the objectives of Recipient Capability Audits include neither an evaluation of the proposed budget of the grant or contract proposals nor the possible effects of any quantitative and qualitative technical reviews performed for the sponsoring HHS agency.

20-04-30-02 Reporting

The report is for use by the awarding agency in making decisions with respect to awarding funds to the organization and/or considering what, if any, special terms and conditions should be imposed to adequately protect Federal funds. Accordingly, a draft report should not be prepared for comment by the auditee. However, care should be exercised to ensure that advance discussion of any findings be held with auditees prior to their inclusion in a final report, and this discussion should be mentioned in the report. Further, the report should generally be addressed to the awarding agency and the auditee should not be provided with a copy of the report.

Upon completion of the field work, the auditor should provide the requesting grant or contracting officer with the verbal results of the audit (if acceptable to the awarding agency) and with the expected date that the report will be issued. Supervisory review of audit results should occur before the results are made known to the contracting officer.

The report should include:

- A statement that the audit was performed in accordance with generally accepted government auditing standards. (See Chapter 30-02, *Reporting on Results of Audits*, Section 30-02-50-11-04, *Methodology - When Following All Generally Accepted Government Auditing Standards*, for the required statements. See Section 30-02-50-11-05 when the standards were not followed.)

- Statements that the report is for use by the awarding agency to assess the financial management capabilities of the organization and that the OAS did not provide the auditee with a copy of the report.

- Discussion of the conditions and the potential effects of any weaknesses found during the audit. Related causes may be included if these are readily determinable.

- A request for the awarding agency to apprise the OAS as to the disposition of issues discussed in the report.

For additional reporting requirements, see Chapter 30-02, *Reporting on Results of Audits*.

20-04-40 BID PROPOSAL AUDITS

The OAS considers performing audits of bid proposals when requested by either HHS OPDIV/STAFFDIVs or other Federal agencies.

20-04-40-01 Requests by HHS OPDIV/STAFFDIVs

Each year HHS agencies award several billion dollars to universities and nonprofit organizations in the form of contracts. While most of these awards are made to large well-established entities, many are also made to new community-based organizations and first-time contractors. When evaluating a request for a Bid Proposal Audit, the OAS will consider the following factors: the contracting officer's concerns, the dollar amount of the proposals, and other work scheduled at the entity. Priority will be provided to those bid proposals that exceed $1 million.

20-04-40-02 Requests by Other Federal Agencies

The Office of Management and Budget (OMB) Circular A-133, Audits of States, Local Governments and Nonprofit Organizations and the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. 200.513), provide that non-Federal entities expending more than $50 million a year in Federal awards shall have a cognizant agency for audit. The designated cognizant agency for audit is the Federal awarding agency that provides the predominant amount of direct funding to an organization unless OMB makes a specific cognizant agency for audit assignment and provides notice in the Federal Register. A Federal awarding agency with cognizance for an auditee may reassign cognizance to another Federal awarding agency which provides substantial direct funding and agrees to be the cognizant agency for audit. For organizations expending less than $50 million a year in Federal awards, the oversight agency for audit is the Federal awarding agency that provides the predominant amount of direct funding to a recipient not assigned a cognizant agency for audit. (Note: For contractors other than educational institutions and nonprofit organizations, DCAA is normally cognizant.)

OAS is the cognizant agency or oversight agency for audit of most of the nation's nearly 3,000 research institutions. Each year, OAS budgets staff days, on a reimbursable basis to perform audits requested by other Federal agencies of funds awarded to institutions by these agencies. When evaluating a request for a Bid Proposal Audit from another Federal agency, OAS will consider the following factors in addition to those listed in Section 20-04-10: dollar amount of the proposal, sensitivity of issues to be reviewed, agency agreements, and other work being done at the institution.

20-04-40-03 Audit Objectives

At the request of the contracting officer, OAS usually will audit cost or pricing data when the contracting officer is negotiating a contract or modification resulting from proposed costs in excess of $1 million. However, the contracting officer may request audit services for cost or pricing data of lesser amounts when reasonable pricing cannot be established because of the lack of knowledge of the particular contractor or the inability to evaluate the reasonableness of price through price analysis or cost analysis of existing data.

When requesting audit services, the contracting officer should describe the extent of support needed, state the specific areas for which input is required and include the information necessary to perform the audit. Based on the contracting officer's request, the auditor will determine the scope and depth of the audit. To provide the contracting officer with information to assist in negotiating a contract, the auditor should usually:

- Determine the reasonableness and allowability of proposed costs.
- Determine whether the proposed costs were supported by current, complete, and accurate cost or pricing data.
- Make a limited assessment of the auditee's internal controls related to the accumulation and segregation of costs by project.

It should be noted that the audit objectives do not address the possible effects of the quantitative and qualitative technical reviews performed by the Federal contracting agency. For example, the objectives of the audit include neither determining the need for nor reasonableness of the proposed positions and related labor hours, equipment, material and supply quantities, travel and other items included as direct costs.

20-04-40-04 Missing or Deficient Cost or Pricing Data

Cost or pricing data submitted by an offeror or contractor permit the Government to perform cost or price analysis and ultimately enable the Government and the contractor to negotiate fair and reasonable prices. Cost or pricing data may be submitted actually or by specific identification in writing (Title 48—Federal Acquisition Regulations System (FAR), Chapter 1-- Federal Acquisition Regulation, PART 15, Contracting by Negotiation, Subpart 15.4, Contract Pricing).

The requirement for submission of cost or pricing data is met if all cost or pricing data which are reasonably available to the offeror are either submitted or identified in writing to the contracting officer by the time of agreement on price. However, there is a clear distinction between submitting cost or pricing data and merely making available books, records and other documents without identification. The latter does not constitute submission of cost or pricing data.

If cost or pricing data and information required to explain the estimating process are required and the offeror initially refuses to provide the necessary data, or the auditor determines that the data provided is so deficient as to preclude an audit or considers the proposal unacceptable as a basis for negotiation, OAS shall notify the contracting officer verbally so that prompt corrective action may be taken. The auditor should immediately confirm the notification in writing, explaining the deficiencies and the cost impact on the proposal.

20-04-40-05 Reporting

The report is for use by the contracting officer to serve as the basis for negotiating a contract. Accordingly, audit results should not be discussed with the auditee and a draft report should not be prepared for comment by the auditee. The auditor should, however, discuss discrepancies and mistakes of fact contained in the proposal with auditee officials to provide them with the opportunity to provide additional or corrected information.

Upon completion of field work, the auditor should provide the contracting officer with verbal results of audit and with the expected date that the report will be issued. Supervisory review of audit results should occur before the results are made known to the contracting officer.

The report should include:

- A statement that the audit was performed in accordance with generally accepted government auditing standards. (See Chapter 30-02, *Reporting on Results of Audits*, Section 30-02-50-11-04, *Methodology - When Following All Generally Accepted Government Auditing Standards*, for the required statements. See Section 30-02-50-11-05 when the standards were not followed.)

- Statements that the report is for use by the contracting officer to serve as the basis for negotiating a contract and that the OAS did not provide the auditee with a copy of the report.

- A statement that the audit did not include a technical evaluation to determine the need for the proposed positions, related labor hours, and other costs. Further, the results of audit do not include the possible effects of any quantitative and qualitative technical reviews performed by the contracting agency.

- A statement of the extent to which the auditor has discussed the results of the audit with auditee officials.
- A request for the contracting officer to provide the OAS with a copy of the *Summary of Negotiation* if the contract is awarded.
- Depending on the needs of the requesting official, any or all of the following evidence may be required:
    - Cost analysis summarizing all pertinent factors considered necessary for negotiating the contract,
    - Data used to develop rates and factors including the latest available actual data,
    - Incurred hours/costs, and/or
    - Comments on any proposal element considered to be inadequately supported by cost or pricing data.

For additional reporting requirements, see Chapter 30-02, *Reporting on Results of Audits*.

20-04-50 GRANT AND CONTRACT CLOSEOUT AUDITS

OAS considers performing audits of selected grantees and contractors for the purpose of issuing a report on cost incurred on completed grants or contracts when requested by HHS grants and contracting officers, HHS Assistant Secretary for Administration and Management and other Federal agencies. Requests for audits of specific grants or contracts that are not yet completed should be considered on a case-by-case basis.

20-04-50-01 Post Award Grant and Contract Audits

When evaluating a request for a Grant Closeout Audit or Contract Closeout Audit, OAS will verify whether HHS or another Federal agency is cognizant and determine whether the grants or contracting officer has utilized the single audit report prepared by non-Federal auditors. Generally, higher risk grants/grantees contracts/contractors will be selected for review.

PHS agencies award several billion dollars each year to educational institutions and other nonprofit organizations in the form of grants and contracts. While most of these awards are made to large, well-established organizations which will have audits performed under OMB Circular A-133 or the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. 200), many are also made to for-profit contractors, new community-based organizations, and first-time contractors which may not receive single audits.

20-04-50-02 Requests by Other Federal Agencies

Under OMB Circular A-133 or the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. 200), OAS has audit cognizance for most of the major research institutions. Audit cognizance authorizes the OAS to perform audits upon request, from all Federal agencies, of funds awarded to educational institutions by these agencies. Each year the OAS budgets staff days and enters into interagency agreements relative to reimbursements to perform these audits. When evaluating requests for Grant Closeout Audits and Contract Closeout Audits, OAS will consider the following factors in addition to those listed in Section 20-04-10: the dollar

amount of the contract, the sensitivity of issues to be reviewed, whether the requesting agency's reimbursable agreements will cover the cost of the audit, and other recent audit work performed at the institution.

20-04-50-03 Audit Objectives

To provide the grant or contracting office with information to assist in closing out the grants or contracts, the auditor will discuss the audit with the requesting office and obtain that office's agreement on the objectives and scope of the audit. Usually a grant or contract closing audit will require the auditor to determine whether the:

- Costs claimed represent allowable, allocable, and reasonable costs under the terms of the contract and applicable Federal regulations.

- Contractor's claim for staff salary agrees with employee time and effort reports certified by the designated responsible official.

20-04-50-04 Reporting

The report is for use by the contracting officer to serve as the basis for closing out the contract. Accordingly, a draft report should not be prepared for comment by the auditee. However, care should be exercised to ensure that advance discussion of any findings be held with auditees prior to their inclusion in a final report. Further, the report should be addressed to the awarding agency and the auditee should not be provided with a copy of the report.

The report should include:

- A statement that the audit was performed in accordance with generally accepted government auditing standards. (See Chapter 30-02, *Reporting on Results of Audits*, Section 30-02-50-11-04, *Methodology - When Following All Generally Accepted Government Auditing Standards*, for the required statements. See Section 30-02-50-11-05 when the standards were not followed.)

- Statements that the report is for use by the grant or contracting officer to serve as the basis for closing out the contract and that OAS did not provide the auditee with a copy of the report.

- A statement, in the scope section of the report, citing the cost principles used in determining the allowability of the proposed costs, e.g., OMB Circular A-21, Cost Principles for Educational Institutions or the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. 200).

- Schedules summarizing the results of the audit. The schedules should show by element of expense: amount claimed, amount recommended for acceptance, amount recommended for disallowance, and amount set aside (no opinion). Such schedules are not necessary if all costs are recommended for acceptance.

For additional reporting requirements, see Chapter 30-02, *Reporting on Results of Audits*.

20-04-60 FACILITIES AND ADMINISTRATIVE COST AUDITS

OAS may provide audit assistance to the DCA on specific facilities and administrative cost issues at selected educational institutions. DCA is located in the HHS Assistant Secretary for Administration and Management and is responsible for negotiating facilities

and administrative cost rates with educational institutions. When evaluating requests for Facilities and Administrative Cost Audits OAS will consider the following factors in addition to those listed in Section 20-04-10: the complexity and significance of the proposal, the existence of controversial studies, large increases in the proposed rates, or significant changes in proposed costs.

20-04-60-01 Audit Objectives

To provide DCA with information to assist in negotiating the organization's facilities and administrative cost rate, the auditor will usually determine whether the costs in the facilities and administrative cost proposal represent allowable, allocable, and reasonable costs under the terms of the applicable Federal regulations.

20-04-60-02 Reporting

The report is for use by DCA officials to serve as the basis for establishing the facilities and administrative cost rates. Accordingly, a draft report should not be prepared for comment by the auditee. However, care should be exercised to ensure that advance discussion of any findings be held with the auditee prior to their inclusion in the final report. Further, the report should be addressed to the responsible HHS official and the auditee should not be provided with a copy of the report.

The report should include:

- A statement that the audit was performed in accordance with generally accepted government auditing standards. (See Chapter 30-02, *Reporting on Results of Audits*, Section 30-02-50-11-04, *Methodology - When Following All Generally Accepted Government Auditing Standards*, for the required statements. See Section 30-02-50-11-05 when the standards were not followed.)

- Statements that the report is for use by the responsible HHS official in negotiating the organization's facilities and administrative cost rate, if applicable, and that OAS did not provide the auditee with a copy of the report.

- A statement, in the scope section of the report, citing the cost principles used in determining the allowability, allocability and reasonableness of the proposed or incurred costs, e.g., OMB Circular A-21, Cost Principles for Educational Institutions or the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. 200).

For additional reporting requirements, see Chapter 30-02, *Reporting on Results of Audits*.

Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. 200)

20-04-70 LIMITED DISTRIBUTION

Since Recipient Capability Audits, Bid Proposal Audits, Grant Closeout Audits, Contract Closeout Audits, and Facilities and Administrative Cost Audits are performed to assist HHS officials in meeting their stewardship responsibilities, including negotiating with grantees and contractors, OAS will address the reports to the responsible Government official and will not provide the audited entity with a copy of these audit reports.

For distribution requirements, see Chapter 30-04, *Distribution of HHS Produced Audit Reports*.

The Recipient Capability Audit, Bid Proposal Audit, Grant Closeout Audit, Contract Closeout Audit, and Facilities and Administrative Cost Audit. reports will not be published on the Internet.

20-04-80 NOTIFICATION LETTERS

Auditors are generally responsible for sending a notification letter to the auditee on all audits and reviews, including special audits. A notification letter provides a means of formalizing the understanding between the OAS and the auditee concerning the objectives of the audit as well as apprising auditees of the documents and records which it should make available to the OAS auditors. Normally, the auditor should apprise the auditee, by telephone, of the planned audit and make arrangements to have an entrance conference. To confirm the arrangements, the auditor should consider sending a letter to the auditee. The letter should usually be sent prior to the entrance conference and start of audit work on-site. Sample notification letters for special audits are available on the Intranet.

USING THE WORK OF OTHERS

20-05-00 PURPOSE

This chapter establishes OAS policies and procedures for using the work of others during the conduct of a performance audit. Using the work of auditors or specialists during an audit can reduce audit effort. This chapter does not apply to the work performed by independent public accountants under contract by the OIG to perform audits of HHS' programs (which is discussed in Chapter 10-05, Contracting for Audit Services.)

20-05-10 STANDARDS

The standards for planning audit work for a performance audit are found in Chapter 6 of the *Government Auditing Standards*. Auditors can use the work of others as long as the auditors follow certain procedures.

20-05-20 POLICY

It is OAS policy to make maximum use of the work of others in accomplishing audit objectives when appropriate. A separate assessment must be documented for each specialist or organization whose work or services are used in conducting the audit.

20-05-30 RESPONSIBILITIES

During the survey phase, the audit team will determine the extent of reliance that can be placed on the work of others such as State auditors, independent public accountants (IPAs), internal auditors, and specialists. These other auditors and specialists may have performed related work prior to or outside of our upcoming audit effort. The team should contact other audit organizations that may have performed work related to the OAS audit objective, make a judgment whether it can be relied on and use the work to the fullest extent possible.

If the audit team is considering using the work of other auditors, the audit team should perform procedures that provide a sufficient basis for using that work. The nature and extent of the procedures depends on the materiality of the other auditors' work and the extent to which the audit team will use that work in its report. The procedures performed by the audit team during this assessment must be included in the audit documentation.

20-05-40 ASSESSING THE OTHER AUDITOR

To use the work of other auditors, the audit team must be satisfied with the other auditors' qualifications and independence. Procedures should be performed to consider the following aspects of the other auditor.

Qualifications

- If not already known, make inquiries about the professional reputation of the other auditor to other practitioners or other appropriate sources.
- Determine whether the audit organization has a program to ensure that its staff meet the continuing education requirements of Chapter 3 of the *Government Auditing Standards*.
- If the work of IPAs is under consideration, check if the IPA meets the licensing requirements of the jurisdiction where the auditee is located and if the license is current.
- Determine whether the audit staff collectively possess the knowledge and experience necessary to perform the audit.
- Determine whether the organization has an internal quality control system in place, and if it participates in an external quality control review program. Consider reviewing a recent audit report or management letter on the results of a review.

Independence

- Obtain a representation that the other auditor is independent as required by the *Government Auditing Standards.*

20-05-50 ASSESSING THE OTHER AUDITORS' WORK

If the audit team intends to use the work of other auditors, the audit team should perform procedures regarding the specific work to be relied on that provide a sufficient basis for that reliance. Procedures should be performed to assess the sufficiency and appropriateness of the other auditors' work. Again, the audit team should exercise professional judgment in determining the extent of procedures needed. The audit team should consider performing the following steps before assuming responsibility for the other auditors' work.

- Review the other auditor's report.
- Visit the other auditor and discuss the audit procedures employed and the results obtained.
- Inquire if the auditor is familiar with *Government Auditing Standards* and if the standards were followed during the review.
- Review the audit plan of the other auditor.
- Review the audit documentation of the other auditor. Assess the sufficiency of the audit documentation and determine if there is evidence that a supervisory review was performed.

The preceding steps are not intended to be all inclusive of the points for consideration before relying on the work of other auditors. The audit team may want to perform supplemental tests of the other auditors' work. The nature and extent of evidence needed will depend on the significance of the other auditors' work and the extent to which the audit team will use that work.

20-05-60 RELIANCE ON SPECIALISTS

When using the work of specialists (physicians, statistical specialists, etc.), the audit team faces similar considerations. The audit team should:

- Satisfy itself as to the specialists' professional reputation, qualifications, and independence.

- Obtain an understanding of the methods and assumptions used by the specialists.

20-05-70 REPORTING

The report should disclose the extent to which the audit team used the work of others. When the audit team uses the work of another auditor or specialist, reference to the other auditor or specialist should be made in the report when describing the audit scope and methodology. An explanatory paragraph can be added to the scope and methodology section that clearly explains the evidence gathered and techniques used by the other auditor or specialist. This explanation should identify any significant assumptions made by the other auditor or specialist in conducting the audit. The report should describe the depth and coverage of work conducted to accomplish the audit objectives.

EVIDENCE AND AUDIT DOCUMENTATION

20-06-00 PURPOSE

This chapter establishes OAS policies and procedures for the accumulation of audit evidence used in supporting conclusions, opinions, and recommendations expressed in audit reports. It also describes policies and procedures for the preparation and retention of audit documentation.

20-06-10 STANDARDS

Government Auditing Standards prescribe the requirements for evidence and audit documentation in Chapter 6. Auditors must prepare audit documentation related to planning, conducting, and reporting for each performance audit. Audit documentation should contain sufficient detail to enable an experienced auditor, with no previous connection to the audit, to understand from the audit documentation the:

- Nature, timing, extent, and results of audit procedures performed.
- Audit evidence obtained and its source.
- Conclusions reached, including evidence that supports the auditors' significant judgments and conclusions.[1]

Chapter 6 also states that auditors must obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions.

[1] An experienced auditor means an individual who possesses the competencies and skills that would have enabled him or her to perform the performance audit. These competencies and skills include an understanding of (a) the performance audit processes (b) *Government Auditing Standards* and applicable legal and regulatory requirements, (c) the subject matter associated with achieving the audit objectives, and (d) issues related to the audited entity's environment.

20-06-20 POLICY

It is OAS policy to comply fully with *Government Auditing Standards* when obtaining evidence and preparing audit documentation, regardless of the nature of the audit assignment.

In conducting audits the audit team should:

- Obtain and record in the audit documentation sufficient, appropriate evidence of the work performed to provide reasonable assurance to support the audit team's judgments and conclusions.

- Record in the audit documentation the objectives, scope, and methodology, including sampling methodology.

Audit documentation is the principal support for the audit team's representation regarding observance of the standards, including planning, supervision, and reporting.

20-06-30 THE AUDIT PROCESS

Chapter 2 of *The Audit Process Handbook* contains guidance on both the collection of audit evidence and the preparation of audit documentation.

Chapter 3 of *The Audit Process Handbook* contains standard audit documents for use in OAS audits. The OAS Intranet site provides links to each standard audit document, as well as instructions on how to download them. Use of these audit documents is encouraged, and they can be customized for individual audit assignments by audit teams, as audit requirements dictate.

20-06-40 EVIDENCE

Audit evidence is the data and information that the audit team obtains during an audit to support findings, opinions, and conclusions. Audit evidence tends to prove or disprove any matter in question or to influence a belief about it and gives the auditors a rational basis for forming judgments. A considerable amount of the audit team's work consists of obtaining, examining, and evaluating evidential matter.

20-06-40-01 Categories of Evidence

Evidence may be categorized as physical, documentary, and testimonial:

.

- Physical evidence is obtained by the audit team's direct inspection or observation of people, property, or events. Such evidence may be documented in summary memorandums, photographs, videos, drawings, charts, maps, or physical samples.

- Documentary evidence is obtained in the form of already existing information such as letters, contracts, accounting records, invoices, spreadsheets, database extracts, electronic stored information, and management information on performance.

- Testimonial evidence is obtained through inquiries, interviews, focus groups, public forums, or questionnaires.

Audit teams frequently use analytical processes including computations, comparisons, separation of information into components, and rational arguments to analyze any evidence gathered to determine whether it is sufficient and appropriate.

20-06-40-02 Sufficient and Appropriate Evidence

Auditors must obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions.

Sufficiency is a measure of the quantity of evidence used for addressing the audit objectives and supporting findings and conclusions. In determining the sufficiency of evidence, the audit team should determine whether enough appropriate evidence exists to address the audit objectives and support the findings and conclusions.

The sufficiency of evidence required to support the auditors' findings and conclusions is a matter of professional judgment. The following presumptions are useful in judging the sufficiency of evidence.

- The greater the audit risk, the greater the quantity and quality of evidence required.
- Stronger evidence may allow less evidence to be used.
- A large volume of audit evidence does not compensate for a lack of relevance, validity, or reliability.

Appropriateness is the measure of the quality of evidence that encompasses its relevance, validity, and reliability in providing support for findings and conclusions related to the audit objectives. In assessing the overall appropriateness of evidence, auditors should assess whether the evidence is relevant, valid, and reliable. The following presumptions are useful in judging the appropriateness of evidence.

- Relevance refers to the extent to which evidence has a logical relationship with, and importance to, the issue being addressed.
- Validity refers to the extent to which evidence is a meaningful or reasonable basis for measuring what is being evaluated. In other words, validity refers to the extent to which evidence represents what it is purported to represent.
- Reliability refers to the consistency of results when information is measured or tested and includes the concepts of being verifiable or supported.

20-06-40-03 Source of Evidence Obtained

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. Each type of evidence has its own strengths and weaknesses.

The nature and types of evidence to support the audit team's findings and conclusions are matters of the auditors' professional judgment based on the audit objectives and audit risk. The following contrasts are useful in judging the appropriateness of evidence; however, these contrasts are not adequate in themselves to determine appropriateness:

- Evidence obtained when internal control is effective is generally more reliable than evidence obtained when internal control is weak or nonexistent.

- Evidence obtained through the auditors' direct physical examination, observation, computation, and inspection is generally more reliable than evidence obtained indirectly.

- Examination of original documents is generally more reliable than examination of copies.

- Testimonial evidence obtained under conditions in which persons may speak freely is generally more reliable than evidence obtained under circumstances in which the persons may be intimidated.

- Testimonial evidence obtained from an individual who is not biased and has direct knowledge about the area is generally more reliable than testimonial evidence obtained from an individual who is biased or has indirect or partial knowledge about the area.

- Evidence obtained from a knowledgeable, credible, and unbiased third party is generally more reliable than evidence from management of the audited entity or others who have a direct interest in the audited entity.

- Testimonial evidence may be useful in interpreting or corroborating documentary or physical information. 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.

When auditors use information gathered by officials of the audited entity, the auditors should determine what the officials did to obtain assurance that the information was reliable. The audit team 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 the auditors or the auditors independently extract it. The nature, timing, and extent of audit procedures to assess sufficiency and appropriateness are 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. The assessment of the sufficiency and appropriateness of computer-processed information includes considerations regarding the completeness and accuracy of the data for the intended purposes.

20-06-40-04 Overall Assessment of Evidence

The audit team should determine the overall sufficiency and appropriateness of evidence to provide a reasonable basis for its findings and conclusions within the context of the audit objectives. Professional judgment about the sufficiency and appropriateness of evidence is closely interrelated, as auditors interpret the results of audit testing and evaluate whether 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.

Sufficiency and appropriateness of evidence are relative concepts, which may be thought of in terms of a continuum rather than as absolutes. Sufficiency and appropriateness are evaluated in the context of the related findings and conclusions. For example, even though auditors may have some uncertainties about the sufficiency or appropriateness of some of the evidence, they may nonetheless determine that in total there is sufficient, appropriate evidence to support the findings and conclusions.

Section 6.69 and 6.72 of *Government Auditing Standards* contains additional information on the overall assessment of evidence.

20-06-50 ACCESS TO RECORDS

The legal citation for the OAS right of access to records is set forth in the Office of Inspector General enabling legislation (IG Act), specifically 5 USC Appendix, Section 6. The legislation authorizes the IG's access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials available to the applicable establishment, which relate to programs and operations for which the IG has responsibility. In addition, other statutes, regulations or grant/contract terms provide access to records of grantees, contractors, and participants in specific programs.

20-06-50-01 Denial of Access to Records

In situations where the audit team is denied access to certain information or records, Section 6(a)(4) of the IG Act provides the authority to require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary in the performance of the functions assigned by the IG Act. The subpoena is enforceable by an order of any appropriate United States district court.

The IG has delegated authority to the DIG and AIG to subpoena records required to complete an audit. If a subpoena is needed, the OCIG must be contacted to review the subpoena request.

Failure to obtain information or records necessary to conduct the audit should be recorded in the audit documentation and disclosed in the scope section of the report, along with the known effect it had on the results of the audit.

20-06-50-02 Substandard Records

When an auditee's records considered essential to complete an audit are found to be inadequate or unauditable, the audit team should consider pursuing alternative auditing techniques as a means of accomplishing the audit objectives. These techniques could include interviewing program officials, employees, or participants, and using various forms of judgmental and statistical sampling. The decision on whether to pursue any or all of the alternative auditing techniques should be based on reasonable economic limits (i.e., the relationship between the cost of obtaining evidence and the usefulness of the information) in consultation with the appropriate RIG or AIG.

The need for and the alternative auditing techniques used should be included in the audit documentation. The documentation should be sufficient to provide for reporting the:

- Additional audit work done.
- Results of the audit work.

- Basis for a qualified opinion or a disclaimer of opinion if the audit team was unable to obtain sufficient evidential matter to form a conclusion.
- Recommendations detailing what must be done by the auditee to make the records auditable.

20-06-60 REQUEST ABOUT OAS CONFIDENTIALITY STANDARDS AND/OR REQUEST TO SIGN A LETTER OF ASSURANCE AS A CONDITION OF BEING GIVEN ACCESS TO RECORDS THAT CONTAIN PII OR OTHER SENSITIVE INFORMATION

Access to and safeguarding of PII and other sensitive information is a concern of many organizations. Before giving OAS access to such information, an auditee may ask OAS to:

- Provide information about the confidentiality standards OAS employees are required to follow and/or

- Sign a confidentiality agreement or letter of assurance as a condition of being given access to records that contain PII or other sensitive information.

