

SEPTEMBER 26, 2013

AUDIT REPORT

OFFICE OF AUDITS

NASA'S COMPLIANCE WITH EXECUTIVE
ORDER 13526: CLASSIFIED NATIONAL
SECURITY INFORMATION

OFFICE OF INSPECTOR GENERAL



National Aeronautics and
Space Administration

Final report released by:



Paul K. Martin
Inspector General

Acronyms

CIGIE	Council of the Inspectors General on Integrity and Efficiency
CFR	Code of Federal Regulations
DOD	Department of Defense
FY	Fiscal Year
NPR	NASA Procedural Requirements
OIG	Office of Inspector General
OCA	Original Classification Authority
OPS	Office of Protective Services

OVERVIEW

NASA'S COMPLIANCE WITH EXECUTIVE ORDER 13526: CLASSIFIED NATIONAL SECURITY INFORMATION

The Issue

In December 2009, the President signed Executive Order 13526, “Classified National Security Information” (Order), to reform the security classification and declassification processes.¹ The Order was intended to produce greater openness and transparency in the Government’s classification and declassification programs while maintaining the Government’s legitimate interests to protect certain information from unauthorized disclosure.

Public Law 111-258, “Reducing Over-Classification Act” of 2010, requires the Inspector General of each Federal department or agency with an employee who is authorized to make original classifications to assess agency compliance with the Order.² In response to the Act, we (1) assessed whether NASA has adopted, followed, and effectively administered classification policies, procedures, rules, and regulations and (2) identified policies, procedures, rules, regulations, or management practices that may be contributing to misclassification of material at the Agency. In accordance with the Act, we will conduct a second evaluation by September 30, 2016, to review the actions NASA takes in response to this review. Details on the scope and methodology for our review can be found in Appendix A.

Results

NASA has adopted classification policies and issued regulations that comply with security classification reform requirements. Specifically, NASA has established procedural requirements for the proper implementation and management of a uniform system for classifying, accounting for, safeguarding, and declassifying national security information under its control. However, while the Agency’s procedures meet Federal requirements, its implementing directive does not require Agency personnel with classification authority to receive all necessary training. Additionally, we found instances in which Agency personnel were not consistently following these NASA policies. Specifically, we found classified documents that were improperly marked,

¹ Classified national security information or classified information means information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure. Classification means the