20-06-60-01 Response to Request for OAS Confidentiality Standards

If the auditee or another organization asks about OAS confidentially standards, provide the following information:

- The OIG has established policies and procedures to reasonably and appropriately protect the security, integrity, and confidentiality of the personally identifiable information including electronic or paper media that the OIG creates, receives, maintains, uses or transmits. For example, the OIG uses encryption and shred software on its laptop and desktop computers and has restricted access entry to protect personally identifiable information obtained during audits. All OIG auditors operate pursuant to these policies and procedures to safeguard against unauthorized use and access of sensitive information entrusted to them.

- The OIG uses and discloses personally identifiable information only in a manner consistent with Federal law, for example, as required by the Privacy Act of 1974 (5 U.S.C. § 552a), the Freedom of Information Act (5 U.S.C. § 552), and the Inspector General Act (5 U.S.C. App.). To further protect particularly sensitive information, files/documents are clearly marked to alert any official reviewer that this information should be treated as confidential. In this respect, the [Name of auditee] should mark any files/documents produced for the audit that it believes to be confidential proprietary information. To the extent that OIG determines that such files/documents contain confidential proprietary information, OIG agrees to treat as confidential proprietary information all such files/documents and information pursuant to 18 U.S.C. section 1905.

- All Federal agencies, including the OIG, are required by the Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. § 3541 *et seq.*) and by OMB Memorandum M-06-19 of July 12, 2006, to report all security incidents (suspected or confirmed) involving personally identifiable information to the United States Computer Emergency Response Team (US-CERT), which is the Federal incident response center, located within the Department of Homeland Security. All such incidents must be reported within one hour of discovering the incident.

20-06-60-02 Letter of Assurance

The auditee or another organization may require OAS auditors to provide written confirmation of OAS's policies and procedures for protecting PII or other sensitive information, e.g., Medicaid beneficiary data, before it will release such information to OAS. OIG generally does not sign confidentiality agreements, but will provide a letter of assurance.

Under no circumstance, should OAS respond to or sign a confidentiality agreement or a letter of assurance without consulting with OCIG. This is to ensure that OAS does not bind itself to any overly restrictive conditions on use and disclosure of information that are contrary to Federal laws or OIG responsibilities.

A template for preparing a letter of assurance is available on OAS's Intranet if a letter of assurance is appropriate. Any letter prepared using this template must be approved by OCIG.

A copy of the letter of assurance should be provided to the appropriate AIG.

20-06-70 AUDIT DOCUMENTATION – GENERAL

The term "audit documentation" encompasses all documents and other media containing the evidence used to provide a reasonable basis for the audit team's conclusions regarding the organization, program, activity, or function under audit. Audit documentation should contain the objectives, scope, and methodology, including any sampling methodology. Audit documentation includes all of the records kept by the audit team of the procedures applied, the information obtained, and the tests performed to support significant conclusions and judgments reached in the audit. It also contains the TeamMate Current Issue(s), also known as Objective Attributes Recap Sheet(s) (OARS), audit plan, copies of grants or contracts, abstracts of documents, memorandums, letters of confirmation and representation, analyses and schedules, and commentaries prepared or obtained by the audit team. Computer programs, record layouts, file descriptions, flow charts, and other documents prepared by computer specialists as members of the audit team are considered audit documentation.

20-06-70-01 Purpose

Audit documentation serves three primary purposes:

- It is the principal support for the audit report.
- It aids the audit team in conducting and supervising the audit.
- It allows others to review the quality of the audit.

Audit documentation should be appropriately detailed to provide a clear understanding of its purpose, source, and conclusions that the audit team reached. The audit documentation should be appropriately organized to provide a clear link to the findings, conclusions, and recommendations contained in the audit report.

Sufficient and appropriate evidence should be contained in the audit documentation to support the audit team's judgments and conclusions. Audit documentation contains:

- The objective, scope, and methodology of the audit, including the sampling methodology.

- The audit team's determination that certain standards do not apply or that an applicable standard was not followed, the reasons for that determination, and the known effect that not following the applicable standard had or could have had on the audit.

- A description of the work performed to support significant judgments and conclusions, including descriptions of transactions and records examined.[2]

- Evidence of supervisory review, before the audit report is issued, to ensure that the work performed supports the findings, conclusions, and recommendations contained in the audit report.

- Information for supervisors and managers to enable them to carry out their assignments and to evaluate the performance of staff assigned to the audit.

- Information for future use in planning and carrying out subsequent assignments.

- Documentation of conformance with *Government Auditing Standards* and compliance with OAS audit policies and procedures, and/or that certain standards or OAS policies and procedures do not apply to the audit.

When the audit team does not comply with applicable *Government Auditing Standards* due to law, regulation, scope limitations, restrictions on access to records, or other issues impacting the audit, the auditors should document the departure from *Government Auditing Standards* and the impact on the audit and on the auditors' conclusions. This applies to departures from both mandatory requirements and presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the standard.

20-06-70-02 Basic Principles

The form and content of audit documentation should be designed to meet the circumstance of the particular audit. The following basic principles should be observed by audit teams when preparing audit documentation:

- The procedures followed by the audit team, including the analysis and interpretation of the audit data, should be included in the audit documentation. An experienced auditor, as defined by *Government Auditing Standards,* with no previous connection to the audit should be able to ascertain from the audit documentation the evidence that supports the audit team's significant conclusions and judgments. Well-prepared audit documentation also permits other audit team members to pick up the audit at a certain point (e.g., at the completion of the survey phase) and carry it to its conclusion.

- The information contained in the audit documentation should be clear and complete, yet concise. Clarity and completeness should not be sacrificed to save time.

- The information in the audit documentation should be restricted to matters that are materially important and relevant to the objectives of the assignment. Before the audit team develops audit documentation such as analyses, exhibits, and schedules, the following should be clearly determined: (1) the objectives or what needs to be

[2] This requirement can be met by listing file numbers, case numbers, or other means of identifying specific documents examined. It is not required that copies of documents examined be included as part of the audit documentation.

proven; (2) the information needed to complete the analysis; (3) the location of the needed information (filed, recorded, etc.); and (4) the comparisons needed to prove the condition(s) or conclusion(s). Unnecessary or irrelevant audit documentation should not be prepared or retained.

- The audit file should include exception-only documentation. The audit team may meet this requirement by listing file numbers, case numbers, or other means of identifying specific documents the team examined. The audit team is not required to include copies of documents it examined as part of the audit documentation, nor is the team required to list detailed information from those documents. However, in error cases, when the audit team's findings may be subject to interpretation, it may be useful to retain more detailed documentation.

- Audit documentation should be well planned and organized. Audit documentation is more than just a record of the work performed. Audit documentation should provide a clear link to the findings, conclusions, and recommendations in the audit report.

- Adequate planning is the key to the development and preparation of good audit documentation.

- Audit documentation should be uniformly designed and arranged to facilitate the reviewer's job. If the audit documentation is of high quality and is developed, organized, and cross referenced to the overall audit plan, supervisors and other reviewers such as quality control reviewers should experience no difficulty in understanding or evaluating it.

20-06-70-03 Electronic Audit Documentation

Electronic audit documentation is required as the standard medium for OAS audits, research and development (R&D) and other efforts (collectively referred to as "projects"). OAS uses TeamMate, including EWP,[3] an electronic audit management tool. TeamEWP must be used in all projects[4], including audits that are expected to result in an issued audit report. Start all projects, including audits and R&D in the *centralized* database – no projects are to be started as distributed, i.e., outside the centralized database.[4]

The retention of hard copy documents too voluminous to scan into TeamEWP may be necessary in some circumstances. In addition, brochures, computer media, and physical items or samples may be retained outside of TeamEWP if they are needed to support the audit findings and conclusions. See the *TeamEWP Handbook* for more information.

[3] EWP – Electronic Working Papers

[4] There are some R&D and other efforts where it is appropriate because of the nature or duration of the effort, e,g., database analysis or effort lasting only a few days, that TeamEWP will not be used.

20-06-70-04 Terminated Audits

When an audit is terminated prior to its completion and an audit report is not issued, the audit team should document the results of the work to the date of termination and why the audit was terminated. In addition, the audit team should communicate the reasons for terminating the audit to management of the audited entity, the entity requesting the audit, and other appropriate officials. This communication should be documented in TeamMate. If such communication might compromise an ongoing or contemplated investigation, the audit team should consult with OI for advice on handling the matter.

20-06-70-05 Suspended Audits

If work on an audit is suspended, the audit team should record the suspension start date in WebAIMS. The reason for the suspension should be documented in the Comments section of the WebAIMS audit record.

If the audit is resumed, the suspension end date should also be recorded in WebAIMS.

If the audit is terminated the auditors should follow the procedures in section 20-06-70-04, *Terminated Audit*.

20-06-80 AUDIT DOCUMENTATION - FOLDERS

See the *TeamMate EWP Handbook* for the folder (file) structure OAS has developed for the electronic audit documentation system.

20-06-90 AUDIT DOCUMENTATION - SPECIFIC

OAS uses specific types of audit documentation that merit further explanation. These are written audit plans, TeamMate Current Issues, and records of discussion.

20-06-90-01 Written Audit Plan

A written audit plan must be prepared for each audit. While the form and content of the plan will vary among audits, the various elements of the plan should be contained in one document. The plan should be updated to reflect any significant changes to the plan made during the audit. The plan should include an audit program and/or audit procedures describing specific steps to be taken to accomplish the audit objectives.

Written audit plans may also include the following:

- A memorandum or other appropriate documentation of key decisions about the audit objectives, scope, and methodology. The plan may also include the audit team's basis for those decisions.

- A description of the program to be audited including sufficient background and criteria on the program to be audited.

- A brief description of the audit objectives(s) scope and methodology and the audit team's basis for those decisions.

The report feature in TeamMate EWP should be used to create an audit program including all the procedure steps to be used on the audit. The created audit program should then be imported into the audit plan.

20-06-90-02 TeamMate Issue

The audit team should prepare a TeamMate Current Issue for each audit objective and include the TeamMate Current Issue in the audit documentation. However, TeamMate Current Issues are prepared at the option of the audit team on special audits as defined in Chapter 20-04, *Special Audits*. A TeamMate Current Issue should be a concise document, ideally one page in length when printed out to a Microsoft Word document as an OARS. A TeamMate Current Issue must include the following:

- Objective - The purpose of the audit work or an explanation of why it was undertaken and what the audit team is trying to accomplish.
- Attributes of the Finding - The criteria, condition, effect, cause, and recommendation.
- Comments by Auditee Personnel - The relevant comments made by auditee personnel with whom the finding was discussed. If no deficiencies were found, that information should also be included in the TeamMate Current Issues.

(See Chapter 1 of *The Audit Process Handbook*, figure 1-1, for an example of an OARS.)

20-06-90-03 Records of Discussions

The results of meetings, interviews, conferences, and phone calls (including report review conferences) should be recorded in the audit documentation. This includes entrance and exit conferences.

20-06-100 INDEXING AND HYPERLINKING/CROSS-REFERENCING

Indexing is essential to facilitate review and understanding of audit documentation. The primary purpose of indexing is to facilitate the hyperlinking of audit documentation. An indexing system is automatically set up within TeamMate EWP.

20-06-100-01 Hyperlinking/Cross-Referencing

Cross-referencing is defined as a notation at one place in the audit documentation referring to information at another place. No audit should be considered complete until the audit documentation is thoroughly and accurately cross-referenced. Changes to supporting information should also be referenced to other affected sections of the audit documentation. At a minimum, the audit plan, TeamMate Current Issue, and the audit report should be cross-referenced to the audit documentation.

For electronic audit documentation, this process is referred to as hyperlinking. Hyperlinking is the ability to automatically navigate/jump from one location to another by clicking a reference link.

20-06-110 CONTENT

The content, quantity, and type of audit documentation for each audit assignment is based on the audit team's professional judgment. Factors entering into the judgment process include the:

- Objective.
- Scope.

- Degree of reliance on internal controls.
- Extent of reliance on the work of others.
- Condition of the auditee's records.
- Nature of the information which the audit team is reviewing.

Certain information is essential to understand individual audit documentation. The following information should be included whenever applicable:

- Attributes - Each audit document should identify the attribute(s) of a finding that the audit documentation addresses. The attributes are criteria, condition, effect, cause, and recommendation. If the audit documentation is not related to an attribute but is necessary background information, the audit documentation should be classified as "background."
- Sources of information - Each audit document should identify where the audit team obtained the information. This applies to schedules prepared by the audited entity and furnished to the audit team and to data compiled by the audit team. The source should be described in sufficient detail for another experienced auditor to obtain the same information.
- Purpose of the audit documentation - The audit document should state the specific reason for preparing the audit document. Clearly stating the purpose of each audit document facilitates review of the document and use by succeeding audit teams.
- Scope of the audit team's examination - Each audit document should describe what the audit team's examination included. This is particularly important when determining:
    - The volume of the transactions involved.
    - The number of transactions examined.
    - What part of the total volume the audit test represents.
    - Why the transactions were selected.
    - The period covered by the audit team's review, and what the examination consisted of (e.g., comparison of data between different periods, matching data to standards, etc.).

  When the analysis was based on a sample of transactions, the sampling plan should be described. When factors external to the audit organization and the audit team restrict the audit or interfere with the audit team's ability to form objective opinions and conclusions, the factors should be explained in the audit documentation.
- Results - This section summarizes in objective terms what the audit team found. It does not contain subjective information such as the audit team's opinion on what it found.
- Conclusions - This section reflects the judgment or opinion the audit team reached after analyzing the data. The conclusion should specifically answer the purpose. It

represents the conclusions drawn from analysis and interpretation of the results of the audit team's tests and from any related facts. When the conclusions recorded on one audit document are based in part on information in other audit documents, this fact should be noted and appropriately cross-referenced.

All audit documentation should also include:

- Title of the audit document.
- The "as of" date for the information and records used in the analysis.
- Common Identification Number.
- Name/initials of a preparer and reviewer.
- Date prepared and reviewed.
- Explanation or legend for any signs, symbols, tick marks, or acronyms used. Refer to the *TeamMate EWP Handbook* for standard tick marks.

When information is common to a series of audit documents, it need only be recorded on one of the audit documents of the series and referred to in the other audit documents.

20-06-120 SAFEGUARDING

Information on safeguarding is included in Chapter 20-11, *Protection of Sensitive OAS Information and Procedures.*

20-06-130 RETENTION

To retain audit documents, audit teams or the Divisional/Regional TeamMate Coordinator are required to finalize audits and send TeamEWP audit files completed in a distributed environment to the audit visual specialist. The audit visual specialist will complete actions required by the *TeamMate Archive CD/DVD/Server Checklist*. For more information, refer to the *TeamMate Archive User Handbook*. TeamEWP audit files completed in a centralized environment remain in the centralized database,

In accordance with the OIG Records Schedule, audit documentation, including electronic media, should be retained for a minimum of 8 years from the end of the fiscal year in which the audit report was closed and the recommendation(s) resolved, which occurs when OAS accepts the OPDIV signed OIG clearance documents (OCD). There may be certain factors, such as controversial or current interest subjects, which would necessitate holding audit documents for longer periods. Also, there may be ongoing congressional or other investigations or unsettled issues where continued reference to the audit documentation is needed.

It may not always be practical to store the numerous electronic media used in an audit. In those cases, the electronic media, the computer programs designed to generate the output, and other programming records should be retained at least until the audit report has been closed and the findings resolved. When data is extracted from a computer-based system, the sampling plan, the methodology used to select records, the computer program designed to generate the information, and the resulting output should be retained.

20-06-140 ACCESS TO AUDIT DOCUMENTATION

Audit documentation is the property of OAS. Access to audit documentation by other parties, either during or after completing the audit, will be decided by OAS management on a case-by-case basis.

In some audits it may be necessary to make copies of audit documentation available to auditee or program officials so that they can respond to findings or to take corrective actions. The audit manager, in consultation with the appropriate AIG or RIG should decide what audit documentation should be released to explain *the* findings to the auditee so that they can adequately respond to the draft report.

The auditee and program officials should never be provided the TeamMate EWP software. Further, the auditee and program officials should never be provided access to the TeamMate EWP audit file, either on an OAS computer or the auditee's program official's computer when they have a TeamMate license.[5] Any request from the auditee or program officials to access TeamMate EWP should be submitted to the Director, Audit Planning and Implementation for consideration.

All other requests for access to audit documentation should be directed to the applicable AIG or RIG. The Director, Human & Financial Resources, serves as the FOIA Liaison Officer for the OAS. In this role, the Director is responsible for providing the appropriate AIG and RIG with the necessary guidance where questions arise as to the appropriateness of granting access to our audit documentation files.

[5] The audit team may allow the auditee or program officials to view TeamMate EWP files on an OAS computer accessed by OAS personnel.

LEGAL REQUIREMENTS

20-07-00 PURPOSE

This chapter establishes OAS policies and procedures for complying with legal requirements including:

- The auditor's responsibility for providing reasonable assurance of the auditee's compliance with laws and regulations when they are significant to audit objectives.
- Coordinating with the OCIG during the audit process.

Chapter 20-08, *Investigative Activities*, provides policy on the auditor's responsibility for detecting illegal acts, and coordinating with OI.

20-07-10 STANDARDS

The standards for compliance with laws and regulations are found in Chapter 6 of the *Government Auditing Standards*. Chapter 6 requires auditors to design the audit methodology and procedures to provide reasonable assurance of detecting violations of laws, regulations, or provisions of contracts or grant agreements that are significant to the audit objectives.

20-07-20 POLICY

The audit team should design the audit to provide reasonable assurance of the auditee's compliance with laws and regulations that are significant to the audit objectives. It is OAS policy to include OCIG as part of the audit team, and generally to seek OCIG advice.

20-07-30 THE AUDIT PROCESS

Chapter 1 of The Audit Process handbook contains guidance on considering laws and regulations when planning and conducting an audit.

During phase 1 of the audit process, planning, the audit team should identify the laws, regulations and guidelines that are significant to audit objectives and determine the criteria to be used. Government programs usually are created by law and are subject to specific laws and regulations. For example, laws and regulations usually set forth what is to be done, who is to do it, the purpose to be achieved, the population served, and how much can be spent on what. Understanding laws and the legislative history establishing a program and the provisions of any contracts or grant agreements can be essential to understanding the program itself. At this point the audit team should seek OCIG advice or interpretation of laws and regulations that are significant to the audit objectives. During phase 2 of the audit process, survey, the audit team should consider the effectiveness of the auditee's internal controls to ensure compliance with laws and

regulations. The audit team's assessment of internal controls will affect the scope and methodology of the audit. When necessary to seek advice from OCIG, the RIG and or AIG may want to request that OCIG participate in the go/no go decision.

20-07-40 LAWS AND REGULATIONS

The audit team should identify the laws and regulations and provisions of contracts or grant agreements that are significant to the audit objectives. Examples of types of laws and regulations that can be significant to the objectives include those that could significantly affect the acquisition, protection, and use of the entity's resources, and the quantity, quality, timeliness, and cost of the products and services it produces and delivers.

The laws and regulations pertaining to the purpose of the program, the manner in which it is to be implemented and the population it is to serve, and the amount to be spent may be significant to the audit objectives. For laws and regulations that are significant to the audit objectives, the audit team should assess the risk that significant illegal acts could occur. Factors that may affect the risk that illegal acts may have occurred include the complexity or newness of the laws and regulations, or the effectiveness of internal controls that were established to ensure compliance with laws and regulations. Based on a risk assessment involving the factors listed above, the audit team should design and perform procedures to provide reasonable assurance of detecting significant illegal acts. The audit team should include their assessment of risk in the audit documentation.

If the audit team determines that there is a possibility that illegal acts may have occurred, the audit team should contact OI. OAS Audit Policies and Procedures Chapter 20-08, *Investigative Activities*, provides policy on when to consult OI.

20-07-40-01 Requests for Advice from the Office of Counsel to the Inspector General

The audit team should consult OCIG when the report is likely to be signed by the IG or the DIG. This consultation should begin during phase 1 of the audit process, planning, and continue throughout the audit, as necessary.

The audit team should also consult OCIG when:

- The audit team is denied access to records. (Chapter 20-06, Evidence and Audit Documentation, provides detailed policy.)
- Audit findings are the subject of investigation or prosecution.

The audit team should consider consulting OCIG when:

- Recommendations involve OAS interpretations of laws or regulations.
- A program is audited for the first time.
- The audit team is relying on definitions or concepts that are not clearly defined by statute, regulations or guidance or these sources present issues of legal interpretation.
- The audit team is uncertain or unfamiliar with a legal concept connected with the audit.

Requests for advice may be made by telephone, e-mail or in writing. Telephone advice should be confirmed via e-mail or in writing.

20-07-40-02 Request for a Formal Legal Opinion

The audit team may obtain a formal legal opinion from OCIG when there are conflicting opinions between OIG and program officials or the audited party. The appropriate AIG, in consultation with the RIG will make the final determination as to when to seek a legal opinion from OCIG. Auditors are also encouraged to seek advice from OCIG when a formal legal opinion is not necessary or to determine whether to seek a legal opinion.

A request for a legal opinion should be specific and include complete and specific background information. Examples of the type of information that should be included in a request for a legal opinion include:

- Citations for statutes, Federal regulations, guidance, cases and legal opinions on which the audit team may rely.
- The audit team's position on the issue and the conflicting position (e.g., auditee's or OPDIV's position) and the citations to statutes and regulations that may support the conflicting position. For example, the auditee may cite the State confidentiality law to prohibit access to records.
- The OAS division and region contact point.

20-07-40-03 Release of OCIG Opinions and Advice

Legal opinions and advice are protected by the attorney client privilege, and thus would typically not be releasable under the Freedom of Information Act (FOIA) or by other means. OCIG should be consulted if the audit team is considering release of an opinion outside HHS. Also, it is OIG policy not to quote directly from OCIG or HHS Office of the General Counsel legal opinions in an audit report or correspondence, or to reveal the existence or content of legal opinions to the public. The substance of the legal analysis may instead be paraphrased and presented as the position of the OIG.

Exhibit 6-20-07-A

SAMPLE REQUEST FOR A FORMAL OCIG LEGAL OPINION

From Assistant Inspector General for Audit Services

Subject Legal Issues Arising from the Audit of the Emergency Assistance Program Administered by the State's Department of Public Welfare

To Office of Counsel to the Inspector General

The Office of Audit Services, Region III is currently conducting an audit of payments made to the State Department of Public Welfare (State Agency) in Fiscal Years XXXX and XXXX under the Emergency Assistance (EA) program. We are requesting that you provide us legal assistance in areas that potentially involve recommendations for significant dollar recoveries.

Our main concern focuses on how the State agency's procedures in authorizing and claiming Federal financial participation (FFP) appear to violate Federal regulations regarding the periods in which the services could be authorized and provided.

State Agency's Time Frames for Authorizing and Providing EA Services

We believe that the State agency violated Federal regulation regarding time frames for authorizing and providing services under the EA program. The language in the approved State Plan, however, may have allowed them to do so. We are requesting determination as to whether language in the State Plan overrides Federal requirements.

Audit results show that the State Agency uses a blanket authorization form, which also serves as the application form, to authorize any and all EA related services: (1) without identifying the specific services required by the client: and (2) for an undefined amount of time "until the emergency is alleviated." We believe this practice violates provisions of 45 CFR Section 233.120(b)(3) which states that FFP "is available only for emergency assistance which the State authorizes during one period of 30 consecutive days in any 12 consecutive months."

The State agency claimed FFP under the EA program for services provided to clients more than 12 months after the date of the clients' application. For example, the State agency claimed FFP for probation services for 18,787 children who were in probation for more than a year. We tentatively plan to question the amount claimed for services provided after the 365th day from the date of the application. This could amount to about $9 million.

State Agency Position

State agency officials told us that their blanket authorization, in effect, authorized all types of EA services immediately, thus meeting the single 30 day period requirement; and that the language in the State Plan allowed them to claim FFP until the emergency condition was alleviated even if it exceeded the 12 month requirement of the Federal regulations. Attachment 1 is the State Plan, which was approved by Region III of the Administration for Children and Families (ACF). Section 3 A (page 1) states that EA to "needy families with children under the age of 21 is provided in accordance with 45 CFR 233.120." Under the section dealing with Emergency Protective Services for Children (page 5), there is a note, which states that the above services "will be provided until the emergency condition is alleviated and must be authorized during a single 30-day period no less than 12 months after the beginning of the family's last EA authorization period. "

Take for example a youth who was arrested for robbery (the emergency) and sentenced by a judge to 12 months in a detention center and 3 months probation. The State agency believes it had the right to claim

Exhibit 6-20-07-A

SAMPLE REQUEST OF OCIG LEGAL OPINION *(Continued)*

EA payments for the entire 15 months because the emergency was not alleviated until the person was released from probation. Furthermore, because of the blanket authorization, the youth could begin to receive counseling services in the 14th month even though the need for such services was not identified on the authorization form.

Federal Criteria and Other Support

We believe the Federal criteria cited above clearly precluded the State agency from exceeding the 12-month period specified in the Federal regulations. The position taken by the Departmental Appeals Board, and the stated position of ACF officials support our position that payments made for services provided outside the 12-month period are unallowable.

Appeals Board Decision (Attachment 2) The State B agency appealed ACF's decision to disallow over $15 million in EA payments. The Departmental Appeals Board ruled that to the extent that the State agency's application and authorization process did not comply with EA program requirements, its claims must be disallowed (page 2). The Board also point out (page 19) that both parties (State agency and ACF) agreed that FFP was available only for emergency assistance, which the State authorizes during one period of 30 consecutive days in any 12 consecutive months.

Declaration of John Smith (Attachment 3) Mr. Smith was the Director of the Division of Self-Sufficiency Programs in the Office of Family Assistance, Administration for Children and Families, Washington, DC. In making a declaration for the Departmental Appeals Board in the State B case, Mr. Smith declared (page 4) that "the regulation at 45 CFR 233.120(b)(3) clearly limits EA to the period of 12 months, which includes a 30-day authorization period " ACF Central Office Staff Position (Attachment 4) On July 28, xxxx, OAS staff met with ACF staff to discuss EA criteria. OAS prepared a memorandum requesting ACF's written confirmation of agreements. The memorandum stated, "The EA services may be authorized and provided for a period not to exceed 12 months. A new authorization is required We also noted a very old policy information memorandum (No.18 dated November 22, 1972) issued by the Social and Rehabilitation Service which states that assistance "must be authorized for a specific emergency" identified in the State's plan for the EA program. This memorandum (attached) appears to indicate that blanket authorizations, such as the one used by the State agency, were not acceptable.

Legal Issue to Address

The Federal regulations appear clear as to the 12-month time frame imposed on the provision of services. The regulations are not as specific with regard to the authorization of specific services of the use of a blanket authorization. We would appreciate it if you would address the following questions:

1. Does the note in the State A State Plan stating that services will be provided until an emergency condition is alleviated override Federal regulations dealing with the 12-month period? (We noted in Attachment 2, page 8 that the Departmental Appeals Board considered the language in the State B State Plan).

2. If the language in the State Plan overrides the Federal regulations, is FFP authorized for the entire period of time that the emergency condition (detention, for example) existed without another application or authorization?

3. Does the blanket authorization authorizing all EA services meet Federal requirements? If not, can we question any additional type services provided more than 30 days after the date of the initial blanket authorizations?

Exhibit 6-20-07-A

SAMPLE REQUEST OF OCIG LEGAL OPINION *(Continued)*

Summary

We appreciate your assistance in answering the above questions. Should you need further information, please call the audit manager or me responsible for this assignment.

Assistant Inspector General for Audit Services

Division Contact Point:
Region Contact Point:

cc: RIG

INVESTIGATIVE ACTIVITIES

20-08-00 PURPOSE

This chapter establishes policies and procedures for investigative activities, including:

- The auditor's responsibility for detecting and reporting on fraud during the course of an audit.
- The auditor's responsibility for receiving and reporting allegations of fraud.
- Providing audit assistance to the OIG investigative offices, i.e., OI and OCIG.
- Providing audit assistance to the Department of Justice (DOJ).

20-08-10 STANDARDS

The standards regarding the auditor's responsibility for detecting and reporting on fraud are found in Chapters 6 and 7 of the *Government Auditing Standards*. Additional guidance can be found in Appendix I, *Supplemental Guidance*, of the *Government Auditing Standards*.

20-08-20 POLICY

It is OAS policy that, in planning the audit, auditors should assess risks of fraud occurring that is significant within the context of the audit objectives.

OAS should:

- Coordinate with OI whenever an audit team identifies potential fraud during the course of the audit.
- Coordinate with OI whenever an audit team receives an allegation of potential fraud.
- Provide audit assistance to OIG investigative offices, whenever audit resources are available.
- Provide audit assistance to DOJ, in conjunction with OIG investigative offices, whenever audit resources are available.

When audit assistance is provided to OIG investigative offices or the DOJ, the audit team will decide during planning whether the work will be performed according to *Government Auditing Standards* or as nonaudit services.

20-08-30 AUDITOR RESPONSIBILITIES FOR DETECTING AND REPORTING ON FRAUD

Auditor responsibilities for detection of fraud, coordination with OI, reporting potential fraud to OI, and allegations of fraud follow.

20-08-30-01 Detection of Fraud

The auditor's responsibility for detecting fraud begins in the planning phase of the audit process. In this phase the audit team determines the laws, regulations or guidelines relevant to the audit objectives.

During the survey phase the audit team should assess risks of fraud occurring that is significant within the context of the audit objectives. Audit team members should discuss 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. An attitude of professional skepticism in assessing these risks assists auditors in assessing which factors or risks could significantly affect the audit objectives.

When auditors identify factors or risks related to fraud that has occurred or is likely to have occurred and they believe the factors or risks are significant within the context of the audit objectives, they should design procedures to provide reasonable assurance of detecting such fraud. 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.

Appendix I, *Supplemental Guidance*, of the *Government Auditing Standards* provides further guidance on the indicators of fraud risk.

20-08-30-02 Coordination with OI

When the audit team identifies situations or transactions that could be indicative of fraud, the RIG (or appropriate AIG should determine if further audit steps should be performed, or whether sufficient evidence exists to refer the potential fraud to OI. If sufficient evidence does exist, the RIG/AIG should confer with OI counterparts immediately.

During discussions with OI counterparts, a decision should be made to either continue the audit or make a formal referral of the potential fraud to OI.

The decision should be noted in the audit documentation and the cognizant AIG notified. If the audit is continued, the audit team should determine if additional audit procedures are necessary to develop sufficient evidence of potential fraud. If the audit is referred to OI for investigative action, a referral memorandum to OI should be prepared, as described in the following section.

20-08-30-03 Reporting Potential Fraud to OI

A memorandum should be prepared and provided to OI to transmit and document formal referrals of potential fraud. This referral should include information such as:

- Identifying information on the individual(s) or organization(s) to be investigated.
- The HHS program involved (e.g., Medicare, Medicaid or Foster Care).

- The Federal or State awarding agency.
- The funds involved.
- The reason for the referral and any evidence acquired that supports the potential illegal act.
- Any other background information that, in the judgment of the audit team, would be needed by OI.

After the referral is made to OI and the referral is accepted, a decision should be made in conjunction with OI to either (1) provide audit assistance to OI (for guidance on providing audit assistance to OI, see Section 20-08-40), or (2) discontinue the audit. The decision should be noted in the audit documentation and, if a regional referral is made to OI, the appropriate AIG notified.

At this time, the OI case number should be included in the Web Audit Information Management System (WebAIMS) and noted in the audit documentation. If the amount of funds in question can be estimated, this amount should be included as a pending questioned cost or funds put to better use. The WebAIMS record should then be suspended. OI should notify the OAS of the outcome of the referral.

20-08-30-04 Allegations of Fraud

Allegations and requests for investigative assistance are received from a variety of sources. They can be provided to an audit team conducting an audit or directly to an OAS office.

When the allegations are indicative of possible fraud, the RIG (or AIG for divisional audits) and other auditors reviewing the allegations should determine if further information should be requested from the alleger, or whether sufficient evidence exists to refer the indications of fraud to OI.

If sufficient evidence does exist, the RIG/AIG should confer with OI counterparts immediately to determine the course of action to be taken. At the same time, if a regional matter, the appropriate AIG should be notified that a decision was made to confer with OI regarding indications of fraud. When the allegations are not indicative of fraud, the matter can be referred to the OPDIV for action.

Disclosures outside the OIG, including referrals to an OPDIV, should not reveal the identities of complainants or other individuals who provided information to the OIG. This is particularly important when the complainant is a Federal employee. When disclosure of individual identities seems unavoidable, the auditors should first consult with the OCIG, or with the DOJ attorney assigned to the case. For additional information on responsibilities for protection of the confidentiality of employee complainants, see OIG Administrative Manual, Chapter 03-25.

All requests for investigative assistance should be referred to OI immediately and the appropriate AIG notified of the referral.

When an allegation or a request for investigative assistance is referred to OI, a transmittal memorandum should be prepared and provided to OI to document the referral of the potential fraud, and the appropriate AIG notified of the referral.

20-08-40 AUDIT ASSISTANCE TO OIG INVESTIGATIVE OFFICES

Joint projects between the OAS and OIG investigative offices (OI and OCIG) are an important function of the OIG. In these projects, the investigative office often requests audit expertise during an investigation. Requests for an investigative audit assist should be submitted to the AIG or RIG. The RIG should notify the appropriate AIG of all such requests received in the region. Since all regional investigative matters (both criminal and civil) are handled by OI, most requests for audit assistance come through the regional Special Agent In Charge.

The request should seek from the OAS professional audit assistance required in carrying out investigations. This request should include information such as:

- The nature of the allegation being investigated.
- The specific matters to be audited.
- The audit objectives to be achieved.
- Specific guidance on how audit results are to be reported and disseminated.

The RIG/AIG is responsible for evaluating the request in terms of feasibility and audit resources. For regional OI requests, the RIG should consult with the appropriate AIG. A written response should be provided to the requesting OIG investigative office.

For all requests that have been approved by OAS, the RIG/AIG and the requesting OIG investigative office should agree on the type of audit of services to be provided, the scope, objectives and methodology of such work, the time frame in which the work is to be completed, and the methodology for reporting and disseminating the results of review. The OI case number should be recorded in the WebAIMS record and in the audit documentation.

Investigative audit assistance can be completed in accordance with *Government Auditing Standards*, or as nonaudit services, depending on the circumstances. For example, obtaining and providing OI with information or data without auditor evaluation or verification of the information or data would be considered a nonaudit service.

In each investigative assist, the audit team should follow instructions from the OIG investigative office so as not to jeopardize the investigation. All inquiries regarding the status of the review, including from program officials, should be directed to the OIG investigative office.

Guidance related to the use of OAS subpoenas is presented in Chapter 20-06, *Evidence and Audit Documentation*.

20-08-40-01 Reporting

At the completion of the assist review, an assist report, for audits performed in accordance with *Government Auditing Standards*, or a memorandum, for nonaudit services provided, should transmit the audit results to the requesting OIG investigative office. Determination of whether an audit report will be released to either the auditee or the operating division will be made by the OAS in consultation with the OIG investigative office. (See Section 20-08-50-01, *Grand Jury Materials*.) If an audit report is issued, applicable OAS Audit Policies and Procedures for reporting will be followed.

20-08-50 AUDIT ASSISTANCE TO THE DEPARTMENT OF JUSTICE

DOJ may request the technical expertise of the OIG to assist in litigation involving HHS programs. DOJ requests for OIG assistance generally involve the OI, OCIG, OAS or a combination thereof.

The OCIG coordinates the OIG's role in the investigation and resolution of health care fraud cases. In all matters when the DOJ has an interest, OCIG is responsible for the imposition of permissive exclusions as well as civil monetary penalties and for mandatory exclusions as well as civil monetary penalties.

Requests for assistance with a qui tam suit or administrative sanction are generally submitted jointly to OI and OCIG. In instances when the DOJ submits requests for audit assistance (both qui tam and non qui-tam) directly to the OAS, the RIG/AIG should confer with OI and OCIG counterparts immediately. For regional audits, the appropriate AIG should be notified that a request was received from the DOJ. The request should then be evaluated in terms of feasibility and audit resources. The RIG/AIG should coordinate with OI counterparts as to whether OAS should work or not work directly with DOJ, and on a response to the DOJ. When consensus as to an appropriate course of action cannot be reached, the matter should be referred to OAS and OI headquarters for a final decision.

When the OAS decides to honor the request, the OI counterparts should be kept informed of the progress of the audit assistance work. The OI case number should be recorded in the WebAIMS record and in the audit documentation.

Investigative audit assistance is to be performed in accordance with *Government Auditing Standards* or as nonaudit services, whichever is applicable. For example, obtaining and providing DOJ with information or data without auditor evaluation or verification of the information or data would be considered a nonaudit service.

In each assist audit, the audit team should follow instructions from the DOJ so as not to jeopardize the investigation. Since each situation will be different, the auditors, with appropriate guidance from the RIG/audit manager, must use their professional judgment regarding the applicability of auditing standards. All inquiries regarding the status of the audit, including from program officials, should be directed to DOJ.

20-08-50-01 Grand Jury Material

The auditors providing assistance to DOJ must exercise due professional care when dealing with materials, including documentary and testimonial evidence. When these materials are received through the powers of a Federal grand jury inquiring into possible Federal criminal violations, specific disclosure restrictions also apply. It is imperative that audit team members, including appropriate management staff, are given access to these materials via a DOJ disclosure letter under Rule 6(e) (3) (A) (ii). This letter adds a team member to what is referred to as the 6e access list. (OI will provide whatever assistance is necessary to ensure appropriate OAS staff are included in the process.) The letter informs individuals of their responsibilities regarding grand jury materials. The 6e access is arranged through the DOJ contact.

In general, access to these materials is for the sole purpose of assisting the Federal attorneys involved in the grand jury investigation in the performance of their duties to enforce criminal law. These proceedings are secret and unauthorized disclosure of grand jury matters is punishable by contempt proceedings. No grand jury material may be disclosed or used for any civil or administrative purpose or for any purpose other than for the grand jury investigation, except by order of the court.

20-08-50-02 Lawsuits Filed Under Seal/QUI TAM Cases Under the False Claims Act

The False Claims Act (codified at 31 U.S.C. §§ 3729-3733) establishes a civil cause of action for the United States to recover from individuals who knowingly present false claims (or false information supporting those claims) to the United States. Awards under the False Claims Act can be substantial. Defendants may be liable for a civil penalty of not less than $5,000 and not more than $10,000 for each false claim, plus three times the amount of the damages sustained by the Government because of the false claim.

The False Claims Act authorizes "qui tam" actions, whereby a private individual (called a "relator") who has knowledge of fraud against the Government, may bring an action in Federal court on behalf of the United States, and share in any damages and penalties recovered. Such complaints are filed in camera (for the court's eyes, only) and remain under seal for 60 days, and during any extensions of that time granted by the Court, while the Government investigates the allegations and determines whether to intervene and prosecute the action. While the matter remains under seal, auditors who are assigned to support a qui tam case may not disclose to the target or to others the existence of the lawsuit or any of the documents filed in the lawsuit. Covered documents will usually bear the legend "Filed Under Seal."

At some point in the proceedings, the Government will likely move for a partial lifting of the seal (to enable it to discuss settlement with the targets). If the Government decides to intervene, the complaint will be fully unsealed and served upon the target - other documents may remain sealed. Accordingly, before taking any action that would disclose the existence of the qui tam matter, auditors should consult with the Department of Justice attorney assigned to the case.

20-08-50-03 Reporting

At the completion of the audit assist, a DOJ assist report, for audits performed in accordance with *Government Auditing Standards*, or a memorandum, for nonaudit services, should transmit the results to the requesting DOJ attorney. Determination of whether an audit report will be released to either the auditee or the operating division will be made by the OAS in consultation with DOJ and OI. (See Section 20-08-50-01, *Grand Jury Material*.) If an audit report is issued, applicable OAS Audit Policies and Procedures for reporting will be followed.

REPORTING LOSS OF SENSITIVE INFORMATION OR ELECTRONIC MEDIA AND COMPUTER INCIDENT DETECTION AND REPORTING RESPONSIBILITIES

20-09-00 PURPOSE

This chapter establishes OAS policies and procedures for reporting to management any incident involving the suspected or confirmed:

- Loss or unauthorized disclosure of Personally Identifiable Information (PII)[1] or loss of electronic media.
- Occurrence or appearance of a threat to an OIG computer system, or any activity that involves using an OIG system in an improper manner.
- Breach or attempted breach of security in an information system.

20-09-10 STANDARDS

The standards for protecting PII and reporting incidents involving the breach of PII are found in OMB Memorandums:

- M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.*
- M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

OMP has issued two OIG Information Security Handbooks. These handbooks provide baseline security guidance for the OIG. One handbook includes guidelines for information owners and system administrators, while the second handbook is geared for all other users. All OIG users (personnel, contractors, and other authorized users) are responsible for reviewing and following the guidelines described in the appropriate handbooks.

[1] Personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name or social security number, or that when combined with other personal or identifying information is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. PII includes but is not limited to medical records, billing records, payment records, claims adjudication records, and case or medical management records that include personal identifiers, e.g., names, Social Security Numbers, and Medicaid recipient numbers.

20-09-20 DEFINING SENSITIVE INFORMATION WITHIN OAS

The OAS definition of sensitive information is contained in Chapter 20-11, *Protection of Sensitive Office of Audit Services Information*.

20-09-30 POLICY

OAS employees must immediately report:

A. Suspected or actual loss, compromise, or theft of PII – not including the receipt of unprotected PII from third parties[2] via email, OAS sensitive information, or OIG electronic media, including:

- Suspected or confirmed incidents resulting in the loss or unauthorized disclosure of PII or other sensitive data. All incidents must be reported even if the data is encrypted or destroyed, e.g. in a fire. Examples of reportable incidents include, but are not limited to:
  - Passphrase/password compromised
  - OAS transmitted unencrypted sensitive information outside the OIG in the body of an email via the HHS/OIG Delivery Server
  - OAS transmitted encrypted or unencrypted sensitive information outside the OIG via email (OAS employees must use the HHS/OIG Delivery Server[3] to transfer files *outside* the OIG containing sensitive information regarding a planned or active audit, or OI or Department of Justice (DOJ) assist work. See Subsection, 20-11-40-06, *Securely Transferring Electronic Files Containing Audit and/or Sensitive Information Over the Internet or Intranet*.)
  - Unauthorized disclosure of sensitive information
  - Unauthorized viewing of sensitive information
- Loss of OIG hardware in their possession, whether or not assigned to them. (Losing an item includes theft of the item. Hardware includes computers, Blackberries, and any electronic media used to store data, e.g., external hard disks, NetDisks, USB drives, and CD/DVDs.)
- A hard drive(s) sent to the manufacturer or repair facility, regardless of whether it is under warranty or not. See Subsection 20-11-40-12, *Destruction of Sensitive Information*.
- TeamMate files sent to the TeamMate vendor, without the express written authorization of the IT Audit Director.

For reporting requirements, see Subsection 20-09-40, *Reporting Suspected or Actual Loss, Compromise, or Theft of PII, OAS Sensitive Information, or OIG Electronic Media*.

B. Computer incidents, including:

- A threat or the appearance of a threat to an OIG computer system, or any activity that involves using an OIG system in an improper manner.

[2] A third-party refers to an organization or person that is not part of HHS or operating on behalf of HHS. Receipt of PII from third parties via mail is addressed in Chapter 20-12, *Receipt of Unprotected Personally Identifiable Information in Email from a Third-Party, HHS OPDIV, or organization operating on behalf of HHS.*

- A breach or attempted breach of security in an information system.

For more reporting requirements, see Subsection 20-09-50, *Computer Incident Detection and Reporting Responsibilities*.

All OAS employees should report suspected or confirmed incidents or losses within one hour of discovery, regardless of the time of day or day of year.

20-09-40 REPORTING SUSPECTED OR ACTUAL LOSS, COMPROMISE, OR THEFT OF PII, OAS SENSITIVE INFORMATION, OR OIG ELECTRONIC MEDIA

If an employee either suspects or confirms an incident resulting in the loss or unauthorized disclosure of PII or other sensitive data, the employee should immediately notify the appropriate management officials as outlined below.

20-09-40-01 Notification Procedures

It is critical to notify the OIG Chief Information Security Officer (CISO), as the CISO has strict guidelines for departmental and Department of Homeland Security reporting, including very tight timeframes.

When appropriate, law enforcement authorities should be notified as well.

20-09-40-01-01 Staff Responsibilities

Upon suspicion or detection of a loss, compromise, or theft of PII, OAS sensitive information, or electronic media OAS employees must immediately (within one hour) take the following actions by phone and email:[3]

- Regional employees must notify their RIG, or designee, and
- Division and headquarters (HQ) employees must notify their HQ Director, or designee.

If an employee is unable to speak to the RIG/HQ Director or designee, the employee should immediately notify an audit manager by phone and email.

Immediately after notifying an OAS management official of the suspected loss, the employee should notify the OIG Information System Security Officer (ISSO) (isso@oig.hhs.gov), at 202-205-9207 (office) or 888-415-8421 (toll free number). The employee should copy the OAS Incident Notification Team (OAS-Incident-Notification@oig.hhs.gov) on the email to the ISSO.

The reporting employee should include as much information about the incident as pertinent/possible in their report, e.g:

- Date and time the incident was suspected/discovered.
- Type of incident, e,g:
  - Lost
  - Stolen
  - Destroyed, e.g., in a fire

[3] During business hours, employees should report incidents via telephone discussion (not voice mail) with email follow-up. During non-business hours they should send emails, if service is available through OIG Intranet (in an OIG office or through VPN); otherwise, employees should leave a voice mail and follow-up with telephone discussion (not voice mail) the next business day.

  - Hard drive sent to manufacturer or repair facility
  - Passphrase/password compromised
  - TeamMate files sent to the TeamMate vendor, without the express written authorization of the Director, Information Systems Audit and Advanced Techniques.
  - Unauthorized disclosure of sensitive information
  - Unauthorized viewing of sensitive information
- Type of Media, e.g:
  - Computer – Desktop
  - Computer – Notebook
  - CD(s) / DVD(s)
  - Electronic file(s), e.g., OAS sent PII via email
  - External Hard Drive
  - Hard Copy (paper)
  - USB (Jump) Drive USB (Jump) Drive - describe
- Was media encrypted (not applicable to paper)? If yes, did encryption method meet the requirements of FIPS 140-2?
  - CD(s) / DVD(s) All Data Encrypted with PGP Self Decrypting Archive
  - CD(s) / DVD(s) All Data NOT Encrypted with PGP Self Decrypting Archive
  - Hard Drive - Whole Disk Encrypted
  - Hard Drive - Not Encrypted
  - USB Drive - Whole Disk Encrypted
  - USB Drive - Partial Disk - All data on encrypted portion
  - USB Drive - Partial Disk - Not all data on encrypted portion
  - USB Drive - Not Encrypted
  - Multiple Media - All Data Encrypted
  - Multiple Media - NOT All Data Encrypted
- Did missing media/electronically transmitted data contain PII and/or sensitive information?
  - Yes – Contains PII
  - Yes – Contains PII and other sensitive information
  - Yes – Contains sensitive information other than PII
  - No – Contains no PII or other sensitive information
  - Not sure
- What is the nature of compromised data, e.g., (1) types of personal information involved (*e.g.*, full name, Social Security number, date of birth, home address, account number, disability code, etc.) and number of individuals affected, (2) audit information or files related to security or IT audits, or (3) proprietary company information, etc.
- If an electronic file(s) is missing, does OAS have a backup copy?
- Location where incident occurred or is believed to have occurred.
- How was incident discovered?
- Was incident reported to law enforcement? If incident reported to law enforcement, what agency/department/city? Include contact information.
- Other pertinent information.

When connected to the OIG Intranet, the employee should use *SD-19A, Report of Suspected or Actual Loss, Compromise, or Theft of Personally Identifiable Information, OAS Sensitive Information, or Electronic Media*. (The SD-19A should never be emailed if service is not available through OIG Intranet (in an OIG office or through VPN.) Revised reports should be submitted as appropriate to report any additional information.

20-09-40-01-02 RIG and Headquarter Director Responsibilities

The RIG or Headquarters Director should provide a follow-up email with further details to the OIG ISSO, with a copy to the OIG CISO (ciso@oig.hhs.gov), within 12 hours of the incident. When possible, the RIG/Headquarter Director or designee should use *SD-19A, Report of Suspected or Actual Loss, Compromise, or Theft of Personally Identifiable Information, OAS Sensitive Information, or Electronic Media* and include any other information that may be pertinent. Revised reports should be submitted as appropriate to report any additional information.

20-09-50 COMPUTER INCIDENT DETECTION AND REPORTING RESPONSIBILITIES

OAS employees have the duty to report any suspected or confirmed "incident" or "security incident" in a timely manner to the local OMP System Administrator (typically the Regional Technical Officer (RTO)) help desk, the OIG ISSO at 202-205-9207 (office) or 888-415-8421 (toll free number) and complete a Computer Security Incident Report. Note: You must be connected to the OIG Intranet to access this report.

The *Information Security Handbook for OIG Information Users*, Chapter 4, *Incident Detection and Reporting,* defines:

- An "incident" as any occurrence, or appearance of a threat to an OIG computer system, or any activity, which involves using an OIG system in an improper manner.
- A "security incident" as a breach or attempted breach of security in an information system. "Breach of security" includes any unusual or apparently malicious break-in attempts (local or over a network), virus or network worm attacks, file or data tampering, unauthorized information access or disclosure, network router or gateway attacks. It also includes any incident where an individual (employee, contractor, other), whether directly or using a program, performs functions for which the individual is not authorized, or acts which violate or appear to violate criminal or civil statutes.

The Computer Security Incident Report must be used to capture both successful intrusions and mitigated attempts.

The report is reviewed by the local OMP System Administrator and ISSO. The local OMP System Administrator and the ISSO will determine the scope and magnitude of the incident and resolve the issue.

When reporting incidents, OAS employees should describe the problem and include contact information. Employees should not include potentially sensitive information such as passwords or other personal information unless specifically requested in the form. Any files, documents, or logs which may provide evidence or clues about the incident should be duplicated on removable media and preserved.

In addition, OAS employees should report incidents to their supervisor.

USE OF ELECTRONIC SCANNING TOOLS TO ASSESS VULNERABILITIES IN WIRELESS NETWORKS, WEB APPLICATIONS, LOCAL AREA NETWORKS, AND DATABASES

20-10-00 PURPOSE

This chapter establishes OAS policies and procedures for executing scanning tools used to assess vulnerabilities in wireless networks, web applications, local area networks, and databases.

20-10-10 STANDARDS

Auditors must use professional judgment and exercise reasonable care in planning and performing audits. Reasonable care involves acting diligently in accordance with applicable professional standards and ethical principles. These standards are found in Chapter 3 of *Government Auditing Standards*.

20-10-20 POLICY

It is OAS policy that:

- Auditors exercise reasonable care in planning and executing electronic scans.

  No audit manager will direct or authorize any employee to execute, nor will any employee execute, any scans on behalf of OIG without first receiving the appropriate training as determined by the Information Technology (IT) Audit Director.

- All scans require prior written approval of the:

  0 Cognizant Audit Manager
  0 IT Audit Director

- Auditors must obtain prior written permission (email is acceptable) from an authorized auditee official for all scans that have the potential to capture Personally Identifiable Information (PII), as defined by HHS Updated Departmental Standard for the Definition of Sensitive Information, dated May 18, 2009. These scans include: wireless network scans that may capture data, web application scans, local area network scans, and database scans.

20-10-30 BACKGROUND

Vulnerability assessment tools, such as scanners for wireless networks, web applications, local area networks, and databases, are essential tools needed to determine whether critical networks, systems, and applications have been properly configured, implemented, secured, and monitored. The use of these tools and the results must be documented and protected in accordance with OAS audit policies and procedures. (See Chapter 20-06, *Evidence and Audit Documentation*.)

These tools, if not used properly and in conformance with this policy, can result in inappropriate and unlawful identification, capture, and disclosure of sensitive information about an auditee's network, as well as the disclosure of PII or electronic protected health information (e-PHI) that could violate privacy and security laws and executive guidance, e.g., Federal Information Security Management Act, Privacy Act, and OMB circulars and memorandums.

20-10-30-01 Standard Model for Networking Protocols and Distributed Applications

The standard model for networking protocols and distributed applications is the International Standard Organization's Open System Interconnect (ISO/OSI) model. It defines seven network layers, as follows: Layer 1 – Physical; Layer 2 - Data Link; Layer 3 – Network; Layer 4 – Transport; Layer 5 – Session; Layer 6 – Presentation; and Layer 7 – Application.

Management information scans involve layers 1 and 2. Data scans involve layers 3 through 7. Data scans have the potential to capture data, e.g., PII.

20-10-40 DEDICATED NON-OIG IMAGED COMPUTERS

For all electronic scans, auditors must use dedicated non-OIG imaged computers that are whole disk encrypted, have a firewall, and have current virus protection. These dedicated computers must never be connected to the OIG network, and must have the latest patches and updates from applicable software companies before conducting scans.

20-10-50 ELECTRONIC VULNERABILITY ASSESSMENT PREPARATION AND PERFORMANCE

Before conducting an electronic scan an auditor must receive appropriate training and sign and submit an authorization form for approval. See SD-18, *Electronic Vulnerability Assessment Authorization Form*. See Section, 20-10-20, *Policy*, for the two required approvals and required auditee permissions for certain types of scans. The auditor is responsible for executing the scan in accordance with OAS policy and legal restrictions. Each region should designate a backup auditor to execute the approved scan. The backup auditor must have received appropriate training and be identified on the SD-18.

20-10-50-01 Documenting Wireless, Application, Local Area Network, and Database Scan

Auditors should document the scan procedures used and the results that were achieved. The scan results identify the vulnerabilities, reasons for the vulnerabilities and suggested remediation. This information should be shared and reviewed with the auditee to determine the validity of the potential finding. The vulnerability assessment reports generated by the scan applications should not be included as part of the audit report.

Auditors should always obtain and document the auditee‘s permission to conduct a scan.

PROTECTION OF SENSITIVE OFFICE OF AUDIT SERVICES INFORMATION

20-11-00 PURPOSE

This chapter establishes OAS policies and procedures for safeguarding sensitive information (both electronic and hard copy) that has been entrusted to OAS.

Sensitive OAS documents and information have the potential to damage government, commercial, or private interests if obtained by persons who do not have a need to know the information to perform their jobs. It is the responsibility of OAS and its employees to safeguard this information.

20-11-10 STANDARDS

The Office of Management and Budget (OMB) has established procedures for protecting sensitive information in OMB Memorandum *M-06-16, Protection of Sensitive Agency Information*.

For HHS, the definition of sensitive information is found in the HHS memorandum entitled *Updated Departmental Standard for the Definition of Sensitive Information, dated May 18, 2009.*

At HHS, sensitive information is information that has a degree of confidentiality such that its loss, misuse, unauthorized access, or modification could compromise the element of confidentiality and thereby adversely affect national health interests, the conduct of HHS programs, or the privacy of individuals entitled under The Privacy Act or the Health Insurance Portability and Accountability Act (HIPAA).

The standards for safe custody and retention of audit documentation are found in Chapter 3 of the *Government Auditing Standards*.

20-11-20 POLICY

OAS employees must:

- Complete mandatory annual security awareness training, per the *Rules of Behavior for Use of HHS Information Resources*.
- Annually review and sign the *Rules of Behavior for Use of HHS Information Resources.*
- Use sensitive information obtained or generated during the course of OAS activities only for official purposes.

- Protect sensitive information, whether in electronic files or hard copies, to prevent unauthorized access.

- Ensure that all OAS computing, mobile devices, and portable media containing sensitive information are encrypted.

- Not use CDs/DVDs to store sensitive information, except for TeamMate files maintained in the regional or divisional safes, without advance approval in writing from the Director, Information Technology Audit Division.

OAS requires all experts, consultants, or other OAS contractor employees/third parties with access to OAS information to execute a confidentiality agreement and whole disk encrypt all storage devices, including mobile devices, containing OAS information in accordance with Federal Information Processing Standard 140-2. See SD-20, Confidentiality Agreement form. If the access relates to an audit, the executed agreement will be maintained in TeamMate.

20-11-30 DEFINING SENSITIVE INFORMATION WITHIN OAS

Sensitive information includes, but is not limited to:

- Personally identifiable information (PII) is any information that can be used to distinguish or trace an individual's identity, such as name or social security number, or that when combined with other personal or identifying information is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. PII includes, but is not limited to medical records, billing records, payment records, claims adjudication records, and case or medical management records that include personal identifiers, e.g., names, Social Security Numbers, and Medicaid recipient numbers.

- Any audit information or files related to security audits, e.g., bioterrorism and counter terrorism.

- IT and other audits containing information that is considered privileged and confidential or prohibited from general disclosure by Federal, state, or local laws and regulations.

- Confidential information from law enforcement and judicial agencies (e.g., FBI, Office of the US Attorney) regarding criminal and civil cases, Federal grand jury information, and whistleblower and Qui Tam actions.

- Proprietary information such as wholesale drug pricing for pharmaceuticals.

- Administrative documents such as personnel files.

- Any information covered by policies set forth in the *OIG Administrative Manual*, Chapter 05-05, *Limited Official Use Information*.

- Any information, which, if inappropriately released, could cause embarrassment to the Federal government.

20-11-40 PROTECTION OF SENSITIVE INFORMATION

OAS employees frequently come into contact with and possess documents and/or electronic data containing PII or other sensitive information. Because of the sensitivity of

such information, the following measures for protecting sensitive information must be followed by all OAS employees.

20-11-40-01 Use of OIG Computers/ Blackberries and Personal Computers

OAS employees:

- Must ensure that firewall and antivirus protections on OIG provided computers remain active when processing data.
- Must ensure that OIG computers and Blackberries are only used by OIG employees. For example, when working at home, family members and friends must not be allowed to use OIG computers or Blackberries.
- Must not transfer audit information to non-OIG computers, devices, or systems, including personally-owned email accounts and removable media. This helps assure proper protection and compliance with HHS and OIG policies.
- Must be aware of their surroundings when using an OIG computer and take precautions to ensure that unauthorized individuals are not able to view sensitive information on the screen. This is particularly important in public places, e.g., lobbies, airports, airplanes, and trains.

20-11-40-02 Accessing OIG Systems and Networks

OAS employees:

- May only access OIG email using an OIG computer or OIG device.
- Must not use a personally-owned Blackberry, Smartphone, or cell phone to access OIG systems and network resources, including email.
- Must not use an auditee's wired or wireless network if the auditee is not an HHS OPDIV or is not connected to the HHS network.
- May use wireless network connections in an:[1]
    - Auditee's office,[2] only with an OIG supplied router (including MIFI card), aircard, or Blackberry (tethered or HotSpot).
    - HHS OPDIV office that is connected to the HHS network. The employee must enable OIG's Check Point VPN immediately after connecting to the HHS network and for the duration of the connection.
    - Hotel (guest and meeting rooms only) only when (1) a wired connection is not available, and (2) using an OIG supplied or personal wireless router, aircard, MIFI card, Blackberry or Smartphone is not possible. Always verify with the hotel front desk the name of the authorized access point provided by the hotel. The employee must enable OIG's Check Point VPN immediately after connecting and for the duration of the connection.

[1] Sometimes you will have poor high-speed or no Internet connectivity, such as when using a wireless card in remote areas or offices located inside of large buildings or in basements.
[2] Non-HHS OPDIV or HHS OPDIV which is not connected to the HHS network

- Home/apartment only with an OIG supplied or personal wireless router, or an OIG supplied MIFI card, Blackberry or Smartphone. OAS employees must ensure that their personal router is configured with WPA2 and AES encryption.[3] The passphrase for the WPA2 encryption must be at least 16 characters in length and include special characters, numbers, and both upper and lower case letters.

  The wireless network connections in an OIG provided computer should remain disabled until the OAS employee needs to use it. When it is no longer needed, the wireless network connection should be immediately disabled.

- May use wireless access on an OIG computer at public hotspots (e.g., airports, coffee shops, malls, and hotel lobbies) to access OIG systems and network resources, including email, only in urgent or emergency situations, and only when OIG cellular hotspots, blackberry hotspots, and blackberry tethering is unavailable. OAS employees must *immediately* establish the OIG Check Point VPN after connecting to the network and ensure the VPN remains connected for the duration of the connection.

- Must not download files from OIG systems and networks to:

  - An auditee's computer to read, or transfer file attachments from an auditee's computer to an OIG computer.

  - A USB drive, CD/DVD, iPod, MP3, etc. using an auditee's computer.

- Must not connect non-OIG computers, devices and equipment, including personally owned devices (e.g., tablet computer, Blackberry, Smartphone, USB drive, or external hard drive) to OIG's networks or systems without written permission from the OIG CISO.

20-11-40-03 Hard Drives in Computers, External Hard Disks, and USB Drives

OAS employees:

- Must treat all electronic media as if they contain sensitive information and safeguard the media accordingly. This is due to the scope of information OAS considers sensitive and the volume of information electronic media can contain in hidden files. There is one exception to this rule: Software used on IT audits may be kept on unencrypted media.

- Must whole disk encrypt all hard drives on laptop and desktop computers, and all external hard drives, including NetDisk. However, devices that are free of data are not required to be encrypted until they are distributed to staff.

- Must use only OAS authorized USB drives. OAS uses two types of USB drives - those that have:

  - Hardware-based encryption that does not require any special software to protect data. Staff can use these devices to store any data and they can be used to perform data exchange with an auditee. Note: Now that OAS uses hardware-based encrypted USB drives, OAS no longer allows use of any partially

[3] If the wireless network is not encrypted, the network has become a public access point for anyone in the area.

encrypted drives.

- Software-based encryption that staff must use to whole disk encrypt the USB drives with PGP before they are used. These drives are for OAS internal use only and should not be used to exchange data with auditees or others.

- Should request auditees to consider the need to protect data before providing files to OAS via the auditee's USB drive or CD/DVD. Considerations include whether the:

  - Auditee's USB drive is hardware-based encrypted.

  - Auditee has the ability to encrypt with a program that OAS can use to read the encrypted file(s), for example PGP.

  - Transfer of data will be in the presence of auditee staff and electronic media returned to the auditee upon transfer.

  Alternatives to using the auditee's USB drive to transfer data to OAS include using an OAS hardware-based encrypted USB drive or using the HHS/OIG Delivery Server. See 20-11-40-06-02, *Authorizing Non-OIG Organizations to Use the HHS/OIG Delivery Server to Transfer Electronic Files Containing Audit and/or Sensitive Information Over the Internet to OAS*.

Instructions for encrypting computers (desktop & notebooks), external hard drives, including NetDisk, and USB (Jump) drives are available on the Intranet.

20-11-40-04 Securely Locking Computers When Unattended During the Work Day

OAS employees must follow OIG policies regarding using the Ctrl-Alt-Delete key sequence to lock laptops and desktops when stepping away from OIG computers, particularly at non-OIG office locations. See *Information Security Handbook for OIG Information Users*, Appendix A: *Standards of Use*, Item 5, *Workstation Locks*.

Once the computer is turned on and the encryption password has been entered, the computer is no longer encrypted and is relying on the protection of the Windows login. Leaving a computer turned on and Windows unlocked, especially at an auditee's office or in a public area, puts any information on that computer at risk of being copied by hacking tools and accessible if the computer is stolen.

20-11-40-04-01 In an OIG Office

When in an OIG office, OAS employees should not turn off the computer before leaving for the evening – but should "Log Out." OMP needs computers powered on at night with staff logged out so OMP can update computers as needed. As requested by local OMP staff, "Reboot" and Log in to "PGP" only, i.e., enter your pass phase for your computer directly after rebooting the computer. Do not enter your Windows password. This will allow any patches that require a reboot to fully install.

20-11-40-04-02 Not in an OIG Office

When not in an OIG office, OAS employees should turn off the computer before leaving the computer unattended for an extended period, e.g., going to lunch, attending a meeting, or overnight. Encryption only protects information on laptops when the machine has been turned off.

20-11-40-05 Sharing Electronic Files with the Auditee and Other Non-OIG Entities During the Audit

The audit team should use its judgment whether to convert electronic files that are shared outside the OIG to PDF. Other routine correspondence during the audit is not normally converted to PDF. Distribution of audit reports is discussed in Chapter 30-04, *Distribution of HHS Produced Audit Reports*, Subsection, 30-04-20-02 *Electronically Distributing DIG, AIG, and Regionally-Issued Draft and Final Audit Reports, Including Special Audits*.

For those files converted to PDF, the source file must not be attached to the PDF and notes in the source document must not be converted to comments. Before electronically converting an electronic file to PDF, the audit team should run a metadata removal tool for Word, Excel and PowerPoint files.

When sharing an electronic file that has not been converted to PDF outside the OIG, the audit team should exercise caution that the electronic file does not contain any hidden data that the audit team does not intend to share.

Such hidden data may include:

- Comments and track changes that may not be displayed.
- Hidden text, worksheets, data columns, and data rows.
- Embedded objects such as Excel worksheets, drawing objects, and pictures.
- PowerPoint speaker notes.

If OAS employees are unsure about procedures to remove hidden data from electronic files, they should contact AATS staff for assistance.

20-11-40-06 Securely Transferring Electronic Files Containing Audit and/or Sensitive Information Over the Internet or Intranet

OAS employees:

- Must use the HHS/OIG Delivery Server to (1) transfer files *outside* the OIG containing audit and/or sensitive information[4] regarding a planned or active audit, or OI or Department of Justice (DOJ) assist work, or (2) transfer large files *inside* or *outside* the OIG. Required use of the HHS/OIG Delivery Server does not include secure applications accessed by OAS directly from an HHS OPDIV, State's or Contractor's information system. These information systems may also allow for secure data transfer, which is acceptable.

  For the purposes of this section, audit information:

  - Includes audit start notices, engagement letters, and requests for information regarding:

    - Homeland security audits – security reviews that cover particularly sensitive topics, e.g., select agents, bioterrorism, and classified or potentially classified information.

[4] For definition, see Section, 20-11-30, *Defining Sensitive Information Within OAS*.

- Information technology systems audits, e.g., Federal Information Security Management Act audits.

- OI or DOJ assist work.

- Includes any file, whether the file contains sensitive information or not, sent to an auditee or others outside the OIG regarding a planned or active audit, or OI or Department of Justice assist work. This includes, but is not limited to, data obtained during the course of an audit or assist work and sent to the auditee or others for confirmation or comment.

- Includes all *Early Alerts of Significant Preliminary Findings*, discussed in Chapter 30-01, *Memorandums to Management*.

- Includes all draft audit reports except those sent to OPDIVs. Draft reports to OPDIVs that are restricted or limited official use should be sent via delivery server.

- Includes all *Memorandums of Impending Release,* discussed in Chapter 30-01, *Memorandums to Management,* regarding restricted or limited official use final reports.

- Includes all restricted final reports, e.g., homeland security audits, information technology systems audits, and OI or DOJ assist work.

- Includes limited official use final reports, e.g., recipient capability, bid proposal and contract closeout audits.

- Does not include:

  - Audit start notices, engagement letters, request for information regarding unrestricted audits, e.g., Medicare or Medicaid audits, or non-sensitive recipient capability, bid proposal, and contract closeout audits.

  - *Memorandums of Impending Release,* discussed in Chapter 30-01, *Memorandums to Management,* regarding unrestricted final reports.

  - Unrestricted final audit reports.

  - Communications that do not deal with audits, OI or DOJ assist work, sensitive information, and do not contain any personally identifiable information, e.g., communications with members of the Association of Government Accountants, Intergovernmental Audit Forum or President's Council on Integrity and Efficiency.

- May use either Microsoft Outlook or the HHS/OIG Delivery Server to transfer files *inside* the OIG.

- Must request government and non-government organizations to send files that contain audit or sensitive information to OAS using the HHS/OIG Delivery Server. If an auditee has a secure transfer site that they wish to use to transfer files to or from OIG, OAS employees must consult their local AATS/IT manager before using.

If an OAS employee receives unencrypted sensitive information, except via the HHS/OIG Delivery Server, the employee must report the incident to the appropriate

RIG/AIG. This does not apply to receiving files via a CD/DVD or an USB drive while on-site.

Caution: When using the HHS/OIG Delivery Server keep the narrative part of the body of the email as brief as possible and do not include any sensitive information in it. The recipient(s) receives the email, with the body of the email unencrypted, and with a download link(s) in lieu of an attachment(s). The recipient(s) then clicks on the link(s) to download the files from the HHS/OIG Delivery Server. Only the accessed files are encrypted and secure.

20-11-40-06-01 Sending Files Outside the OIG

When transferring files outside the OIG, OAS employees must ensure the email address is correct and current before the OAS employee sends any information.

20-11-40-06-01A Files That Contain Audit and/ or Sensitive Information

When transferring files outside the OIG that contain audit and/or sensitive information, OAS employees must request the recipient to send the OAS employee an email before the OAS employee sends any information. This allows the OAS employee to copy and paste the email address into the HHS/OIG Delivery Server or Microsoft Outlook, thus avoiding the possibility of sending information to an unintended recipient.

OAS employees must:

- Use the HHS/OIG Delivery Server to transfer files that contain audit and/or sensitive information outside the OIG. Since the HHS/OIG Delivery Server only encrypts attachments, sensitive information should not be contained in the subject or body of the email itself.

  Note: OAS no longer requires encrypting files with PGP, or other software, when transmitting files *outside* the OIG via the HHS/OIG Delivery Server.

- Include instructions if the recipient needs the email resent, contact information for the staff transmitting the files, and the standard OIG email disclaimer.

20-11-40-06-01B Files That Do Not Contain Audit and/or Sensitive Information

OAS employees may use the HHS/OIG Delivery Server or Microsoft Outlook to transfer files outside the OIG if the files do not contain audit and/or sensitive information.

20-11-40-06-02 Authorizing Non-OIG Organizations to Use the HHS/OIG Delivery Server to Transfer Electronic Files Containing Audit and/or Sensitive Information Over the Internet to OAS

OAS employees should authorize non-OIG organizations to send a file(s) that contains audit *and/or sensitive inf*ormation, including PII, to OIG via the HHS/OIG Delivery Server. Since the HHS/OIG Delivery Server only encrypts attachments, sensitive information should not be included in the subject or body of the email itself. If an auditee has a secure transfer site that they wish to use to transfer files to or from OIG, OAS employees must consult their local AATS/IT manager before files are sent using the auditee's transfer site.

20-11-40-06-03 Sending Files Inside the OIG Using the HHS/OIG Delivery Server

Using the HHS/OIG Delivery Server, OAS employees can securely transfer any file type, including ".exe," ".mdb," ".tmb" and ".zip."

This includes all TeamMate files transferred between OAS Field and Regional offices, e.g.:

- TeamMate replicas created during the audit.
- TeamMate finalized audits.

20-11-40-06-04 Technical Guidance - Using the HHS/OIG Delivery Server and PGP

Technical guidance is available in the following documents:

- *Instructions for Using the HHS/OIG Delivery Server – Transferring Files Outside the OIG and Large Files Over the Internet/Intranet* – published by OAS.
- *Instructions to Request File(s) from Non-OIG Organizations Via the HHS/OIG Delivery Server - for OAS Employees Use Only* - published by OAS.
- *Instructions to Send File(s) to the U.S. Department of Health and Human Services, Office of Inspector General Via the HHS/OIG Delivery Server* - published by OAS.

  Accellion: Sending email with large file attachments Instructions - published by OMP.
- *Instructions for Creating and Opening PGP Self Decrypting Archives (SDAs)* - published by OAS.

OAS employees can consult with AATS staff for current technical requirements.

20-11-40-07 Email and Fax Disclaimers and Special Notice

All email, including those sent via HHS/OIG Delivery Server or Blackberry, and FAX transmissions that originate from OAS, regardless of destination, should include a general disclaimer at the end of the email or fax.

In lieu of the general disclaimer, all files sent outside the OIG, e.g., correspondence with law enforcement agencies or external peer review teams, containing sensitive, non-public information, such as PII or proprietary information, in addition to being encrypted must contain a special notice at the beginning of the email. See Section 20-11-30, *Defining Sensitive Information within OAS*, for the scope of information OAS considers sensitive.

20-11-40-07-01 General Email and Fax Disclaimer

Email disclaimer:

> This email may contain confidential and/or privileged information. If you are not the intended recipient (or have received this email in error) please notify the sender immediately and destroy this email. Any unauthorized copying, disclosure, or distribution of the material in this email is strictly forbidden.

FAX disclaimer:

> This FAX may contain confidential and /or privileged information. If you are not the intended recipient (or have received this FAX in error) please notify the sender immediately and destroy this FAX. Any unauthorized copying, disclosure, or distribution of the material in this FAX is strictly forbidden.

20-11-40-07-02 Files Transmitted Outside the OIG Via Delivery Server That Contain Sensitive, Non-Public Information

In addition to using the delivery server to send files that contain sensitive, non-public information, such as PII or proprietary information, emailed outside the OIG, the following notice must be placed at the top of the delivery server email.

Special Notice:

> NOTICE: THIS FILE CONTAINS HIGHLY SENSITIVE, NON-PUBLIC INFORMATION. SAFEGUARD TO PREVENT ACCESS BY UNAUTHORIZED PERSONS. UNAUTHORIZED RELEASE MAY BE A VIOLATION OF FEDERAL REQUIREMENTS TO PROTECT PERSONALLY IDENTIFIABLE INFORMATION. DO NOT REPRODUCE OR RELEASE TO ANY PARTY WITHOUT EXPRESS PRIOR WRITTEN APPROVAL OF THE HHS DEPUTY INSPECTOR GENERAL FOR AUDIT SERVICES.

20-11-40-08 Fax Transmissions and Reproduction

OAS employees must not use hotel, personal, or commercial fax and copy machines to transmit or reproduce audit and/or sensitive information.

OAS employees may fax or reproduce sensitive documents on Federal government-owned equipment or equipment belonging to the owner of the information.

20-11-40-09 Electronic Data Mailed or Removed from OIG Offices or Audit Sites

If necessary, OAS employees can send or receive hard copy documents or encrypted electronic media (e.g., a jump drive) via the U.S. mail (Express, Certified, or Registered Mail) or OIG approved common carrier. OAS employees should keep a backup of sensitive electronic data and an inventory of sensitive hard copy data sent.

OAS employees must provide the passphrase (if applicable) directly to the recipient. OAS employees must not include the pass phrase in:

- The recipient's voice mail
- A file on the USB drive.
- A document transmitted with the USB drive.
- The body of an email.

OAS employees must never:

- Email unencrypted electronic data or encourage an auditee to do so.
- Mail encrypted or unencrypted electronic data or encourage an auditee to do so.
- Hand carry unencrypted electronic data to or from an auditee's office.

Note: If the recipient has an email address, use the HHS/OIG Delivery Server, as described in Subsection 20-11-40-06, *Securely Transferring Electronic Files Containing Sensitive Information over the Internet or Intranet*, to transfer electronic files.

20-11-40-10 Traveling with Sensitive Information

Sensitive information may be hand carried outside an OAS office as long as the person carrying the electronic media/document can control access to the electronic media or hard copy document being transported. Electronic media must be encrypted. For example, if the auditee provides an OAS employee unencrypted data while on-site, the employee should transfer the data to an encrypted OAS laptop computer or USB drive prior to leaving the auditee's office.

OAS employees must turn off laptop computers before packing them for travel. (The wireless network connection should be disabled before turning off the computer.) If an employee is required to turn on a laptop computer for airport security screeners, the employee must shut the computer down promptly afterwards. Once the encryption password has been entered when the computer is turned on, the laptop computer is no longer encrypted and is relying on the protection of the Windows login.

20-11-40-10-01 Checked Luggage

OAS employees should not store computers or sensitive information, whether on electronic media or hard copy, in checked luggage when traveling. If the weight or volume of the computer, electronic media, or hard copy documentation makes it impractical for an OAS employee to carry it and maintain it under the employee's direct control at all times, it should be sent via U.S. mail or OIG approved common carrier.

20-11-40-10-02 Vehicle

OAS employees should not leave computers or sensitive information in a vehicle, including in the trunk, overnight. OAS employees should not store a computer or sensitive information in a vehicle where it is visible. When renting a vehicle, while in travel status, consider this requirement if you think you temporarily may need to store computers or sensitive information in a vehicle during the day.

20-11-40-11 Prohibition of Sending TeamMate Files to the TeamMate Vendor

OAS employees must not send TeamMate files to the TeamMate vendor.

20-11-40-12 Destruction of Sensitive Information

When sensitive files are no longer needed, whether on electronic media or in hard copy, they should be destroyed.

Before discarding any information, OAS employees should consult OIG's Records Schedule and policy as set forth in Chapter 20-06*, Evidence and Audit Documentation*,

Section 20-06-120, *Retention*. If they have any questions, OAS employees should talk to their supervisors about records management, data security, and disposing of data.

OAS employees must properly destroy electronic media and hard copy documents. OAS employees must not discard electronic media in trash receptacles. Electronic media (e.g., USB drives and hard drives) should be sanitized by OMP. CDs/DVDs and hard copy documents should be shredded.

All excess/defective computers, hard drives (internal and external), Blackberries and USB drives must be returned to OMP to be sanitized, i.e., all data completely destroyed so that even file recovery software cannot recover the data. OMP will dispose of these items.

20-11-50 Storing Sensitive Information on CD or DVD

Employees may store sensitive information on CD or DVD without obtaining prior approval from the Director, Information Technology Audit if the CD or DVD is created in an OAS divisional or regional office for the sole purpose of backing up audits on the TMArchive Server.

Employees must obtain prior approval from the Director, Information Technology Audits in all other circumstances.

20-11-50-01 Safeguarding Sensitive Information Stored on CD or DVD

The following steps should be taken to safeguard sensitive information stored on CD or DVD:

- Encrypt, with the self-decrypting archive (SDA) feature of PGP, all data, including TeamMate files, before copying it to the CD or DVD.

- CD or DVD Stored in Safe – The CD or DVD with the encrypted files must be stored in the divisional or regional safe and should never be left unattended if removed from the safe. The CD or DVD must be returned to the safe and never be removed from the divisional or regional office.

- CD or DVD Provided to Entities Outside OIG – The CD or DVD with the encrypted files must be hand delivered by OAS staff and should not be mailed through USPS or common carrier, without advance approval in writing from the Director, Information Technology Audits. The approval must be retained in the TeamMate file.

PROPERLY SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION TRANSMITTED TO OAS OVER THE INTERNET AND ACTIONS REQUIRED WHEN INCIDENTS OCCUR

20-12-00 PURPOSE

This chapter establishes OAS policies and procedures regarding:

- Notifying auditees, OPDIVs, organizations,[1] and persons (third parties) contacted for information during the course of an audit how to properly safeguard personally identifiable information[2] (PII) transmitted to OAS over the Internet.
- Action required when OAS receives unprotected PII within an email (i.e., where unencrypted PII is contained within an email message or attachment) from any third-party that OAS has:
  - Provided with instructions on how to protect PII.
  - Not provided with instructions on how to protect PII.

20-12-10 STANDARDS

The standards for protecting PII and reporting incidents involving the breach of PII are found in OMB Memorandums:

- M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*.
- M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

[1] The term organization includes but is not limited to CMS business partners. A CMS business partner (contractor) is a corporation or organization that contracts with CMS to process or support the processing of Medicare fee-for-service claims. These business partners include Medicare carriers, Fiscal Intermediaries, Common Working File (CWF) host sites, standard claims processing system maintainers, regional laboratory carriers, claims processing data centers, Data Centers, Enterprise Data Centers (EDCs), and Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors (DMEMAC) and A/B Medicare Administrative Contractors (ABMAC).

HHS procedures for reporting and responding to incidents involving the breach of PII by third-parties are found in HHS Privacy Incident Response Team guidance: *Unprotected Personally Identifiable Information in Email from a Third-Party*.

20-12-20 IDENTIFYING PERSONALLY IDENTIFIABLE INFORMATION

PII is any information that can be used to distinguish or trace an individual's identity, such as name or social security number, or that when combined with other personal or identifying information is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. PII includes but is not limited to medical records, billing records, payment records, claims adjudication records, and case or medical management records that include personal identifiers, e.g., names, Social Security Numbers, and Medicaid recipient numbers.

20-12-30 POLICY

OAS employees must:

- Provide information about the approved method for securely transmitting electronic information, including PII, to OAS to the following:
    - OPDIV audit liaisons for all new assignments that will have reports addressed to OPDIV headquarters officials. See Section 20-01-50, *Audit Start Notices*. A template for preparing an audit start notice is available on the OAS Intranet.
    - Third-parties contacted for information during an audit. See Section 20-01-60, *Audit Notification Letters*. Templates for preparing audit notification letters are available on the OAS Intranet.
- Provide OPDIV audit liaisons and third parties:
    - Instructions for using the HHS/OIG Delivery Server.
- Remind auditees at the entrance conference, as needed throughout the audit, and at the exit conference of the approved method for securely transmitting information containing PII, to OAS over the Internet.
    - Reply to the sender of any PII not sent to OAS via the HHS/OIG Delivery Server or other approved transfer site as specified in Subsection 20-12-50, *Reply to the Sender.*
    - Report the receipt of PII not sent to OAS via the HHS/OIG Delivery Server or other approved transfer site as specified in *Subsection 20-12-60, Reporting Receipt of PII Not Sent to OAS via the HHS/OIG Delivery Server or Other Approved Transfer Site.*

20-12-40 AUTHORIZING NON-OIG ORGANIZATIONS TO USE THE HHS/OIG DELIVERY SERVER TO TRANSFER ELECTRONIC FILES CONTAINING PERSONALLY IDENTIFIABLE INFORMATION OVER THE INTERNET TO OAS

OAS employees should authorize non-OIG organizations to send a file(s) that contains PII to OIG via the HHS/OIG Delivery Server. Since the HHS/OIG Delivery Server only encrypts attachments, PII should not be included in the subject or body of the email itself. If an auditee has a secure transfer site that they wish to use to transfer files to or from OIG, OAS employees must consult their local IT audit manager before files are sent using the auditee's transfer site.

20-12-50 REPLY TO THE SENDER

There are two general scenarios when OAS may receive PII via email and will need to reply to the sender.

I. OAS has previously provided the third-party with instructions on how to protect PII but the third-party sent PII to OAS via email.

Reply to the sender with a restatement of PII protection requirements and instructions for using the HHS/OIG Delivery Server. A template for replying to the sender is available on OAS's Intranet. When responding to the sender, remove the unprotected PII found in the attachment or email body from the original message OAS received.

II. Receipt of PII was not anticipated (e.g., PII sent from a member of the public) and OAS has not previously provided the third-party with instructions on how to protect PII.

Reply to the sender with a statement to raise awareness of the importance of protecting PII and provide instructions on how to request authorization to use the HHS/OIG Delivery Server to securely send information to OAS. A template for replying to the sender is available on OAS's Intranet. When responding to the sender, remove the unprotected PII found in the attachment or email body from the original message that OAS received.

20-12-60 REPORTING RECEIPT OF PERSONALLY IDENTIFIABLE INFORMATION NOT SENT TO OAS VIA THE HHS/OIG DELIVERY SERVER OR OTHER APPROVED TRANSFER SITE

An employee must report the receipt of PII transmitted to OAS over the Internet if it is not encrypted or if the encryption method used does not meet the requirements of FIPS 140-2 (e.g., files encrypted with Microsoft Word or Excel, WinZip). The employee should notify the appropriate management officials, as outlined below.

20-12-60-01 Staff Responsibilities

Within 1 business day of the receipt of PII transmitted to OAS over the Internet, OAS employees must take the following actions by email:[3]

- Regional employees must notify their RIG, or designee, and
- Divisional and headquarters (HQ) employees must notify their HQ Director, or designee

The reporting employee should include as much pertinent information about the incident as possible in the report, e.g.:

- Date and time the incident was discovered

[3] During business hours, employees may report incidents via telephone discussion (not voice mail) with email follow-up. During non-business hours they should send emails, if service is available through OIG Intranet (in an OIG office or through VPN); otherwise, employees should leave a voice mail and follow-up with telephone discussion (not voice mail) the next business day.

- Type of entity that used email to transmit PII to OAS instead of using the HHS/OIG Delivery Server or other FIPS 140-2 compliant appliance. Types of entities include:
  - CMS Business partner (contractor)
  - Educational institution
  - HHS OPDIV (non-OIG)
  - Indian tribal government
  - Local government
  - State government
  - Other non-Federal organization
  - Other Federal agency – not HHS
  - Member of the general public

- General Information about the entity or person that used email to transmit PII (when known), such as:
  - Name
  - Title
  - Organization
  - Address
  - Email
  - Phone number

- The nature of compromised data, e.g., medical records, billing records, payment records, claims adjudication records, and case or medical management records that include personal identifiers, e.g., names, Social Security Numbers, and Medicaid recipient numbers. Indicate the number of individuals affected.

- If all or some of the data in the email was encrypted with a method that did not meet the requirements of FIPS 140-2, identify (if possible) the program used to encrypt the data, e.g., Microsoft Word or Excel, WinZip, etc.

- Confirmation that the third-party has been provided with instructions for sending PII to HHS via email in a protected manner and any other mitigation steps taken.

When connected to the OIG Intranet, the employee should use *SD-19B, Report of Receipt of PII not sent to OAS via the HHS/OIG Delivery Server or Other Approved Site*. (The SD-19B should never be emailed if service is not available through OIG Intranet (in an OIG office or through VPN.) Revised reports should be submitted as appropriate to report any additional information.

20-12-60-02 RIG and Headquarters Director Responsibilities

Within 1 business day of being notified by staff of the receipt of PII transmitted to OAS over the Internet, the RIG or HQ Director, or designee, will notify:

- The ISSO at (isso@oig.hhs.gov), or 202-205-9207 (office) or 888-415-8421 (toll free number), and a copy to the OIG CISO (ciso@oig.hhs.gov). A separate telephone call is not required if you send an email.

- The OAS Incident Notification Team (OAS-Incident-Notification@oig.hhs.gov). A separate telephone call to members of the OAS Incident Notification Team is not required.

When possible, the RIG or Headquarters Director, or designee, should use *SD-19B, Report of Receipt of PII not sent to OAS via the HHS/OIG Delivery Server or Other*

Approved Site and include any other information that may be pertinent. Revised reports should be submitted as appropriate to report any additional information.

Part III

Reporting Chapters

INFORMING DEPARTMENT OFFICIALS ABOUT SIGNIFICANT PRELIMINARY FINDINGS AND SIGNIFICANT AUDITS OF EXTERNAL ENTITIES

30-01-00 PURPOSE

This chapter establishes policies and procedures for preparing memorandums to inform Department officials about significant preliminary findings and, significant audit reports on States, contractors, grantees, or other entities that are not part of the Department (external entities).

30-01-10 STANDARD

Chapter 6 of the *Government Auditing Standards* contains the fieldwork requirements for performance audits. It states that for some matters early communication to those charged with governance or management may be important because of their relative significance and the urgency for corrective follow-up action. Further, when a control deficiency results in noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse, early communication is important to allow management to take prompt corrective action to prevent further noncompliance.

Chapter 7 of the *Government Auditing Standards* contains the reporting requirements for performance audits. It requires communicating the results of audits to those charged with governance, appropriate officials of the audited entity, and appropriate oversight officials.

30-01-20 POLICY

It is OAS policy to prepare memorandums to management, as covered in this chapter, which will:

- Provide the Secretary, OPDIV heads and other departmental officials with an early alert of significant preliminary findings. (Section 30-01-30)

- Alert OPDIV heads and other departmental officials to significant audit matters before the impending release of a final report issued to a State, contractor, grantee, or other external entity that deals with significant audit matters. (Section 30-01-40)

See Exhibit 30-01-A for a *Summary of Selected Requirements for Memorandums to HHS Management*.

OAS policy with regard to public release of memorandums to management is as follows:

- Early alerts of significant preliminary findings will generally be posted on the Internet.

- Memoranda of impending release will generally not be posted on the Internet.

30-01-30 EARLY ALERT OF SIGNIFICANT PRELIMINARY FINDINGS – SHORT TITLE "EARLY ALERT"

Early alerts provide a mechanism for alerting the Secretary, OPDIV heads and other departmental officials of significant preliminary findings, both internal (such as a program deficiency) and external (such as those relating to a contractor, grantee, or other external entity). These memorandums usually will not contain recommendations.

An early alert should be used in those instances where the team plans to issue an audit report after fieldwork is completed, but timely communication of significant problems is necessary to enable the Department to take corrective action immediately.

In some cases an early alert may not be appropriate. For example, if problems are identified late in the audit process it may be more appropriate to wait and report them in the audit report, rather than delaying the report to issue a memorandum.

30-01-30-01 Decision to Prepare an Early Alert

The audit team should consider preparing an early alert if the findings involve any of the following conditions and require the immediate attention of, or action by, the OPDIV:

- significant program violations,
- a significant threat to health or safety,
- questions of law and maladministration, or
- potential significant internal control weaknesses.

The RIG should contact the appropriate AIG to determine whether to prepare an early alert.

30-01-30-02 Preparation and Content

Consistent with *The Audit Process*, the team should hold a team meeting to discuss the framework and focus of the early alert. The memorandum should be prepared by the RIG and the audit team with input from the appropriate AIG.

The early alert should be concise, informative, and self-contained. It should contain sufficient background information and be written in nontechnical terms so that readers can readily understand the preliminary finding. The memorandum should usually not exceed five pages exclusive of any appended material.

The following information should generally be in an early alert:

- The subject line should include the full title of the early alert and the Common Identification Number (CIN), which should not be the same CIN assigned to the associated audit.

- The first paragraph should state "The purpose of this memorandum is to alert you to a preliminary finding relating to our audit of..." and should include a brief explanation of why the audit was done and the audit objective relative to the preliminary finding that is the subject of the alert.

- A brief description of the program under review.

- The period covered by the audit.
- Evidence that supports the preliminary finding or potential significant internal control weakness with reference to program regulations or legislation. Regulations generally should not be quoted.
- The program dollars audited, or for external reviews, Federal funding received by the auditee and the amount audited.
- For potential significant internal control weakness, the basis for believing that the effect of the weakness is likely to be significant.
- A statement that the information in the early alert is preliminary, the audit is continuing, and OIG will issue a draft report at the conclusion of audit.
- The statement "Any questions or comments on any aspect of this memorandum are welcome. Please call me or have your staff contact...." should appear at the end of the memorandum and should contain the name, telephone number and email address of the appropriate AIG or RIG.

30-01-30-03 Review by Department and Auditee Officials

Department or OPDIV officials should be provided an opportunity to comment on the factual accuracy of any early alert that will be posted on the Internet. When the auditee is not the Department or an OPDIV, the auditee should also be provided an opportunity to comment on the factual accuracy of the early alert.

30-01-30-04 Addressees, Signatories, and Headquarters Review

The early alert should be addressed to the Secretary, OPDIV heads, or other departmental officials. Copies should also be sent to the regional OPDIV when appropriate.

The early alert should be signed by the IG, DIG, or AIG as determined by the DIG.

All early alerts should be submitted to the Division. The AIG will determine the need for review by the Headquarters Review Team; however at a minimum a Headquarters Review Team editor will edit the early alert.

30-01-30-05 Public Release/Internet Posting

Early alerts will be posted on the Internet unless the audit team anticipates that the related audit report will be restricted or the DIG approves restricting the early alert based on justification provided by the audit team.

30-01-40 MEMORANDUM OF IMPENDING RELEASE – SHORT TITLE "MIR"

A MIR is used to keep the OPDIV and other departmental officials informed about significant audit reports issued to external auditees such as States, grantees, and contractors. A MIR will be issued to the OPDIV within 5 business days before the release of a final report dealing with significant audit matters.

30-01-40-01 Preparation and Content

The RIG and the audit team should prepare a MIR when a final report issued to an entity outside the Department contains significant audit matters. Significant audit matters are defined as:

- Significant program violations, significant threats to health or safety, politically sensitive issues, or questions of law and maladministration that require the immediate attention of, or action by, the OPDIV.

- Findings of a controversial nature; known congressional, media, or IG interest; and management findings that reflect seriously on the overall efficiency of administration of HHS funds or precedent-type issues.

- Significant prospective monetary savings or proposed significant monetary adjustments.

Section 30-02-40-01, IG- and DIG-Signed Reports and Memoranda of Impending Release contains specific criteria for IG- and DIG-signed memoranda of impending release.

The MIR should contain the following information:

The subject line will include the full title of the report and the report number. The first paragraph should briefly state why the audit was done, and that the report will be issued within 5 business days of the date of the memorandum.

The first two sentences should read:

> Attached is an advance copy of our final report on [subject of report]. We will issue this report to [the auditee] within 5 business days. [If the review was requested, indicate by whom. If the review was mandated by law, indicate the law and the mandate. Do not indicate that the review was self-initiated.]

The final paragraph should include contact information in the format presented below.

> If you have any questions or comments about this report, please do not hesitate to call me, or your staff may contact [AIG or RIGs name and title,] at (XXX) XXX-XXXX or through email at [email address] or [RIG's name and title if not previously provided,] at (XXX) XXX-XXXX or through email at [email address]. Please refer to report number A-XX-XX-XXXXX.

30-01-40-02 Addressees, Signatories, and Headquarters Review

The MIR is addressed to OPDIV heads or other departmental officials and can be signed by the IG, DIG, or AIG, as decided by the DIG.

The RIG should submit the MIR to the Headquarters review team with the related final report.

30-01-40-03 Public Release/Internet Posting

The MIR should not be posted on the Internet without approval from the DIG.

Exhibit 6-30-01-A

Summary of Selected Requirements for Memorandums to HHS Management

	Early Alert of Significant Preliminary Findings	Memorandum of Impending Release
Addressed To		
Secretary, OPDIV Head or other Department Official	As Appropriate	As Appropriate
Copy To		
Department Officials or Regional OPDIV Official	As Appropriate	As Appropriate
Prepared By	RIG[1 & 2]	RIG[2]
Reviewed By	HQ Review Team	HQ Review Team
Approved By	Appropriate AIG	Appropriate AIG
Signed By	IG, DIG, or AIG	IG, DIG, or AIG
For Further Information Contact	Appropriate AIG or RIG	Appropriate AIG or RIG
Length	Usually No Longer Than Five Pages[3]	Usually No Longer Than One Page[3]

Notes

1. Consistent with *The Audit Process*, a team meeting should be held to discuss the framework and focus of the memorandum.
2. For audits conducted by the Headquarters Division, the memorandum should be prepared by the cognizant director.
3. Exclusive of any appended material.

REPORTING ON RESULTS OF AUDITS

30-02-00 PURPOSE

This chapter establishes policies and procedures for preparing OAS audit reports.

This chapter discusses:

- Sharing audit results before issuing a draft report.
- Who should sign a transmittal memorandum, a memorandum of impending release (MIR), or a transmittal letter.
- When Headquarters Review Team review of a report is required.
- The report format, including required disclosures.
- Reporting audit objectives, scope, and methodology, as well as any scope impairments.
- Reporting audit findings, recommendations, auditee comments, and OAS response to those comments.
- Issuing Public Summaries for restricted reports (see Chapter 30-02-70 for more information on Public Summaries).

The *OAS Style Manual* contains information about writing conventions and an example of the OAS report format.

30-02-10 POLICY

OAS must issue audit reports communicating the results of each completed audit.

OAS policy is to involve team members in developing the report. Consistent with *The Audit Process*, team meetings should be held among assigned team members before drafting the report and during the writing of the report as necessary. The focus of these meetings is to ensure that team members fully understand and agree on the audit objective(s), finding(s), and recommendation(s).

In addition, team members should ensure that the report:

- Complies with *Government Auditing Standards*.
- Complies with the Plain Writing Act of 2010. Guidance for complying with this Act can be found in OMB Memorandum M-11-05, which references the Federal Plain Language Guidelines. Additional information about complying with the Plain Writing Act and examples of plain language can be found on the Website for PlainLanguage.gov.
- Provides management with a timely, written record of audit results.
- Provides the reader, at the outset, with a summary of audit results that is balanced to highlight positive as well as negative audit results.
- Clearly communicates the audit objective(s), scope, and methodology.
- Includes fully developed findings that contain the appropriate attributes, e.g., condition, criteria, effect, cause, and recommendation.
- Presents supporting evidence that is accurate and fair.
- Includes sufficient facts to provide a basis for conclusions and recommendations.
- Reports the views of the auditee and OIG's response to those views as appropriate.
- Conforms to the principles of good written communications. Please refer to the *OAS Style Manual* as a reference on the principles of good written communications.

It is OAS policy not to release a draft report in any form (e.g., a working draft) to any entity external to OIG before the draft report is formally issued.

It is OAS policy to post Public Summaries of most reports that are designated as restricted because they contain sensitive information.

30-02-20 TIMELINESS

Audit reports should be issued promptly so they are available for timely use by management, legislative officials, and other interested parties. The report may be of little value to decision makers if it is perceived as stale or if the audit report arrives too late. Draft reports should be completed as soon as possible after the completion of audit field work.

30-02-30 SHARING AUDIT RESULTS BEFORE ISSUING A DRAFT REPORT

The audit team must not release a draft report in any form (e.g., a working draft) to any entity external to OIG before the draft report is formally issued.

The audit team may share the preliminary results of an audit with an auditee or OPDIV using TeamEWP Issues or another document that briefly outlines the audit results.

Unless approved by the DIG, no information will be released to third parties external to HHS, such as congressional staff, on audit results until the draft audit report has been issued and discussed with the auditee and at least oral, preferably written, comments received. OAS should ensure that the audit results released to external parties are fair, complete, and objective and that the auditee does not plan to submit new information or

present an argument that will have an impact on that fairness, completeness, and objectivity.

For information on distributing draft reports refer to Chapter 30-03, *Transmitting Audit Reports*, and Chapter 30-04*, Distribution of HHS Produced Audit Reports*.

30-02-40 REPORT TRANSMITTALS AND COVERS

OAS uses both memoranda and letters to transmit reports.

A transmittal memorandum is used to transmit results of an audit to departmental operating officials when recommendations are made directly to the Department or an OPDIV. It is signed by the IG or DIG. The cover of a report should show the name and title of the official who signed the transmittal memorandum for the final report.

A transmittal letters is used to transmit audit results to auditees outside the Department and is signed by the RIG, or the AIG responsible for the IT Audit Division. Some reports issued to auditees outside the Department are also transmitted to the Department or OPDIV with a MIR alerting the Department or OPDIV of the report (See Chapter 30-03, *Transmitting Audit Reports)*. The MIR is signed by the IG or DIG.

If a report is issued to an auditee outside the Department and is not transmitted to the Department or OPDIV, the cover should show the name and title of the AIG who approved the report. If a report issued to an auditee outside the Department is also transmitted to the Department or OPDIV, the cover of the report should show the name and title of the official who signed the MIR.

30-02-40-01 IG- and DIG- Cover Reports

The following chart identifies the criteria for IG- and DIG- cover reports (i.e. those reports with a transmittal memoranda or a MIR).

	IG	DIG
1. National Policy Implications	✓	
2. Cumulative Cost Questioned, Costs Set Aside, and Funds Put to Better Use ≥ $50 million*	✓	
3. Cumulative Costs Questioned, Costs Set Aside, and Funds Put to Better Use ≥$5 million < $50 million		✓
4. Congressional Request or Interest	✓	
5. Nationwide Rollup Reports (DIG determines signature; default is IG signed)	✓	✓
6. Significant Media Coverage or Interest	✓	
7. Highly Sensitive Issues (HIV/AIDS for example)	✓	
8. Secretarial Initiatives or Projects	✓	
9. Other Departmental Top Management Initiatives or Projects (if other criteria are not met)		✓
10. Reports addressed to a State Governor (if other criteria are not met)		✓

* The DIG will consult with the OIG's Immediate Office about whether the IG should sign reports with cumulative cost questioned, costs set aside, and funds put to better use between $25 million and $50 million.

30-02-50 HEADQUARTERS REVIEW

All audit reports expected to have an IG or DIG cover and model reports should be submitted to the Headquarters Review Team. To initiate the review process, the audit team should send the related *Report Submission Summary Sheet* (SD-17) to the Headquarters Review team, which will create a record in the *Headquarters Audit Report Tracking and Inventory System* (HARTIS).

Any Congressional correspondence should also be submitted to the Headquarters Review Team via email at OASHQReview@oig.hhs.gov. The Headquarters Review Team will coordinate its review with the Office of External Affairs.

Audit reports expected to have an AIG cover should be submitted to the applicable AIG for review and clearance to issue.

For more information, refer to the Intranet.

30-02-60 REPORT CONTENTS

The following paragraphs set forth the general content requirements for each section of the report. However, situations occur that do not fit a standardized format. In these cases, the report format should be modified.

OAS reports should contain the following elements discussed below, as appropriate.

- Transmittal Memorandum (Reports issued directly to the Department of an OPDIV) (Section 30-02-60-01)
- Transmittal Letter (Reports issued to aduitees outside the Department) (Section 30-02-60-02)
- Cover—Draft and Final Reports (Section 30-06-20)
- Report Notices Page (Section 30-06-30)
- Executive Summary (Section 30-02-60-04)
- Table of Contents (Section 30-02-60-05)
- Headings (Section 30-02-60-06)
- Appropriate Tone (Section 30-02-60-07)
- Abbreviations and Acronyms (Section 30-02-60-08)
- Introduction (Section 30-02-60-09)
- Why We Did This Review (Section 30-02-60-10)
- Objective(s) (Section 30-02-60-11)
- Background (Section 30-02-60-12)
- How We Conducted This Review (Section 30-02-60-13)
- Findings (or Results of Audit) (Section 30-02-60-14)
- Conclusion (optional) (Section 30-02-60-15)
- Recommendations (Section 30-02-60-16)
- Privileged and Confidential Information Omitted from Report (Section 30-02-60-17)
- Ongoing or Contemplated Investigation (Section 30-02-60-17-01)
- Administratively Confidential Information (Section 30-02-60-17-02)
- Personally Identifiable Information (Section 30-02-60-17-03)
- Implementation of Prior Recommendations (Section 30-02-60-18)
- Inadequate or Unauditable Records (Section 30-02-60-19)
- Instructions for Requesting Auditee Comments (Section 30-02-60-20)
- Auditee Comments on Draft Reports (Section 30-02-60-21)
- OIG Response to Auditee Comments (Section 30-02-60-22)

- Auditee Comments on Final Reports (Section 30-02-60-23)
- Other Matters (Section 30-02-60-24)
- Appendixes (Section 30-02-60-25)
- Audit Scope and Methodology (Sections 30-02-60-25-01 through -04)
- Auditee's Comments on Draft Report (Technical Issues) (Section 30-02-60-26-01 through -03)

See Exhibit 30-02-A for a *Summary of Standard Report Format.*

30-02-60-01 Transmittal Memorandum (Reports to the Department and OPDIVs)

The format of and information included in transmittal memorandashould follow the guidelines in Chapter 30-03, *Transmitting Audit Reports*.

30-02-60-02 Transmittal Letter (Auditees Outside of HHS)

The format and information included in transmittal letters for reports should follow the guidelines set forth in Chapter 30-03, *Transmitting Audit Reports*.

30-02-60-03 Report Cover, Notices Page, and Page Margin Notices

For policy on report titles, covers, and notices page see Chapter 30-06, *Report Covers, Notices Page and Bottom Page Margin Notices*.

30-02-60-04 Executive Summary

The Executive Summary is designed for readers who desire a quick, clear synopsis of the audit results and do not have time or a need to read the entire report. Since the Executive Summary is a condensed version of the report, appropriate emphasis is placed on the audit objectives, findings in response to the objectives, and recommendations. An Executive Summary is not required for reports with no findings or simple, single topic reports that are 3 pages or less, exclusive of appendixes.

The Executive Summary in reports less than 10 pages in length usually should be no more than one and a half pages in length, and the Executive Summary in reports longer than 10 pages in length usually should be no more than two pages in length. For purposes of this discussion, the length of the report is exclusive of the Executive Summary, Table of Contents, and appendixes.

The Executive Summary should be free of technical jargon and excessive use of acronyms. When it makes sense, use key words instead of acronyms. For example, instead of referring to Wyoming State Department of Social Services as WSDSS, refer to it as the State or Social Services.

The general characteristics of the Executive Summary are:

- A box at the beginning of the Executive Summary, which contains a brief statement (one or two sentences) of the finding that includes the dollar effect, the impact on beneficiaries, or both.

- Why We Did This Review, which has a brief introduction to the topic of the audit and information to provide context and a rationale for the audit. The second paragraph is the objective, as a natural follow-on from the rationale paragraph.

- Brief background section (usually limited to a few paragraphs), including other necessary background that allows executive-level readers to understand the remainder of the Executive Summary.

- How We Conducted This Review, which is optional. It has an explanation of the scope of review, including details on any sample necessary to understand the findings.

- What We Found, which contains a finding (or answer) for each objective.

  Each finding should include executive-level information on the finding attributes. Vital criteria should be brief and paraphrased.

- What We Recommend, which has an emphasis on actions (recommendations) to improve future conditions.

- Synopsis of auditee comments and OIG response (if necessary) is included in final reports. For guidance, see Subsection 30-02-60-19, *Auditee Comments on Draft Reports*.

- Executive Summary follows the same general sequence as the report itself.

To help readers find information of particular interest, headings are used in the Executive Summary. The headings usually used are:

- Why We Did This Review
- Background
- How We Conducted This Review (optional)
- What We Found
- What We Recommend
- Auditee Comments and Our Response (finals only, Our Response only if necessary)

30-02-60-05 Table of Contents

The Table of Contents lists the headings with the corresponding page numbers and appendixes that are used in the report.

Note: Reports with no findings and no Executive Summary do not require a Table of Contents.

30-02-60-06 Headings

Headings are of four types:

- 1st level headings: capitalized (all letters), boldface, and centered.
- 2nd level headings: capitalized (all letters), boldface, and placed at the left margin.

- 3rd level headings: capitalized (first letter of each key word), boldface, and placed at the left margin.

- 4th level headings: capitalized (first letter of each key word), italicized, and placed at the left margin.

1st level headings are used for the titles of separate sections of a report. They are capitalized (all letters), in boldface, and centered. The 1st level headings in an audit report are:

- Executive Summary
- Introduction
- Finding(s)/Results of Audit[1]
- Recommendation(s)
- Auditee Comments and Office of Inspector General Response (finals only)
- Other Matters (if applicable)
- The titles of Appendix(es)

To distinguish headings from each other and show which material is subordinate, 2nd, 3rd, and 4th level headings are used as necessary to further divide report content into logical parts and are tailored according to the contents of each report:

- 2nd level headings are primarily used to identify major subsections within the Executive Summary, Introduction, Findings, and Audittee Comments and OIG Response sections. For example, titles of audit findings within the Findings section will use this style of heading.

- 3rd level headings are used to separate blocks of text under 2nd level headings.

- 4th level headings are normally used when further separations are needed within text under a 3rd level heading.

30-02-60-07 Appropriate Tone

OAS reports should have a professional, objective, courteous tone. The tone of reports should encourage favorable reaction to findings and recommendations.

[1] Results of Audit is generally used when there are positive findings or no findings.

30-02-60-08 Abbreviations and Acronyms

While the use of abbreviations and acronyms should be kept to a minimum in the report, their use is often necessary to avoid unnecessary repetition. Obscure acronyms should be avoided. The abbreviation or acronym should be spelled out the first time it is used, with the abbreviation or acronym following in parentheses. Acronyms or abbreviations defined in the executive summary must be defined again the first time they are used in the body of the report. They are not reestablished in the appendix(es).

In longer reports, the authoring team may wish to include a glossary of abbreviations and acronyms used in the report at the end of the table of contents, especially if many abbreviations or acronyms are used or they are not widely known. In shorter reports, it is usually unnecessary to include a glossary.

30-02-60-09 Introduction

The Introduction (1st level heading) is the formal opening of the report. The Introduction consists of Why We Did This Review, the Objective, the Background, and How We Conducted This Review (2nd level headings).

30-02-60-10 Why We Did This Review

This section uses the same wording as was in the Executive Summary, but it is sometimes expanded with more detail. A reference to previous OIG reviews in a Related OIG Reports appendix can be placed at the end of this section.

30-02-60-11 Objective(s)

The Objective(s) section is a statement of the purpose of the audit or the question(s) the audit report will answer.

30-02-60-12 Background

The Background section is intended to provide a concise, general description of the audited program, function, or activity primarily to enable the less familiar reader to understand, in reasonable perspective, the Objective(s), How We Conducted This Review, Findings (or Results of Audit), and Recommendations sections. It generally includes comments on the nature, authority, purpose, size, and organization of the audited entity, program, function, or activity and general information related to applicable laws and regulations.

30-02-60-13 How We Conducted This Review

The How We Conducted This Review section follows the Background section.

Report readers need to understand the purpose of the audit and depth and coverage of audit work. A clear understanding of these enables the readers of the report to determine the usefulness of the findings and recommendations. How We Conducted This Review should summarize the detailed information in the Scope and Methodology appendix.

Place this statement from *Government Auditing Standards* at the end of this section:

> 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.

30-02-60-14 Findings (or Results of Audit)

A section entitled Findings (or Results of Audit) follows the How We Conducted This Review section. While the Executive Summary provides the reader with an overview of the report, the Findings section provides the details and relevant audit evidence to support the summary of audit results presented in the opening paragraph.

In the Findings section:

- Give a complete accounting of audit results, e.g.,
  - how much of the total activity was audited, how much is allowable, and how much is unallowable or
  - the sample size, how many items of the sample are allowable, and how many items are unallowable and the dollar amount.

  Examples of different paragraphs applicable to accounting for dollars or sample of claims audited follow:
  - Of the $31.5 million that the State agency claimed for reimbursement for the period August 31, 20xx, through August 30, 20xx, $31 million was allowable. However, the State agency claimed $529,977 in expenses for budget years 2005 ($98,893) and 2006 ($431,084) that were not allowable.
  - Of the 147 FPBP claims in our sample, 110 were eligible for Federal Medicaid reimbursement, but 37 were not. As a result, the State improperly received $918,816 in Federal Medicaid funds.
- Each topic or group of related topics (including the auditee comments and OIG response) should be discussed separately under headings tailored for an orderly and logical presentation. Standards concerning characteristics of the report content are applicable. In addition, each negative audit finding should generally contain all five attributes of a fully developed finding, i.e., condition, criteria, effect, cause, and recommendation.

30-02-60-15 Conclusion (optional)

The Conclusion section should include information on the effect of the findings to add more context for the recommendations, including summarizing causes and adding the effect on program integrity. This is optional and will be used mostly on more complex reports.

30-02-60-16 Recommendations

Each recommendation must address a finding discussed in the report. The recommendations in this section repeat the recommendations from the Executive Summary. If the recommendations are summarized in the Executive Summary, the full recommendations are shown in the body.

30-02-60-17 Privileged and Confidential Information Omitted from Report

Federal, State, or local laws or regulations may prohibit certain information from general disclosure. Such information may be provided on a need-to-know basis only to persons authorized by law or regulation to receive it. Before omitting pertinent data from the report, OAS auditors should obtain assurance that a valid requirement for the omission exists, and consult with OCIG. As appropriate, the report should include a statement on whether any pertinent information has been omitted because it is privileged or confidential. If so, the nature of the information must be described, unless disclosure of such information might compromise an ongoing or contemplated investigation, and the law or other basis for withholding such information must be stated.

30-02-60-17-01 Ongoing or Contemplated Investigation

When it is considered critical to make reference to an ongoing or contemplated investigation in a report:

- All personal identifiers, names of organizations and any other information that may serve as a basis for identification of the subject of investigation must be excluded.

- Information obtained by the Grand Jury process, classified information, tax information from IRS or SSA, or information subject to a court seal or protective order must not be included in an audit report. Such information should be transmitted by letter or memorandum to an addressee authorized to receive the information.

In addition, clearance must be obtained from both the OI and the appropriate AIG before including in audit reports any reference to an ongoing or contemplated investigation. See Chapter 20-08, *Investigative Activities*, Section 20-08-40-01, *Reporting,* and Subsection 20-08-50-03, *Reporting*.

30-02-60-17-02 Administratively Confidential Information

Since OAS reports on grantee or contractor operations are made available to the public, all administratively confidential information should be excluded from the reports. Examples of the administratively confidential items are: names of borrowers and lenders, payments to individual recipients and beneficiaries, and descriptions of internal control systems designed to protect government assets. The name of a sole healthcare practitioner should not be included in a report that will be posted on the Internet. Names of organizations should also in some instances not be included.

30-02-60-17-03 Personally Identifiable Information

Draft and final reports and their appendixes, with the exception of reports prepared for OI, OCIG, or DOJ, must not contain any personally identifiable information (PII). See Chapter 20-11, *Protection of Sensitive OAS Information*, Section 20-11-30, *Defining Sensitive Information Within OAS*, for examples of PII.

30-02-60-18 Implementation of Prior Recommendations

OAS follows up on findings developed during prior audits with similar objectives. A separate caption within the Findings and Recommendation section entitled "Implementation of Prior Recommendations" should be used. If the prior finding is still valid, an updated version of a previously reported finding is restated in the current report under the same caption as it originally appeared, with appropriate reference in the text to the earlier report and the continuing nature of the condition. If the prior finding has been corrected or is no longer relevant, the report should contain a statement to that effect.

30-02-60-19 Inadequate or Unauditable Records

When a finding on inadequate or unauditable records is reported, the finding, at a minimum, should include:

- A detailed description of the additional audit work performed.
- The results of the audit work.
- The basis for a qualified opinion or a disclaimer of opinion if the auditor was unable to obtain sufficient evidential matter to form a conclusion.
- Recommendations detailing what needs be done by the auditee to make the records auditable.

30-02-60-20 Instructions for Requesting Auditee Comments

Instructions for requesting auditee comments are set forth in Chapter 30-03, *Transmitting Audit Reports*, Section 30-03-40, *Instructions for Requesting Auditee Response*.

30-02-60-21 Auditee Comments on Draft Reports

OAS considers the reviewed entity or operating division (OPDIV) comments to be an essential part of a report's development. These comments contribute to balance, accuracy, and objectivity in the final product. Guidance on how to handle auditee's comments is discussed in Subsection 30-02-60-25, *Appendixes*.

If comments to the draft are not provided within the approved time, the draft report may be, subject to the approval of the Principal Deputy Inspector General or DIG, issued in final without the auditee's comments.

On occasion auditees may request that certain information be redacted from the final report. If the request is based on legal issues, e.g., if the auditee asserts the material meets one of the exemptions of the Freedom of Information Act, the audit team should consult with OCIG before redacting the information.

The auditee's formal comments to each recommendation should be included in the final audit report. In addition, during the audit there should have been advance discussion with responsible management officials at the audited entity. Advance discussion, in its broadest sense, is defined as oral and written communication related to the findings before the final report is issued.

The auditee may present new information in its formal written comments to the draft report. In these instances, the information should be evaluated before incorporating the comments and issuing the final report.

Occasionally auditees will include technical comments in their response to the draft report. These comments can be contained in (1) a separate document from the general response, or (2) same document as the general response.

The auditee comments should appear in the final audit report in three places:

- The Executive Summary. After the recommendation(s), include a synopsis of the auditee comments.

- After the Recommendation(s) section in the body of the report. Include a synopsis of auditee comments after the recommendation(s).

  Only the information in the comments that pertains to each finding(s) should be included in the synopsis. The auditee may offer additional information that is immaterial to the evidence or conclusions. To avoid confusing the reader and distorting the main elements, this information should be excluded. When incorporating comments, the auditee's statements are usually paraphrased. When paraphrasing, the original context of the auditee's position must be maintained. Direct quotations also may be used, taking care that the context of the auditee's statements is maintained.

  In a separate paragraph following the paragraph summarizing the auditee's comments, add a statement that the complete text of auditee's comments is included as an appendix. If a portion of the auditee's comments have been excluded from the appendix, provide the reason. Examples of different paragraphs applicable to three different situations follow.

  - The the State agency's comments are included in their entirety as the Appendix.

  - CMS also provided technical comments, which we addressed as appropriate. CMS's comments, excluding technical comments, are included as the Appendix.

  - (Name of auditee)'s response to our draft report is included as the Appendix. We excluded the attachments to (name of auditee)'s comments because they contained personally identifiable information.

- As an Appendix to the report. Include the complete text of the auditee comments except for technical comments and personally identifiable information (PII). See Subsections 30-02-60-26, *Auditee Comments on Draft Reports;* 30-02-60-26-02, *Auditee's Technical Comments;* and 30-02-60-26-03, *Personally Identifiable Information in Auditee's Comments*.

30-02-60-22 OIG Response to Auditee Comments

After considering the auditee's formal position, OAS has a final opportunity to defend its audit position and, if necessary, provide additional clarification. This clarification is provided in the OIG Response section.

Having presented each relevant auditee comment, OAS auditors may respond with counterarguments, which concentrate on an auditee's misinterpretation or faulty logic. In responding to the auditee's comments, the OAS auditor should guard against the introduction of new evidence. The key to presenting a good rebuttal is persuasion. A harsh tone should be avoided. If an auditee does not respond to a recommendation,

OAS auditors should inform the reader that the auditee was nonresponsive to the particular recommendation.

There are generally three ways to present the OIG response to an auditee's comments:

- The OIG response is presented after the auditee comments under a separate heading.
- The OIG response is presented after the auditee comments under a combined heading, e.g., Auditee Comments and Office of Inspector General Response.
- The OIG response to multiple arguments raised by the auditee should usually be presented as follows:
    - A combined heading, e.g., Auditee Comments and Office of Inspector General Response, is used for the entire section and is usually followed by a summary paragraph.
    - A heading is used for each relevant argument presented by the auditee.
    - The auditee comment and OIG response are usually presented separately under separate subheadings.

30-02-60-23 Auditee Comments on Final Reports

OAS apprises the auditee of where to direct comments to the final report. See Chapter 30-03, *Transmitting Audit Reports*, Section 30-03-40, *Instructions for Requesting Auditee Response*.

30-02-60-24 Other Matters

Where necessary, a section entitled Other Matters can be used for information that does not belong elsewhere. For instance, when the audit identifies significant issues that warrant further audit work but are not directly related to the audit objectives and the auditor does not have the time or resources to expand the audit to pursue them, the auditor may:

- Report as Other Matters issues identified during the audit for which the attributes have not been sufficiently developed to support recommendations, or
- Refer the issues to the appropriate division within OAS responsible for planning future audit work.

Data or comments specifically requested by management officials may also be reported as Other Matters—for instance, explanations of factors contributing to variations in administrative costs claimed by Medicare intermediaries.

While there is no established format for this section, to the extent the elements of a finding are developed, they should be presented in a logical sequence.

30-02-60-25 Appendixes

The last part of a report contains the Appendixes. When there is more than one appendix, each is identified in alphabetical order in its title, e.g., Appendix A: Audit Scope and Methodology.

The purpose of appended material is to provide further details, explanations, or support for statements included earlier in the report. The data should be self-evident, clear, and descriptive. Such information might include financial schedules, statistical tables, or graphics that cannot be merged smoothly within the narrative of the audit report.

When reporting on the results of sampling, both statistical and nonstatistical, and estimations or generalizations relevant to the audit objectives, the report should include a discussion of the sampling methodology and details of the sample design. (See Chapter 20-02, *Statistical Sampling and Mathematical Calculation Estimation Techniques in Auditing*, Section 20-02-30, *The Audit Process*, Subsections 20-02-30-04-B, C and D, *Reports, Supplementary Estimation Documentation, and Reporting Composite Figures* for guidance.)

30-02-60-25-01 Audit Scope and Methodology – Scope

The details of the scope and methodology are in this appendix.

Scope is the boundary of the audit and should be directly tied to the audit objectives. For example, the scope defines the parameters of the audit, such as the period of time reviewed, how much of the total activity was audited, the availability of necessary documentation or records, and the location at which field work was performed.

Auditors should include in the scope section a description of the extent of their work on internal controls.

Audit scope impairments are factors external to the audit organization that can restrict the auditor's ability to render objective opinions and conclusions. Examples of audit scope impairments include: (1) restriction of access to records and personnel, and (2) substandard records. When a scope impairment cannot be removed, a statement disclosing the scope impairment and the known effect it had on the results of the audit should be included.

30-02-60-25-02 Audit Scope and Methodology – General Information on Methodology

The methodology information should describe the procedures and methods used to gather evidence and verify and analyze information that was used to formulate the conclusions in the report and should, as applicable:

- Explain the relationship between the universe and what was audited.
- Identify organizations and geographic locations at which audit work was conducted and the time period covered by the audit.
- Cite the kinds and sources of evidence used and the techniques used to verify them.
- Discuss scope limitations when applicable.
- Explain any quality or other problems with the evidence. If unverified data are used, this should be stated.

When reporting on the results of sampling and estimations or generalizations relevant to the audit objectives, include a statement as required by Chapter 20-02, *Statistical Sampling and Mathematical Calculation Estimation Techniques in Auditing, and Subection 20-02-30-04, Phase 4 – Reporting*.

When an auditee has delayed providing comments or has not provided comments at the time the report is issued, the methodology section should include an explanation of efforts made to overcome excessive delays to obtain the views of responsible auditee officials on the audit findings and recommendations or an explanation of efforts made to obtain the auditee's comments.

30-02-60-25-03 Audit Scope and Methodology – When Following All Generally Accepted Government Auditing Standards

Include the statement from the *Government Auditing Standards* in the methodology appendix of the report.

> 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.

30-02-60-25-04 Audit Scope and Methodology – When All Applicable Generally Accepted Government Auditing Standards Were Not Followed

When auditors do not comply with all applicable *Government Auditing Standards*, they should include a modified Government Auditing Standards compliance statement in the audit report. Auditors should use a statement that includes either: (1) the language in Subsection 30-02-60-13, modified to indicate the standards that were not followed or (2) language that the auditor did not follow Government Auditing Standards.

30-02-60-26 Auditee's Comments on Draft Report (Technical Issues)

The complete text of the auditee's written comments on the draft report is included as an appendix to the final report except for the auditee's technical comments, which should be addressed as appropriate, and any PII.

30-02-60-26-01 Tentative Findings Have Been Modified or Deleted

When some auditee comments are no longer applicable to the final report because tentative findings have been modified or deleted, a footnote on the auditee's written comments may be appropriate. An illustrative footnote is:

> **Office of Inspector General Note**—This paragraph is not applicable because the finding or issue referred to by the auditee is not included in this report.

Care should be exercised not to minimize auditee comments by use of footnotes because the auditor does not agree. Such comments should be dealt with in the applicable part of the Findings section.

30-02-60-26-02 Auditee's Technical Comments

The complete text of the auditee's written comments on the draft report is included as an appendix to the final report, except for the auditee's technical comments, which should be addressed as appropriate.

We usually receive technical comments only from OPDIVs. These technical comments are usually in a separate document from the general response. When we receive technical comments from external auditees, they are frequently in the body of the response.

If we have appropriately addressed comments received as a separate document from the auditee's general response, the comments should be excluded from the final report. See Subsection 30-02-60-21, *Auditee Comments on Draft Reports*, for guidance on how to acknowledge the exclusion.

If technical comments are received in the same document as the general response and we have appropriately addressed them, the comments may be omitted from the auditee's response. A footnote of the omission is appropriate. Following is an example of such a footnote:

> **Office of Inspector General Note**—Technical comments in the auditee's response to the draft have been omitted from the final report and all appropriate changes have been made.

30-02-60-26-03 Personally Identifiable Information in Auditee's Comments

OAS must ensure that any PII contained in auditee's comments on draft reports is not included in the final report. See Chapter 20-11, *Protection of Sensitive OAS Information*, Section 20-11-30, *Defining Sensitive Information Within OAS*, for examples of PII.

Occasionally auditees will include PII in their response to the draft report. The PII can be contained in (1) a separate document from the general response, or (2) same document as the general response.

If the PII is in a separate document from the general response or attachment to the general response, the document or attachment should be excluded from the final report. See Subsection 30-02-60-21, *Auditee Comments on Draft Reports*, for guidance on how to acknowledge the exclusion.

If the PII is in the same document as the general response, the PII must be redacted from the auditee's response. A footnote of the redaction is required. An illustrative footnote in the auditee's response is:

> **Office of Inspector General Note**—The deleted text has been redacted because it is personally identifiable information.

30-02-70 PUBLIC SUMMARIES OF RESTRICTED REPORTS

When a report or series of reports is restricted because it contains sensitive information, such as details of Information Technology vulnerabilities or information related to bioterrorism prevention or response, OAS may issue a Public Summary of the restricted report(s) that includes a high-level overview of the findings without details that might be exploited by a hacker or other individual with malicious intent.

OAS does not issue Public Summaries of Limited Official Use reports or reports that contain classified information.

30-02-70-01 Types of Public Summaries

Following is a description of the three types of Public Summaries that OAS issues:

Public Summary of a single restricted report

This is the most common type of Public Summary. It should present a high level summary of the findings of a single restricted report covering a single entity or OPDIV.

Public Summary of multiple restricted reports

A Public Summary covering multiple restricted reports may be used to present high-level summary of findings from multiple restricted reports that are related in some logical way (e.g., a common objective). A public summary of multiple reports should only be used to present a summary of the individual reports that are covered by the summary and should not contain any information, findings, or recommendations that were not included in the individual reports. If an audit team intends to include new information, findings, or recommendations, it should prepare a restricted roll-up report for issuance to the Department or appropriate OPDIV.

Public Summary of a restricted roll-up report

A restricted roll-up report is used to communicate the results from a series of restricted reports with additional information, findings, or recommendations that were not included in the individual restricted reports.

A public summary of the restricted roll-up report should include a high-level summary of the findings and recommendations from the restricted roll-up report. The public summary should not include any information from the individual restricted reports that was not included in the restricted roll-up report.

30-02-70-02 Contents of Public Summaries

A Public Summary follows the regular report format with the following exceptions:

It includes an introductory paragraph (before "Why We Did This Review") that explains that:

- It is an overview of a previously issued report(s).
- It omits specific details of the vulnerabilities that we identified because of the sensitive nature of the information.
- We provided more detailed information and recommendations to officials of the audited entity.

It does not generally include:

- An executive summary
- Appendixes*

*If an auditee, the Department, or an OPDIV provides comments on a Public Summary, they should be included as an appendix.

30-02-80 GRAPHICS

The use of tables, schedules, graphs, and charts (collectively referred to as graphics) to consolidate and interpret the audit results can aid the reader in understanding data gathered and conclusions reached. A table or schedule is a visual tool for summarizing or presenting data. A graph or chart is a tool for explaining or comparing data.

Before determining whether to use a graphic, the following questions should be addressed:

- What is the idea the report reader will get from it?
- Does it accurately portray the data or relationship?
- Will it assist the report reader in understanding conditions found or OAS conclusions?

30-02-90 TERMINATED AUDITS

When an audit is terminated before its completion and an audit report is not issued, the audit team should document the results of the work to the date of termination and why the audit was terminated. In addition, the audit team should communicate the reasons for terminating the audit to management of the audited entity, the entity requesting the audit, and other appropriate officials. This communication should be documented in TeamMate. If such communication might compromise an ongoing or contemplated investigation, the audit team should consult with OI for advice on handling the matter.

Exhibit 6-30-02-A

Summary of Standard Report Format

Report Element	For Guidance See Chapter/Section
Transmittal, Cover, Title Page	
• Transmittal Memorandum (Internal Reports)	30-02-60-01
• Transmittal Letter (Grantee or Contractor)	30-02-60-02
• Report Cover, Notices Page, and Page Margin Notices	30-02-60-03
• Inside Cover- All Draft and Final Reports (Describes OIG)	30-06-20-04
• Notices Page	30-06-30
• Final Reports – Notices Page – Required Notices (Final only)	30-06-30-02
• Bottom Page Margin Notices	30-06-40
Executive Summary	30-02-60-04
• Executive Summary [1]	30-02-60-04
• The Box	30-02-60-04
• Why We Did This Review [2]	30-02-60-04
• Background [2]	30-02-60-04
• How We Conducted This Review (Optional) [2]	30-02-60-04
• What We Found [2]	30-02-60-04
• What We Recommend [2]	30-02-60-04
• Auditee Comments and Office of Inspector General Response (Finals Reports) [2]	30-02-60-04
• Table of Contents [1]	30-02-60-05
• Glossary of Abbreviations and Acronyms (Optional) [1]	30-02-60-08
Report	
• Introduction [1]	30-02-60-09
• Why We Did This Review [2]	30-02-60-10
• Objective(s) [2]	30-02-60-11
• Background [2]	30-02-60-12
• How We Conducted This Review [2]	30-02-60-13
• Findings (or Results of Audit) [1] Each topic or group of related topics discussed separately under 2nd level headings [2]	30-02-60-14
• Implementation of Prior Recommendations, if applicable [2]	30-02-60-18
• Conclusion (optional) [2]	30-02-60-15
• Recommendations [1]	30-02-60-16
• Instructions for Requesting Auditee Comments	30-02-60-20
• Auditee Comments on Draft Reports [1, 3]	30-02-60-21
• OIG Response to Auditee Comments [1, 3]	30-02-60-22
• Auditee Comments on Final Reports	30-02-60-23
• Other Matter(s) [1]	30-02-60-24
• Appendixes, including the audit scope and methodology and complete text of auditee's formal comments to draft report (Final Reports) [1]	30-02-60-25

Headings (For additional guidance see Subsection 30-02-60-06.)

[1] 1st level heading, capitalized (all letters), boldface, and centered. Note: reports with no findings and no executive summary do not require a table of content`s.

[2] 2nd level heading, capitalized (all letters), boldface, and at the left margin.

[3] Present the auditee's comments and OIG response under one 1st level heading.

TRANSMITTING AUDIT REPORTS

30-03-00 PURPOSE

This chapter establishes policies and procedures for transmitting OAS audit reports.

30-03-10 POLICY

It is OAS policy to:

- Provide addressees of OAS reports with a cover memorandum or letter, when appropriate, that identifies the program, function or activity, and period audited.
- Exclude from OAS reports all administratively confidential information.
- Follow OIG-wide requirements set forth in the OIG Administrative Manual, Part 9-40, Freedom of Information Requests, relative to release of reports to the public and to grantees or contractors.

See Exhibit 30-03-A for a *Summary of Selected Transmittal Requirements*.

30-03-20 ADDRESSEES BY TYPE OF AUDIT

The addressees for audit reports are based on the type of audit as follows:

- Audits of HHS administration and management should be addressed to top management officials, including division heads or other departmental officials responsible for the activities audited.
- Audits of grantee or contractor operations are addressed to the auditee's administrative executive, except for recipient capability audits, bid proposal audits, grant and contract closeout audits, and facilities and administrative cost audits.
- Recipient capability audits, bid proposal audits, and grant and contract closeout audits relative to HHS grants and contracts are addressed to the HHS requesting official with a copy to the audit liaison responsible for tracking corrective action on recommendations.
- Facilities and administrative cost audits are addressed to the HHS, Division of Cost Allocation.

- Reimbursable audits, including grant and contract closeout audits, should be addressed to the requesting official or in accordance with the requestor's instructions.

30-03-30 TRANSMITTAL MEMORANDUMS AND LETTERS FOR REPORTS ISSUED BY OFFICE OF AUDIT SERVICES

OAS should prepare transmittal memorandums for reports issued to departmental officials and transmittal letters for reports issued to grantees and contractors. The content requirements for transmittal memorandums and letters are discussed below.

30-03-30-01 Transmittal Memorandums (Departmental Officials)

The transmittal memorandums should be usually no more than two pages in length, should not contain headings or footnotes, and should include the following information:

- OAS policy for safeguarding draft reports.

- State whether a response to the report is required, including notifying the auditee that the final audit report will include the auditee's comments to the draft report and will be posted on the Internet (unless the report contains restricted information under the Freedom of Information Act (FOIA)).

The transmittal memorandum should contain instructions for auditee response (for draft and final reports) in accordance with requirements set forth in Section 30-03-40, *Instructions for Requesting Auditee Response*.

The original signed transmittal memorandum is attached to the cover of the original signed report sent to the addressee. Copies of the transmittal memorandum are also attached to copies of the report that are kept in OAS files. The transmittal memorandum is not sent with copies of the report distributed outside of HHS.

See Chapter 30-06, *Report Covers, Title Pages, Notices Pages and Bottom Page Margin Notices*, Section 30-06-40, *Page Margin Notices*, for margin notice required on transmittal memorandums that contain restricted or limited official use information.

Templates for preparing transmittal letters and memorandums are available on OAS's Intranet.

30-03-30-02 Transmittal Letters (Grantee or Contractor Officials)

Transmittal letters should be usually no more than two pages in length and include the following information:

- The program, function or activity, and period audited.

- State whether a response to the report is required, including notifying the auditee that the final audit report will include the auditee's comments to the draft report and will be posted on the Internet (unless the report contains restricted information under the FOIA.)

- OAS policy for safeguarding draft reports.

For final reports, the HHS action official to whom the grantee should direct its reply should be shown at the end of the letter. The auditee may, if it wishes, submit questions or comments to the HHS action official on reports which have no findings. For reports

with findings, each grantee should be requested to reply to the action official in accordance with requirements set forth in Section 30-03-40, *Instructions for Requesting Auditee Response*.

The original signed transmittal letter is sent to the auditee with the report. All other copies of the report should include a copy of the transmittal letter immediately following the title page.

See Chapter 30-06, *Report Covers, Title Pages, Notices Pages and Bottom Page Margin Notices*, Section 30-06-40, *Page Margin Notices*, for margin notice required on transmittal letters that contain restricted or limited official use information.

Templates for preparing transmittal letters and memorandums are available on OAS's Intranet.

30-03-30-03 Transmittal Letters to Congress

Transmittal letters to Congress should be prepared when a Member, group of Members, Committee, or the Congress has specifically requested that we conduct the review, or if OIG is required by statute to conduct the review and transmit the results to Congress. Such letters generally should be limited to a single page and should contain the following information:

- The source of the request to which OIG is responding, either a specific statute or the date of the incoming letter, and the nature of the request.
- If more than one Member requested the review, letters addressed to each requesting Member should be prepared. The closing paragraph of each letter should indicate that the report is being sent to the other requesting Members. However, if more than 10 Members requested the review, Executive Secretariat may permit a generic transmittal to all Members.
- For letters addressed to the Chairman of a committee, an identical letter addressed to the Ranking Member of the committee should be prepared. The closing paragraph of each letter should indicate that the report is being sent to the other Member.
- For letters addressed to Congress, identical letters are sent to the Speaker of the House and the President of the Senate. The closing paragraph of each letter should indicate that the report is being sent to both houses of Congress.
- The closing paragraph of each letter should provide the name and telephone number of the OIG Director of External Affairs as the contact point.

All transmittal letters to Congress will be signed by the IG.

As each letter to Congress is unique, templates are not available. An example of a letter to a Senator is shown as Exhibit B.

30-03-40 INSTRUCTION FOR REQUESTING AUDITEE RESPONSE

Transmittal memorandums and letters should contain instructions for the auditee's response to the report.

The response instructions should tell the auditee to whom its response should be directed, to respond within 30 days, and to refer to the Report Number in all report-related correspondence. On occasion, however, the auditee may be instructed to respond in fewer than the usual 30 days but no fewer than 15 business days.

30-03-40-01 Draft Reports Signed by the Inspector General

OIG considers operating division (OPDIV) comments to be a critical part of the report process as they reflect the position of the OPDIV regarding OIG findings and recommendations and often include information about ongoing Department initiatives. In addition, the comments on the draft report allow OIG the opportunity to incorporate additional information from the OPDIV into the final report, as appropriate.

OPDIV requests for additional time to respond to draft reports signed by the IG must be submitted to the OIG Executive Secretariat via email, fax, or mail before the expiration of the 30-day comment period. Requests should include information about the extenuating circumstances that warrant an extension. OIG will consider the request and inform the OPDIV of whether OIG is able to accommodate its request. If an extension is not granted, OIG will notify the OPDIV and may issue a final report without OPDIV comments. The audit report will then be subject to the conflict resolution process described in Chapter 8-30, *Conflict Resolution Mechanism for Inspector General Reports*, of the *HHS General Administrative Manual*.

Suggested language for requesting comments is presented below:

> To properly consider your views on the validity of the facts and reasonableness of the recommendations in this report, we request that you provide us with written comments within 30 days from the date of this letter. Please include the status of any action taken on our recommendations, as well as any planned action. Your written comments will be summarized in the body of our final report and included as an appendix.
>
> Requests for additional time to respond to this draft report must be submitted to the OIG Executive Secretariat via email (include email address), fax (include fax number), or mail before the expiration of the 30-day comment period. Requests should include information about the extenuating circumstances that warrant an extension.
>
> OIG will consider the request and inform you whether OIG is able to accommodate the request. If an extension is not granted, OIG will notify you and may issue a final report without OPDIV comments.

30-03-40-02 Draft Reports Signed by the Deputy or Regional Inspector General for Audit Services

OAS considers the reviewed entity responses and comments to be an essential part of a report's development. These comments contribute to balance, accuracy and objectivity in the final report. An illustrative request for comments is:

> To properly consider your views on the validity of the facts and reasonableness of the recommendations in this report, we request that you provide us with written comments within 30 days from the date of this letter. Please include the status of any action taken on our recommendations, as well as any planned action. Your written comments will be summarized in the body of our final report and included as an appendix.

Recognizing the complexity of the issues and the time needed to research and respond to draft reports, extensions may be granted to written requests on a case-by-case basis, under special circumstances. (Guidance on how to handle auditee's responses is discussed in Chapter 30-02, *Reporting on Results of Audits*, Subsection 30-02-60-21, *Appendixes*.)

- Internal Reports — (those issued to parties within the Department)

  The OPDIV can be granted extensions up to a maximum of an additional 30 calendar days to respond to a draft report. Written requests for extensions should be directed to the appropriate RIG for regional reports or to the appropriate AIG for headquarters signed reports.

- External Reports — (those issued to parties outside the Department)

  Management of the entity audited is provided the opportunity to review and respond to the draft report. In addition to the initial time provided for review and response, auditee management can be granted extensions up to a maximum of an additional 30 calendar days. Written requests for extensions should be directed to the appropriate RIG for regionally-signed reports or to the DIG for headquarters-signed reports. Requests for additional extensions or extensions beyond 30 calendar days will be considered on a case-by-case basis.

  For draft reports that contain significant audit matters,[1] the audit team may provide an informational copy to the OPDIV action official concurrently when providing the draft report to the audited entity. If the OPDIV central offices or action official choose to offer verbal or written comments, OAS will consider them, as appropriate. These comments, if any, are not to be attached to the final report.

If an auditee's response to the draft report is not provided within the approved time, including any extensions, the draft report may be issued in final without the auditee's comments. The audit report will then be subject to the conflict resolution process described in the *HHS General Administrative Manual,* Chapter 8-30, *Conflict Resolution Mechanism for Inspector General Reports*.

30-03-40-03 Final Reports

The response instructions should tell the auditee to whom its response should be directed and to refer to the Report Number in all report-related correspondence.

- Internal Reports — (those issued to parties within the Department)

  Within the body of the transmittal memorandum, the addressee should be directed to provide OAS with the status of actions taken or contemplated on recommendations within 6 months of the report issue date. The OAS Intranet contains a template of a transmittal memorandum for a final report issued to an HHS official.

- External Reports — (those issued to parties outside the Department)

[1] See Chapter 30-01, *Memorandums to Management*, Section 30-01-30-01, *Significant Audit Matters* for definition. Certain reports, such as Recipient Capability Audits; Bid Proposal Audits; Grant and Contract Closeout Audits; and Facilities and Administrative Cost Audits will not be subject to the above requirement of requesting the auditee's written comments. However, care should be exercised to ensure that advance discussion of any findings be held with auditees before the comments inclusion in a final report.

Within the body of the transmittal letter, the addressee should be directed to provide the HHS action official with the status of actions taken on recommendations within 30 days of the report issue date. The language to be used is provided below:

> Final determination as to actions taken on all matters reported will be made by the HHS action official named below. We request that you respond to the HHS action official within 30 days from the date of this letter. Your response should present any comments or additional information that you believe may have a bearing on the final determination.

The caption "Direct Reply to HHS Action Official:" should be capitalized (first letter of each key word), boldface type, placed at the left margin, and placed at the end of the report transmittal letter after the signature block. The OAS Intranet contains a template of a transmittal letter for a final report issued to an HHS grantee or contractor.

30-03-50 OBTAINING COMMENTS FROM ENTITIES TO WHICH RECOMMENDATIONS ARE NOT ADDRESSED

Government Auditing Standards require that auditors obtain and report the views of responsible officials of the audited entity, preferably in writing. For most audits, OAS meets this requirement by seeking comments from the entity to which recommendations are addressed. However, in some cases an audit may involve significant audit work at a single entity, but recommendations are not addressed to that entity. Following are examples of this situation:

- Auditors performed significant work at a Medicaid provider but make recommendations to the State agency.
- Auditors performed significant work at a head start grantee to evaluate the grantee's ability to manage Federal funds but make recommendations to the Administration for Children and Families.

In such cases, the auditors should provide the entity where significant audit work was performed an opportunity to comment on the accuracy of the draft report before it is issued to the entity to which the report is addressed. This is referred to in WebAIMS as the "initial draft report."

After an entity's comments to the initial draft are incorporated to the report, the auditors should issue a second draft report to the entity to which recommendations are addressed. This is referred to in WebAIMS as the "draft report."

30-03-60 AUTHORIZED SIGNATORIES

See Chapter 30-02, *Reporting on Results of Audits*, Section 30-02-40, *Report Signatories.*

Exhibit 6-30-03-A

Summary of Selected Transmittal Requirements

Reports Addressed To	
• Departmental Officials (Internal)	Memorandum
• Grantees and Contractors (External) (1)	Letter
The Transmittal	
• Cites OAS policy for safeguarding draft reports	Draft & Final Reports
• States whether a response to the report is required	Draft Reports
• Cites OAS policy regarding auditee comments and posting on the World Wide Web	Draft & Final Reports
• Instructions for Requesting Auditee Response	
Time Allowed for Response:	
Draft Reports - **Initial** (1 & 2)	30 Days
Draft Reports - Extensions Up To (1 & 2)	30 Days
Final Reports (3)	60 Days
Internal - Response to OAS	30 Days
External - Response to Action Official	
Distribution	
• Original Signed Memorandum/Letter	Addressee (4)
• Copies	(5), (6) & (7)

Notes

1. See Subsection 30-03-40-01, *Draft Reports Signed by the Inspector General*
2. See Subsection 30-03-40-02, *Draft* Reports Signed by the Deputy or Regional Inspector General for Audit Services
3. See Subsection 30-03-40-03, *Final Reports*.
4. Attached to cover of the original report.
5. See Chapter 30-04, *Distribution of HHS Produced Audit Reports*.
6. The transmittal memorandum is not sent with copies of the report distributed outside the HHS.
7. A copy of the transmittal letter should be inserted immediately following the title page of the report.

Exhibit 6-30-03-B

EXAMPLE TRANSMITTAL LETTER – TO CONGRESS

The Honorable Charles E. Grassley
Ranking Member, Committee on Finance
United States Senate
Washington, DC 20510

Dear Senator Grassley:

In a December 19, 2005, letter, you requested that the Office of Inspector General (OIG) assess the beneficiary complaints system and the fiscal integrity of the Quality Improvement Organizations (QIO). In the Medicare program, QIOs were established to promote the effective, efficient, and economical delivery of health care services and to promote the quality of services. With respect to the fiscal integrity of the QIOs, your letter specifically asked OIG to review, at a minimum, the following areas:

1. board member and executive staff compensation;
2. board member and executive staff travel;
3. costs relating to legal fees, including administrative charges;
4. equipment and administrative charges;
5. business relationships and conflicts of interest; and
6. contract modifications.

The enclosed final report, which is one of a series of nine audits of QIOs, presents the results of our review. OIG has examined issues related to beneficiaries' quality of care concerns and the beneficiary complaint resolution process in another review (OEI-01-06-00170).

We are sending an identical letter to the Chairman of the Finance Committee.

If you have any questions or comments regarding the issues discussed in the report, please contact me, or your staff may call Claire Barnard, Director of External Affairs, at (202) 205-9523.

Sincerely,

Daniel R. Levinson
Inspector General

Enclosure

DISTRIBUTION OF HHS PRODUCED AUDIT REPORTS

30-04-00 PURPOSE

This chapter establishes policies and procedures to be followed in distributing audit reports produced by OAS. This includes audit reports pertaining to programs operated or funded by HHS as well as audit reports prepared for other Federal agencies (reimbursable audits).

30-04-10 STANDARDS

The standards for distributing audit reports are found in Chapter 7 of the *Government Auditing Standards*.

30-04-20 POLICY

It is OAS policy that audit reports produced by OAS should be distributed to:

- Appropriate officials of the audited entity, except for those reports discussed in Chapter 20-04, *Special Audits*.
- Those charged with governance.
- Oversight bodies requiring or arranging for the audits.

Audit reports on grantee or contractor operations are distributed simultaneously to HHS operating division (OPDIV) officials and officials of the grantee or contractor.

If the subject of the audit involves material that contains restricted or limited official use information, OAS should limit the report distribution.

A *Report Distribution Schedule* should be prepared and retained in the audit documentation for all OAS produced final reports[1]. The distribution schedule should:

- Not be included in or attached to the report.
- List the recipients of the report.
- List the number of copies sent to each recipient if hard copies are distributed.
- Indicate whether the report was posted on the Internet.

The distribution schedule should also contain the recipients' email addresses, if the report is distributed electronically. It is the audit team's responsibility to:

- Obtain and verify current email addresses before the reports are distributed to the auditee and/or report requestor. This does not include email addresses of HHS Action Officials and Audit Liaisons, which Audit Planning and Implementation (API) will obtain and publish on the Intranet.
- Provide email addresses on the distribution schedule and include with the report submitted for signature. This will facilitate timely providing most auditees a copy of the report and posting of final unrestricted reports on the Internet within 3 days of issuance, which is currently required by law.

In addition, packages for IG-signed reports must include a completed OIG Executive Secretariat (ES) form, *Electronic Transmission of Report Procedures for Distribution*.

Questions concerning report distribution that are not answered in this chapter should be referred to the Director of API.

30-04-20-01 Electronically Distributing Unrestricted Draft and Final OIG Reports Signed by the IG

OIG ES, in a document titled *Distribution of Draft and Final Reports,* set forth OIG policy relative to electronically distributing draft and final reports signed by the IG. OAS headquarters will prepare documents needed by ES to implement this policy.

For memorandums of impending release (see Chapter 30-01*, Memorandums to Management*), the A headquarters Audit Visual specialist will advise the AIG and RIG of the date that the report should be issued. The RIG should not issue the audit report until the memorandum has been signed and a report issue date established. The report issue date is usually within 5 business days of the date of the memorandum.

Headquarters will provide the audit team with any documents that should be maintained with the audit documentation.

30-04-20-02 Electronically Distributing DIG-, AIG-, and RIG-Signed Draft and Final Audit Reports, Including Special Audits

Most audit reports should be distributed via email (Microsoft Outlook or HHS/OIG Delivery Server), as an Adobe Acrobat Portable Document Format (PDF) attachment. This applies to both reports distributed to HHS and non-HHS auditees and HHS and

[1] For IG-signed reports, the OIG Executive Secretariat prepares and maintains the distribution schedule.

other government officials. Under no circumstances may a non-PDF copy of the report, e.g., created in Microsoft Word, be distributed outside OIG. Copies of emails transmitting reports, including all attachments, should be retained in TeamMate.

Note: OAS no longer requires encrypting files with PGP, or other software, when transmitting draft or final reports *outside* the OIG via the HHS/OIG Delivery Server.

OAS employees should electronically convert or scan to PDF all draft and final audit reports. Notes in the source document must not be converted to comments and the source file(s) must not be included as an attachment to the PDF or email. Before electronically converting an electronic file to PDF, OAS employees should run a metadata removal tool for Microsoft Word, Excel and PowerPoint files. This tool also will remove comments.

When draft reports are transmitted via email, the body of the email should contain the following statement:

> **NOTICE—THIS DRAFT IS RESTRICTED TO OFFICIAL USE**
>
> This document is a draft report of the Office of Inspector General and is subject to revision; therefore, recipients of this draft should not disclose its contents for purposes other than for official review and comment under any circumstances. This draft and all copies thereof remain the property of, and must be returned on demand to, the Office of Inspector General.

For reports to HHS OPDIVs, the report should be sent to the OPDIV's audit liaison. For reports to non-HHS entities, the report should be sent to the head of the entity and the entity's liaison, if any. Final reports should be sent electronically within 1 business day after the report is signed. In the event that OAS is unable to obtain an email address for the addressee, a hard copy of the report should be sent via overnight mail. OAS will send hard copies of the report to those auditees who request hard copies.

See Exhibit 30-04A for a *Summary of Report Transmittal Methods Applicable to Draft & Final Reports Distributed to HHS and Non-HHS Auditees and Other Non-OIG Entities*.

30-04-20-02-01 Early Alert of Significant Preliminary Findings and Memorandums of Impending Release

All *Early Alerts of Significant Preliminary Findings*, and *Memorandums of Impending Release,* regarding restricted or limited official use final reports discussed in Chapter 30-01, *Memorandums to Management*, may be emailed as an attachment using the HHS/OIG Delivery Server.

Memorandums of Impending Release regarding unrestricted final reports may be transferred as an attachment using Microsoft Outlook.

Templates for preparing emails are available on the Intranet.

30-04-20-02-02 Unrestricted Reports

Unrestricted draft reports may be emailed as an attachment using the HHS/OIG Delivery Server. OAS employees may not use Microsoft Outlook to transfer draft reports, whether or not encrypted, outside the OIG.

Unrestricted final reports may be transferred as an attachment using Microsoft Outlook.

Templates for preparing transmittal emails are available on the Intranet.

30-04-20-02-03 Restricted Reports, Including Security Reviews

Restricted reports (draft and final), including Security Reviews, must be transmitted using the HHS/OIG Delivery Server.

OAS employees may not use Microsoft Outlook to transfer restricted reports outside the OIG. Security reviews are those reviews that cover particularly sensitive topics such as homeland security issues (e.g., select agents, bioterrorism, and classified or potentially classified information). The audit team should consult with the appropriate AIG on proper distribution of security review reports.

When transferring restricted reports outside the OIG using the HHS/OIG Delivery Server, OAS employees must request the recipient to send the OAS employee an email before the OAS employee sends any information. This allows the OAS employee to copy and paste the email address into the HHS/OIG Delivery Server, thus avoiding the possibility of sending sensitive information to an unintended recipient.

The transmittal email, using the HHS/OIG Delivery Server, should contain the following warning, in caps and bold:

> **WARNING: THIS REPORT CONTAINS RESTRICTED, SENSITIVE INFORMATION, SUCH AS CONFIDENTIAL PROPRIETARY MATERIAL WITH A HIGH POTENTIAL FOR MISUSE.**
>
> **DISTRIBUTION SHOULD BE STRICTLY LIMITED. DO NOT REPRODUCE OR RELEASE TO ANY PERSON WITHOUT THE PRIOR APPROVAL OF THE OFFICE OF AUDIT SERVICES.**

The following language should also be included in the email:

> Please safeguard the attached report from unauthorized access and/or use and appropriately encrypt it, if the report is stored on any electronic media. If you send this report electronically, please encrypt it and communicate the pass phrase to the recipient(s) by telephone – not in the email or email attachment. Also, please do not distribute the attached report to unauthorized individuals or organizations without specific, written authorization of the Deputy Inspector General for Audit Services, Office of Inspector General, U.S. Department of Health and Human Services.

Templates for preparing transmittal emails using the HHS/OIG Delivery Server are available on the Intranet.

30-04-20-02-04 Limited Official Use Reports

Generally, OAS does not issue draft limited official use information reports. In the rare case where issuing a limited official use information draft report may be appropriate, consult with the Director for Quality Assurance and Policy before issuing the draft report.

OAS employees must use the HHS/OIG Delivery Server to transfer limited official use reports (draft and final) outside the OIG firewall. OAS employees may not use Microsoft Outlook to transfer limited official use reports, whether or not encrypted, outside the OIG.

The HHS/OIG Delivery Server transmittal email should contain the following warning, in caps and bold:

> **NOTICE: THIS IS A LIMITED OFFICIAL USE REPORT. DISTRIBUTION IS LIMITED TO AUTHORIZED OFFICIALS.**

The following language should also be included in the email:

> This report was prepared at your request to provide information to assist management decision-making. Accordingly, (addressee organization) may distribute this report at its discretion.

Templates for preparing transmittal emails are available on the Intranet.

30-04-20-02-05 Additional Email Required Elements - Whether Using Microsoft Outlook or the HHS/OIG Delivery Server

In the interest of uniformity across OAS, emails transmitting audit reports (draft and final) must have a standard subject line, instructions if recipient needs the email resent, signature block for the staff transmitting the report in the format shown below, and the standard OIG email disclaimer. Do not add background colors or images to emails.

The standard subject line will be:

> Official Correspondence – Draft Report from U.S. Department of Health and Human Services, Office of Inspector General (Report Number A-XX-XX-XXXXX)
>
> or
>
> Official Correspondence - Report from U.S. Department of Health and Human Services, Office of Inspector General (Report Number A-XX-XX-XXXXX)

The last sentence of the email before the email sender's information should be:

> If you have trouble opening the attached report and need this email resent, please contact the staff list below.

The signature block should contain:

> Email Sender's Name
> Office of Audit Services
> Office of Inspector General
> U.S. Department of Health and Human Services
> Sender's Email Address
> Sender's Telephone Number
>
> Attachments – as stated

The OIG standard email disclaimer is:

> This email may contain confidential and/or privileged information. If you are not the intended recipient (or have received this email in error) please notify the sender immediately and destroy this email. Any unauthorized copying, disclosure or distribution of the material in this email is strictly forbidden.

30-04-20-02-06 Providing Recipients of Draft Reports and Annotated Restricted Final Reports Access to the HHS/OIG Delivery Server to Securely Provide Written Comments or OIG Clearance Documents

Using the HHS/OIG Delivery Server, government and non-government organizations are able to securely send electronic files to OAS.

Emails transmitting draft reports should inform auditees that a separate email will follow with instructions on using the HHS/OIG Delivery Server to securely transmit their written response to the draft report.

Emails transmitting annotated reports of restricted final reports should inform Action Officials they should use the HHS/OIG Delivery Server to securely transmit to the OIG, in PDF, the OIG Clearance Document (OCD) regarding management decisions and actions taken on OIG recommendations. For some action officials, OAS will establish accounts to use the HHS/OIG Delivery Server. For others, OAS will provide access on a case-by-case basis.

30-04-20-02-07 Transmitting Reports When OAS Is Not Able to Obtain and Confirm Email Address(es) to Transmit Reports Electronically

In the event that OAS is unable to obtain and confirm an email address for the addressee(s) to transmit the report, the report should be hand carried or sent overnight via U.S mail or OIG approved common carrier. In these cases, OAS will send hard copies via:

- U.S. mail: Express, Certified, or Registered Mail.
- OIG approved common carrier. (Approved common carriers are those that OIG has an account with. Contact your administrative officer for the current list.)

The audit team should consult with the appropriate AIG on proper distribution of security review reports.

30-04-30 DISTRIBUTION SCHEDULE

Although the distribution of each report is unique, a consistent approach helps ensure that each OAS produced report is distributed to as many interested officials as is practical. Such an approach helps the auditor in identifying appropriate officials who should be provided with a copy of the audit report.

OAS uses three basic types of distribution schedules for OAS produced reports, one for IG-signed reports, one for OAS headquarters-signed reports, and one for OAS regionally signed reports.

For policy as to who is authorized to sign reports, see Section 30-02-40, *Report Signatories*.

The OAS Distribution Schedule for IG-signed reports generally includes the following: Deputy Secretary, Chief of Staff, Assistant Secretary for Planning and Evaluation, Assistant Secretary for Public Affairs, Assistant Secretary for Legislation, Assistant Secretary for Resources and Technology, Assistant Secretary for Administration and Management, OIG officials, and other persons with particular interest in the report subject.

The OAS Distribution Schedule for headquarters-signed reports is determined on a case-by-case basis.

The OAS Distribution Schedule for regionally signed reports contains the addresses of action officials, audit liaisons, and non-HHS and other OIG officials. This document is updated periodically by API and is available on the Intranet.

30-04-30-01 Additional Distribution Requirement for Procurement Reports

Copies of all procurement reports (draft and final) involving any OPDIV should be provided to the Deputy Assistant Secretary for Acquisition Management and Policy, Office of Assistant Secretary for Administration and Management (ASAM).

Procurement reports for this purpose include reports on:

- The Department's contracting operations.
- Contractor billings and performance.

Procurement reports for this purpose do not include:

- The CMS contractor responsible for reviewing and paying Medicare claims.
- Contract closeouts requested by contracting officers.

An electronic copy of the report should be sent to:

> Deputy Assistant Secretary for Acquisition Management and Policy
> Office of Acquisition Management and Policy
> 200 Independence Ave. S.W., Room 328E
> Washington, DC 20201

The body of the email should read:

> Attached for your information is an electronic copy of OIG's [insert draft or final] report entitled, [insert name of report in quotes], [insert Report Number].
>
> This report is provided for your information only.

If the report contains restricted information, the email (using the HHS/OIG Delivery Server) should contain the additional information in Subsection 30-04-20-02-02.

If the report contains limited official use information, the email (using Microsoft Outlook) should contain the additional information in Subsection 30-04-20-02-03.

30-04-40 ADDRESSEES BY TYPE OF AUDIT

The audit report's addressee is based on the type of audit:

- Audit reports for audits of HHS administration and management should be addressed to top management officials, including OPDIV heads or other departmental officials responsible for the activities audited.

- Audit reports for audits of grantee or contractor operations are addressed to the auditee's administrative executive, except for special audits. (Addressees for special audits are discussed in the bullets below.)

- Audit reports for recipient capability audits, bid proposal audits, and closeout audits related to HHS grants and contracts are addressed to the HHS requesting official with a copy to the audit liaison responsible for tracking corrective action on recommendations. The reports have limited distribution; copies are not provided to the audited entity. (See Section 30-04-90, *Limited Distribution of Special Audits*.)

- Audit reports for facilities and administrative cost audits are addressed to the HHS Division of Cost Allocation (DCA).

- Audit reports for reimbursable audits, including grant and contract closeout audits, are addressed to the requesting official or addressed in accordance with the requesting instructions.

30-04-50 ACTION OFFICIAL

OAS will designate an action official for all OAS produced audit reports, except for reports to top management officials, including OPDIV heads, where no action official is required. In these cases, addressees are requested to respond directly to OAS.

The designation of the action official for audit reports is based on whether the audit covers single or multiple OPDIVs, except for:

- Audits of facilities and administrative cost proposals.

- Cost allocation plans, payment management systems.

- HHS administration and management.

These exceptions are covered below after discussion of audits covering single or multiple OPDIVs.

30-04-50-01 Single OPDIV

The action official should be provided with a copy of the report that is annotated to the recommendation(s) coded in Web Audit Information Management System (WebAIMS).

The action official for regionally signed reports can be found in Distribution Schedule for Regionally Issued Reports. This document is updated periodically by API and is available on the Intranet.

The action official for recipient capability audits, bid proposal audits, and closeout audits related to HHS grants and contracts is normally the addressee.

For reports to top management officials, including OPDIV heads, no action official is required. (See Section 30-04-50-06, *HHS Administration and Management Audits*, for requirements.)

30-04-50-02 Multiple OPDIVs

The action official should be provided with a copy of the report that is annotated to the recommendation(s) coded in WebAIMS.

The action official is:

Director, Division of Audit Resolution
Office of Grant and Acquisition Management
Assistant Secretary of Management and Budget
U.S. Department of Health and Human Services
Wilbur J. Cohen Building, Room 1067
330 Independence Avenue, S.W.
Washington, DC 20201

30-04-50-03 Facilities and Administrative Cost Proposal Audits

The action official should be provided with a copy of the report that is annotated to the recommendation(s) coded in WebAIMS.

The action official for other than profit-making organizations is:

Regions I and II
Director, Northeastern Office
Division of Cost Allocation
U.S. Department of Health and Human Services
26 Federal Plaza, Room 41-118
New York, NY 10278

Regions III and IV
Director, Mid-Atlantic Office
Division of Cost Allocation
U.S. Department of Health and Human Services
Wilbur Cohen Building, Room 1067
330 Independence Ave. S.W.
Washington, DC 20201

Regions V, VI and VII
Director, Central Office
Division of Cost Allocation
U.S. Department of Health and Human Services
1200 Main Tower Building, Room 1130
Dallas, TX 75202

Regions VIII, IX and X
Director, Western Office
Division of Cost Allocation
U.S. Department of Health and Human Services
90 – 7th Street, Suite 4-600
San Francisco, CA 94103

The action official for profit-making organizations is generally the contracting official.

30-04-50-04 Cost Allocation Plan Audits

The action official should be provided with a copy of the report that is annotated to the recommendation(s) coded in WebAIMS. The action official is:

Director, Northeastern Office
Division of Cost Allocation
U.S. Department of Health and Human Services
26 Federal Plaza, Room 41-118
New York, NY 10278

In addition to its responsibility for approving cost allocation plans, DCA is also responsible for coordinating the resolution of allocation findings that involve costs shared by two or more programs or functions (including direct and facilities and administrative costs of program administration). Auditees will be requested to respond to DCA as the coordinating action official. Responsibility for obtaining financial adjustments rests with the cognizant action official of the respective program or function.

After DCA has coordinated the resolution of audit findings, DCA will notify each respective cognizant action official of resolution actions necessary. The cognizant action official will submit OIG clearance documents based on this notification. (For additional information related to audit clearance documents, see Chapter 10-06, *Audit Resolution and Follow Up*.)

Reports containing both cost allocation findings and other types of findings will require the auditee to respond to the Office of Grant and Acquisition Management action official as in Section 30-04-50-02, *Multiple OPDIVs*.

30-04-50-05 Payment Management System Audits

The action official should be provided with a copy of the report that is annotated to the recommendation(s) coded in WebAIMS. The action official is:

Chief, Accounting and Control Branch
Division of Payment Management, ORM/OM
U.S. Department of Health and Human Services
P.O. Box 6021
Rockville, MD 20852

30-04-50-06 HHS Administration and Management Audits

For reports to top management officials, including OPDIV heads, no action official is required. Addressees are requested to respond directly to OAS with the status of actions taken on recommendations. A copy of the annotated report is sent to the audit liaison. (See Section 30-04-60, *Audit Liaison*.)

If an action official is not designated for a regional report, the RIG will make that designation. As a general rule, the action official will be at least one level higher in the organization than the auditee. The action official should be provided with a copy of the report that is annotated to the recommendation(s) coded in WebAIMS.

30-04-60 AUDIT LIAISON

The audit liaison is determined by the program(s) or activities covered in the audit. The audit liaison should be provided with an annotated copy of the report.

An audit liaison is not designated for audits of facilities and administrative cost proposals, cost allocation plans, payment management systems, and HHS administration and management.

30-04-70 NON-HHS OFFICIALS

Audit reports on recipients of HHS funds generally will not be distributed to other Federal or State agencies unless their funds are specifically covered in the audit. Other Federal and State agencies may have an interest in OAS reports, either because of funds at the same auditee site that were not included in the report or because of the possible award of funds to the auditee.

OAS will make reports available to other agencies when requested or when the AIG or RIG believes the report may be of interest to other agencies. A copy of the email, memorandum, or letter transmitting the report to the other agency should be furnished to API.

30-04-80 ELECTRONIC FREEDOM OF INFORMATION ACT

The Electronic Freedom of Information Act Amendments of 1996 (E-FOIA) requires that audit reports be made available to the public in electronic format. OIG has interpreted the electronic format prescribed in the E-FOIA as the Internet and the file format as PDF. Within 3 days of release, Public Affairs will post most final reports on the OIG Internet site making them available in the public domain. OAS will post on the Internet a copy of the same report transmitted to the auditee. This will ensure that the report publically available on the Internet is an exact duplicate of the report transmitted to the auditee.

The following should not be posted on the Internet:

- Reports issued within OIG, including internal quality control reviews, OI and OCIG assist work, and assist work between OAS regions or divisions.
- Reports addressed to departmental officials that are considered internal correspondence, e.g., early alerts.
- Reports with limited distribution, as defined in Section 30-04-90, *Limited Distribution of Special Audits*, and Section 30-04-100, *Restricted Reports*.
- Reimbursable audits performed for another Federal agency when the report is addressed to the other Federal agency.
- A transmittal letter to a sole healthcare practitioner even when the report will be posted on the Internet. (Note: per Chapter 30-02, *Reporting on Results of Audits*, Section 30-02-60-13-02, *Administratively Confidential Information*, the name of a sole practitioner should not be included in a report that will be posted on the Internet.)

These are subject to Freedom of Information Act provisions and may be available for release to the media, public, and members of Congress on a case-by-case basis, after consultation with OCIG.

See Exhibit 30-04B for a *Summary of Electronic Posting Requirements*.

The distribution schedule should indicate whether the report was posted on the Internet.

30-04-90 LIMITED DISTRIBUTION OF SPECIAL AUDITS

Recipient Capability Audits, Bid Proposal Audits, Grant and Contract Closeout Audits, and Facilities and Administrative Cost Audits are addressed to the responsible government official and the audited entity is not provided a copy of these audit reports. Since the distribution of these reports is limited, it is up to the organization that requested the audit to determine if the report should be distributed to other parties.

These reports will not be published on the Internet. Requests for such reports should be referred to the organization that requested the audit.

For additional information of these reports, see Chapter 30-06, *Report Covers, Notices Page, and Bottom Page Margin Notices*.

30-04-100 RESTRICTED REPORTS

Restricted audit reports contain information on matters that are sensitive and are not released in the "normal" manner. Audit reports containing the following types of information are considered restricted:

- Homeland security issues – security reviews that cover particularly sensitive topics, e.g., select agents, bioterrorism, and classified or potentially classified information.
- Information technology issues – audits that cover information technology systems, e.g., Federal Information Security Management Act audits.
- Confidential or proprietary information, e.g., drug pricing audits.
- Reference to an ongoing or contemplated investigation. (See Chapter 20-08, *Investigative Activities*.)

30-04-110 ANNOTATED AUDIT REPORTS

OAS maintains detailed information with respect to:

- All audit reports, including those discussed in Chapter 20-04, *Special Audits*.
- Audit recommendations (except those in reimbursable audits requested by another Federal agency – see Section 30-04-120, *Reimbursable Audits*).
- OPDIV actions to clear those recommendations.

This information is maintained in WebAIMS. OAS uses WebAIMS to track all audit recommendations, except those for reimbursable audits, until final decisions are made on the amount of funds to be recovered and on the corrective actions to be taken by recipient organizations.

OAS notifies OPDIVs, i.e., the action official and the audit liaison office, of recommendations they are to address by annotating reports with recommendation codes. OAS inputs these codes into WebAIMS. The WebAIMS recommendation code should be placed next to each recommendation in the report and the word "Annotated" and "Not for

Public Release" should be placed in red letters in the upper right and left hand corner of the audit report cover, respectively.

Annotating the report will help those officials responsible for audit resolution and monitoring audit resolution to more quickly match each recommendation code with the section of the audit report that discusses the finding.

In addition to the number of copies listed in the report distribution schedule, an annotated audit report should be provided via email to the audit liaison office, action official, and API when the final audit report is issued.

30-04-110-01 Unrestricted Reports

Annotated audit reports should be emailed within 5 business days of the report issue date. Email addresses of audit liaison officials can be found in Distribution Schedule for Regionally Issued Reports.

Templates for preparing transmittal emails are available on the Intranet.

30-04-110-02 Restricted or Limited Official Use Reports

Annotated audit reports should be sent via the HHS/OIG Delivery Server within 5 business days of the report issue date. Email addresses of audit liaison officials can be found in Distribution Schedule for Regionally Issued Reports.

Templates for preparing transmittal emails are available on the Intranet

30-04-120 REIMBURSABLE AUDITS

OAS performs audits requested by other Federal agencies, such as bid proposal audits and grant and contract closeout audits. Copies of the OAS report should be distributed to the requesting official and any other individual or office indicated in the request.

Annotated copies, as discussed in Section 30-04-110, *Annotated Audit Reports*, are not required for reimbursable audits.

Exhibit 6-30-04-A

Summary of Report Transmittal Methods Applicable to Draft & Final Reports Distributed to HHS and Non-HHS Auditees and Other Non-OIG Entities

OAS employees should electronically convert or scan to PDF all draft and final audit reports. Notes in the source document must not be converted to comments and the source file(s) must not be included as an attachment to the PDF or email. Before electronically converting an electronic file to PDF, run a metadata removal tool for Word, Excel and PowerPoint files.	Use		Post On Internet (Final Only)
	Microsoft Outlook Attach PDF to Email	HHS/OIG Delivery Server Attach PDF	
1. Reports – Post to the Internet			
a. Draft	No	Yes [1, 2, 3 & 4]	No
b. Final	Yes [1, 2, 3 & 4]	No	Yes [5]
2. Reports – Not Posted to the Internet			
a. Limited Distribution			
Limited Official Use Information			
i. Draft [6]	No	Yes [1, 2, 3 & 4]	No
ii. Final [7]	No	Yes [1, 2, 3 & 4]	No
b. Restricted Distribution, Including Security Reviews [8]			
i. Draft	No	Yes [1, 2, 3, 4 & 9]	No
ii. Final	No	Yes [1, 2, 3, 4 & 9]	No
Restricted Reports Includes: • Information Technology/Systems Information – Audits that cover Information technology/systems, e.g., Federal Information Security Management Act audits • Confidential or proprietary information, e.g., drug pricing • OIG Office of Investigations and Department of Justice assist work • Reference to an ongoing or contemplated investigation • Homeland Security Information - Security reviews that cover particularly sensitive topics, e.g., select agents, bioterrorism and classified or potentially classified information			

1. It is the audit team's responsibility to obtain and verify current email addresses before reports are distributed to auditees and/or report requestors. This does not include HHS action officials and audit liaisons.
2. OAS will continue to send hard copies of the report to those auditees who request hard copies and as a backup to electronic distribution. In the event that OAS is unable to obtain an email address for the addressee, the report should be sent via overnight mail.

Exhibit 6-30-04-A

Summary of Report Transmittal Methods Applicable to Draft & Final Reports Distributed to HHS and Non-HHS Auditees and Other Non-OIG Entities

Notes - Continued:

3. Under no circumstances may a non-PDF copy of the report, e.g., created in Microsoft Word, be distributed outside OIG.
4. Copies of emails transmitting reports, including all attachments, should be retained in TeamMate.
5. Post on the Internet a copy of the same report transmitted to the auditee. This will ensure that the report publically available on the Internet is an exact duplicate of the report transmitted to the auditee.
6. Generally, OAS does not issue draft limited official use information reports. In the rare case where issuing a limited official use information draft report may be appropriate consult with the appropriate AIG before issuing the draft report.
7. See Chapter 20-04, *Special Audits* - includes: recipient capability audits, bid proposal audits, grant and contract closeout audits, and facilities and administrative cost audits. These reports are prepared at another government organization's request to assist management decision-making and are transmitted to the responsible government official. Accordingly, a draft report should not be prepared for comment by the auditee and the audited entity is not provided a copy of the final audit report. Since the distribution of these reports is limited, it is up to the organization that requested the audit to determine if the report should be distributed to other parties. These reports will not be published on the Internet.
8. These reports have restricted distribution due to the sensitive subject matter. These reports will not be published on the Internet and precautions noted in the above table must be followed when transmitting the reports.
9. Request the recipient to send an email before sending any information. Copy and paste the email address into the HHS/OIG Delivery Server, thus avoiding the possibility of sending sensitive information to an unintended recipient.

Exhibit 6-30-04-B

Summary of Electronic Posting Requirements

	Post On Internet
I. Correspondence	
a. Internal - Departmental Officials	
1. Early Alert of Significant Preliminary Findings	No[1]
2. Memorandum of Impending Release	No[1]
b. External	
1. Closeout memorandum/letter (terminated audit)	No[1]
II. Report Transmittal Letter(s)/Memorandum(s)	
a. Letters Addressed to Grantees and Contractors, for Blue Cover Reports	No[2]
b. Memorandums Addressed to Departmental Officials for Blue Cover Reports	No[2]
c. Letters/Memorandums Addressed to Others	No[2]
III. Dated and Signed Copy of Final Report	
a. Does Not Contain Limited Official Use Information Restricted, Including Security reviews	Yes[1]
b. Contains Restricted or Limited Official Use Information	No[1]
c. Reimbursable Audits Performed for Another Federal Agency When the Report is Addressed to the Other Federal Agency	No[1]
IV. Internal OAS Documents	
a. Initial Report Distribution Schedule	No[1]
b. Annotated Final Report	No[1]
c. Internal Quality Control Reviews	No[1]
d. OI and OCIG Assist Work	No[1]
e. Assist Work Between OAS Regions or Divisions	No[1]

Notes

1. See Section 30-04-80, *Electronic Freedom of Information Act*.
2. See Chapter 30-03, *Transmitting Audit Reports*, Sections 30-03-30-01, *Transmittal Memorandums (Memorandum Reports)* and 30-03-30-02, *Transmittal Letters (Grantee or Contractor)*.

INDEPENDENT REPORT REVIEW

30-05-00 PURPOSE

This chapter establishes OAS policies and procedures for performing independent report reviews (IRR). These reviews help ensure that our written products are accurate and adequately supported.

30-05-10 STANDARDS

Chapter 3 of the *Government Auditing Standards* provides that audit organizations conducting government audits have an appropriate internal quality control system in place. The IRR process is an integral part of the OAS internal quality control system. (For additional information about the OAS quality control system, see Chapter 10-03, *Quality Control and Assurance*.)

30-05-20 POLICY

IRR is a process in which an experienced auditor who is independent of the audit verifies that statements of fact, figures, and dates are correctly reported, the findings are adequately supported by the audit documentation, and the conclusions and recommendations flow logically from the support.

Although the IRR is one of the elements of the OAS internal quality control program, the audit team has the ultimate responsibility for the quality of the audit report.

It is OAS policy that all draft reports and final reports must be independently reviewed. This review includes the report transmittals, report covers, title pages, notices pages, table of contents, glossary, and appendixes.

Also to be independently reviewed are:

- Memorandums to management (as defined in Chapter 30-01, *Memorandums to Management*).
- Executive summaries posted to the Internet.
- Products of assist audit work provided to other regional or divisional offices that may be used in the preparation of a report.
- Reports to other OIG components (i.e., OI, OCIG, OEI).
- Reports to the US Attorney's Office or other investigative or law enforcement agencies (unless precluded by the investigation).

Auditors should not perform an IRR of nonaudit services and reports produced by other organizations (e.g., other Federal agencies, State audit organizations, independent public accountant firms).

30-05-30 AUDIT TEAM'S RESPONSIBILITIES

Before the report is given to the reviewer, the audit team is responsible for assuring that:

- The report is prepared in accordance with *Government Auditing Standards* and OAS audit policies and procedures.
- The attributes of findings have been developed and are included in the audit documentation and report.
- Sampling plans or estimation plans have been developed and approved in accordance with OAS policies and procedures.
- The audit documentation has been adequately reviewed.
- The report, including any alternative text as appropriate for charts, graphs, and other images[1], is appropriately cross-referenced to the supporting audit documentation.
- The draft or final report and its appendixes, with the exception of reports prepared for OI, OCIG, or DOJ, contains no personally identifiable information (PII).
- The draft or final report and its appendixes that contains other sensitive information or is prepared for OI, OCIG, or DOJ is issued as a restricted information or limited official use information report under a green cover. See Chapter 20-11, *Protection of Sensitive OAS Information*, Section, 20-11-30, *Defining Sensitive Information Within OAS*, and Chapter 30-06, *Report Covers, Title Pages, Notices Pages and Bottom Page Margin Notices*.

The audit team is also responsible for providing the reviewer with a fully cross-referenced version of the report and the audit documentation.

Within the audit team, the audit manager is responsible for assuring that appropriate action is taken by the audit team to resolve issues raised by the reviewer.

30-05-40 INDEPENDENT REPORT REVIEWER'S RESPONSIBILITIES

The IRR process consists of three distinct phases. These are:

- General familiarization with the report to be reviewed.
- Detailed review.
- Resolution and disposition of the comments raised during the review.

At the start of the IRR process, the reviewer is responsible for reviewing the cross-referenced version of the report and the audit documentation provided by the audit team to obtain a general familiarization. Any report not fully cross-referenced to adequately reviewed audit documentation should be returned to the audit team for further actions.

[1] For processes OAS has implemented to make audit reports accessible to the widest possible audience, including individuals with disabilities, refer to the Intranet.

After becoming familiar with the report and the audit documentation, the reviewer is responsible for:

- Verifying that the reported information is accurately and completely cross-referenced to the audit documentation. (See Chapter 20-06, *Evidence and Audit Documentation*, Section 20-06-90, *Indexing and Hyperlinking/Cross-Referencing*.) In performing this step, the reviewer should verify that statements of fact, figures, and dates are correctly reported by examining satisfactory evidence in the audit documentation or performing necessary mathematical or clerical checks. Generally, it should not be necessary to go beyond the top schedules of the audit documentation, although selected critical items may be checked to detailed supporting audit documents.

- Determining that the report is adequately supported by sufficient, appropriate evidence in the audit documentation.

- Verifying that a statistical specialist has examined and approved the manner in which estimates have been developed and presented in the report. The reviewer is not expected to review these technical matters. (See Chapter 20-02, *Statistical Sampling and Mathematical Calculation Estimation Techniques in Auditing*.)

- Checking statements of fact, figures, and dates for consistency within the report.

- The draft or final report and its appendixes, with the exception of reports prepared for OI, OCIG, or DOJ, contains no PII.

- The draft or final report and its appendixes that contains other sensitive information or is prepared for OI, OCIG, or DOJ is issued as a restricted information or limited official use information report under a green cover. See Chapter 20-11, *Protection of Sensitive OAS Information*, Section, 20-11-30, *Defining Sensitive Information Within OAS*, and Chapter 30-06, *Report Covers, Title Pages, Notices Pages and Bottom Page Margin Notices*.

The reviewer is responsible for:

- Providing written comments to the audit team.

- Discussing and resolving open issues with the audit team.

- Documenting the resolution and disposition of all issues raised in the IRR.

When issues between the reviewer and the audit team cannot be resolved, the issues will be presented to the cognizant AIG or RIG for final resolution.

30-05-50 DOCUMENTING THE INDEPENDENT REPORT REVIEW

As part of the IRR process, the following should be included in the audit documentation:

- The reviewer's comments.

- The resolution of all IRR issues raised in the reviewer's comments.

30-05-60 SELECTION OF INDEPENDENT REPORT REVIEWER

The cognizant AIG or RIG is responsible for ensuring that audit reports are reviewed by an experienced auditor who is independent.

An experienced reviewer understands the audit process, *Government Auditing Standards*, and OAS policies and procedures. This experienced reviewer should have sufficient skills and knowledge to determine whether the conclusions and recommendations presented in the report are adequately supported by the audit documentation.

To ensure independence, the reviewer should not have worked on the audit or the preparation of the report.

30-05-70 CHANGES TO THE REFERENCED REPORT

If changes are made to a report after the IRR has been completed, the reviewer should review the changes to the revised document. These changes include all revisions made in either the region or in headquarters. Only new or revised statements of fact, figures, and dates should be cross-referenced to the audit documentation. Minor editorial changes do not have to be reviewed.

All new material should be reviewed following the usual IRR policies and procedures. Special care should be exercised in checking new statements of fact, figures, and dates for consistency within the report.

REPORT COVERS, NOTICES PAGE, AND BOTTOM PAGE MARGIN NOTICES

30-06-00 PURPOSE

This chapter establishes policies and procedures for preparing report covers, notices page, and bottom page margin notices for reports issued by OAS.

30-06-10 POLICY

It is OAS policy to use appropriate report covers, notices page, and bottom page margin notices for each audit report.

30-06-20 REPORT COVERS

OIG uses a uniform cover in issuing draft and final reports. Each report cover will:

- Include a title that briefly describes the results of the audit. The title should be specific and concise and should be consistent with the tone and balance of the report. Note: The name of a sole healthcare practitioner should not be included in a report title that will be posted on the Internet.
- Show the Report Number and the month and year of issuance.
- Include the name of the official signing the report and their title (i.e., Inspector General, Deputy Inspector General, Assistant Inspector General, or Regional Inspector General). If the official signing the draft report and the official signing the final report (or MIR) are not the same, the name and title of the official signing the final report should also be used on the draft report.

Include the following statement: *Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.* Templates and guidance for preparing report covers are available on OAS's Intranet.

30-06-20-01 Reports Not Containing Restricted Information or Limited Official Use Information – Draft and Final

OAS reports not containing restricted information or limited official use information[1] will be available to the public on the Internet.

[1] The Freedom of Information Act generally provides that any person has a right, enforceable in court, to obtain access to Federal agency records, except to the extent that such records (or portions of them) are protected from disclosure by one of nine exemptions or by one of three special law enforcement record exclusions. Access may not include categories or types of information within the OIG which are

30-06-20-02 Reports Containing Restricted Information or Limited Official Use Information – Draft and Final

There are two types of OAS reports that are not posted on the Internet. Those that:

- **Contain Restricted Information**
  - Homeland Security Information - Security reviews that cover particularly sensitive topics, e.g., select agents, bioterrorism and classified or potentially classified information.
  - Information Technology/Systems Information – Audits that cover Information technology/systems, e.g., Federal Information Security Management Act audits.
  - Confidential or proprietary information, e.g., drug pricing.
  - OIG Office of Investigations and Department of Justice assist work.
  - Reference to an ongoing or contemplated investigation.
- **Are Prepared for Limited Official Use**
  - Reports specifically requested by HHS officials to assist in meeting their stewardship responsibilities.
  - Recipient capability audits.
  - Bid proposal audits.
  - Grant and contract closeout audits.
  - Facilities and administrative cost audits.

  Since these audits are performed to assist HHS officials in meeting their stewardship responsibilities, including negotiating with grantees and contractors or at the request of other Federal agencies, OAS will address the reports to the responsible Government official and will not provide the audited entity with a copy of these audit reports. See Chapter 20-04, *Special Audits*, for reporting requirements.

considered Limited Official Use material. For more information, see *OIG Administrative Manual*, Chapter 7-40, *Freedom of Information Act Requests*.

30-06-20-02-01 Reports Containing Restricted Information

Covers of reports that contain restricted information will be labeled with a red label containing the following statement:

WARNING: THIS REPORT CONTAINS RESTRICTED, SENSITIVE INFORMATION, SUCH AS CONFIDENTIAL PROPRIETARY MATERIAL WITH A HIGH POTENTIAL FOR MISUSE. DISTRIBUTION SHOULD BE STRICTLY LIMITED. DO NOT REPRODUCE OR RELEASE TO ANY PERSON WITHOUT THE PRIOR APPROVAL OF THE OFFICE OF AUDIT SERVICES.

30-06-20-02-02 Reports Containing Limited Official Use information

Covers of reports that contain limited official use information will be labeled with a red label containing the following statement:

NOTICE—THIS IS A LIMITED OFFICIAL USE REPORT. DISTRIBUTION IS LIMITED TO AUTHORIZED OFFICIALS.

30-06-20-03 All Draft Reports – Required Notices

The front of report covers will include the following statement for draft reports:

NOTICE—THIS DRAFT IS RESTRICTED TO OFFICIAL USE

This document is a draft report of the Office of Inspector General and is subject to revision; therefore, recipients of this draft should not disclose its contents for purposes other than for official review and comment under any circumstances. This draft and all copies thereof remain the property of, and must be returned on demand to, the Office of Inspector General.

This notice is not usually applicable to special audits since these reports are not usually issued in draft. (See Chapter 20-04, *Special Audits*.)

In addition, for all draft reports, the word “DRAFT” should be inserted as a watermark across the cover. Each page of the report, including all exhibits and appendixes, should be marked “DRAFT,” in boldface, in the top right-hand corner.

30-06-20-04 Inside Cover – All Draft and Final Reports

The inside of all report covers will contain a description of the mission of the OIG and the functions of the OAS, OEI, OI, and OCIG. The inside cover should also contain the Internet address of the OIG.

30-06-30 NOTICES PAGE

All final reports will have a notices page immediately following the cover.

30-06-30-01 Draft Reports – Notices Page

The notices page is not used in draft reports.

30-06-30-02 Final Reports – Notices Page – Required Notices

For final reports, the notices page immediately follows the cover. These notices state whether or not the report will be available to the public on the Internet and contain a statement that qualifies findings and opinions set forth in the report as being those of OAS.

Templates for preparing notices page are available on OAS's Intranet.

30-06-30-02-01 Reports Posted on the Internet– Notices Page – Required Notice

The notices page of final reports posted on the Internet will include the Freedom of Information Act citation:

> **THIS REPORT IS AVAILABLE TO THE PUBLIC**
> at http://oig.hhs.gov
>
> Pursuant to the principles of the Freedom of Information Act, 5 U.S.C. § 552, as amended by Public Law 104-231, Office of Inspector General reports generally are made available to the public to the extent the information is not subject to exemptions in the Act (45 CFR part 5).

30-06-30-02-02 Reports Not Posted on the Internet – Notices Page – Required Notice

The notices page of any final report that contains restricted information or limited official use information that cannot be released to the public must include a statement containing the basis for exemption and notice of restriction:

A. Restricted Information

> **THIS REPORT CONTAINS RESTRICTED INFORMATION**
>
> This report should not be reproduced or released to any other party without specific written approval from OAS.

B. Limited Official Use Information

> **THIS IS A LIMITED OFFICIAL USE REPORT**
>
> The organization for whom this report was prepared may distribute the report at its discretion.

OAS reports that contain restricted information or are designated as limited official use reports will not be published on the Internet.

30-06-30-02-03 Notices Page – OAS Findings and Opinions

All OAS produced final reports must contain a statement that qualifies findings and opinions set forth in the report as being those of OAS. The following statement is required, as appropriate.

A. OAS Produced Reports Other Than Special Audits

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

B. Recipient Capability Audits

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Final determination on these matters will be made by authorized officials of the HHS operating divisions.

C. Bid Proposal Audits

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The recommendation for the disallowance of proposed costs and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Final determination on these matters will be made by authorized officials of the awarding agency.

D. Grant and Contract Closeout Audits

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The recommendation for the disallowance of costs incurred or claimed and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Final determination on these matters will be made by authorized officials of the awarding agency.

E. Facilities and Administrative Cost Audits

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The conclusions and recommendations contained in this report represent findings and opinions of OAS. Final determination on these matters will be made by authorized officials of the appropriate HHS office.

30-06-40 BOTTOM PAGE MARGIN NOTICES

Reports that contain restricted or limited official use information will have required notices in the bottom margin of each page.

30-06-40-01 Reports Containing Restricted Information – Draft and Final Reports

The bottom margin of each page of the report, including all exhibits and appendixes, and the transmittal memorandum/letter should be marked in bold italics:

Warning—This report contains restricted information for official use.
Distribution is limited to authorized officials.

30-06-40-02 Limited Official Use Reports

The bottom margin of each page of the report, including all exhibits and appendixes, and the transmittal memorandum/letter should be marked in bold italics:

Notice—This is a limited official use report.
Distribution is limited to authorized officials.

REPORTING AND CODING MONETARY RECOMMENDATIONS

30-07-00 PURPOSE

This chapter establishes policies and procedures for reporting monetary recommendations in OAS audit reports.

This chapter discusses the:

- Types of monetary recommendations reported by OAS
- Coding of monetary recommendations in the Web Audit Information Management System (WebAIMS)

30-07-10 STANDARDS

The Inspector General Act of 1978 as amended by the Inspector General Reform Act of 2008 (the Act) requires each Inspector General to prepare semiannual reports summarizing the activities of the Office during the immediately preceding 6-month periods ending March 31 and September 30.

Such reports must include a listing, subdivided according to subject matter, of each audit report issued during the reporting period and for each report, where applicable, the total dollar value of questioned costs, unsupported costs, and recommendations that funds be put to better use.

The Act defines the terms “questioned cost,” “unsupported cost,” and “funds put to better use” as follows:

Questioned Cost – A cost that is questioned because of:

- an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds;
- a finding that, at the time of the audit, such cost is not supported by adequate documentation; or
- a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.

Unsupported Cost – A cost that is questioned because the Office found that, at the time of the audit, such cost is not supported by adequate documentation. (Note: Unsupported Costs is a subset of Questioned Costs.)

Recommendation That Funds Be Put to Better Use – a recommendation that funds could be used more efficiently if management of an establishment took actions to implement and complete the recommendation, including:

- reductions in outlays;
- deobligation of funds from programs or operations;
- withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds;
- costs not incurred by implementing recommended improvements related to the operations of the establishment, a contractor, or grantee;
- avoidance of unnecessary expenditures noted in preaward reviews of contract or grant agreements; or
- any other savings which are specifically identified.

In addition to questioned costs, unsupported costs, and funds-put-to-better-use, the OIG is also required to report cost savings in its Semiannual Report to Congress. Cost savings are an after-the-fact determination when laws are enacted or administrative changes are implemented and the OIG can demonstrate that its work (i.e., recommendations) supported those changes.

30-07-20 POLICY

To meet the semi-annual reporting requirements of the Act, it is OAS policy to report questioned costs, including unsupported costs, and funds-put-to-better-use identified in individual audits, and to record that information in WebAIMS.

When an audit cannot identify an exact amount of questioned costs or cannot conclude that costs were or were not claimed in violation of applicable criteria, OAS may recommend that HHS management determine the amount that should be disallowed. OAS refers to such a recommendation as a set-aside and does not report the set-aside in the Semiannual Report to Congress.

The most common situation in which a set-aside may be appropriate is when the OIG cannot conclude that costs were or were not claimed in accordance with applicable criteria, generally because of conflicting guidance.

A set-aside recommendation may only be reported and coded in WebAIMS with the approval of the DIG or AIG.

Cost savings generally represent third-party estimates of funds made available for better use through reductions in Federal spending, deobligation of funds, and/or avoidance of unnecessary expenditures. To identify legislative savings, OAS uses estimates that the Congressional Budget Office prepares to inform Congress of the potential impact of legislation under consideration. To identify administrative savings, the OAS uses estimates developed by or in consultation with the OPDIVS.[1]

[1] These cost savings are not coded by the audit team at the time a report is issued.

30-07-30 REPORTING AND CODING MONETARY RECOMMENDATIONS

Individual audit reports may include three types of monetary recommendations: questioned costs (including unsupported costs), funds-put-to-better-use, and set-aside costs.

30-07-30-01 Questioned Costs

The OAS reports monetary recommendations as questioned costs when it concludes there have been alleged violations of criteria, including a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds. Recommendations related to costs that were not allowable as charges to the contract or program reviewed but that could be charged to other Federal Government contracts or programs should also be coded as questioned costs.

Questioned costs that **are not** unsupported costs are coded in WebAIMS as "01-Questioned costs."

Questioned costs that **are** unsupported costs are coded in WebAIMS as either "17-Provide documentation or make financial adjustment," or "18-Obtain approval or make financial adjustments." These codes indicate that the costs are both questioned and unsupported and ensure that they are reported accordingly in the Semiannual Report to Congress.

30-07-30-02 Funds Put to Better Use

The OAS reports monetary recommendations as funds-put-to-better-use when it concludes that funds could be used more efficiently if management of an establishment took actions to implement and complete the recommendation, including:

- reductions in outlays;
- deobligation of funds from programs or operations;
- withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds;
- costs not incurred by implementing recommended improvements related to the operations of the establishment, a contractor, or grantee;
- avoidance of unnecessary expenditures noted in preaward reviews of contract or grant agreements; or
- any other savings which are specifically identified.

The following are specific examples of the types of recommendations that should generally be reported as funds-put-to-better-use:

- Recommendations expected to result in the Department avoiding costs in future years;
- Recommendations to reduce proposed costs in bid proposal audits;
- Recommendations in roll-up reports related to costs that the Department avoided based on individual recipient capability audits; and

- Recommendations in pension related audits that auditees identify unallowable pension costs.

The WebAIMS code used for funds-put-to-better-use is “02-Funds Put to Better Use.”

OAS does not use the term funds-put-to-better-use in individual audit reports but identifies as funds-put-to-better-use costs that could have been saved or avoided.

30-07-30-03 Set-Aside Costs

When an audit cannot identify an exact amount of questioned costs or cannot conclude that costs were or were not claimed in accordance with applicable criteria, the audit team may consider obtaining DIG or AIG approval to report the costs as a set-aside. The most common situation in which reporting a set-aside may be appropriate iswhen there is conflicting guidance. A description of this situation follows.

An OPDIV provided inconsistent or conflicting guidance to auditees and it is not reasonable to conclude that what the auditee did was wrong. For example, *Review of a Sponsor’s Direct and Indirect Remuneration Reports for Payment Reconciliation for Contract Year 20XX* contained the following explanation:

> We could not determine whether the Sponsor complied with Federal requirements for reporting rebates in its contract year 20XX DIR reports. The Sponsor reported all rebates that it received, but the Sponsor did not report a portion of its rebates retained by its PBM. CMS guidance addressed reporting manufacturer rebates retained by PBMs; however, the guidance contained unclear language. The Sponsor interpreted the guidance as allowing it to report only the rebates that it received. We could not express an opinion on whether the Sponsor’s decision to exclude rebates retained by its PBM complied with Federal requirements for reporting rebates.

The WebAIMS code used for Set-Asides is “03-Unable to express opinion.” This code may only be used when the DIG or AIG has approved use of a set-aside.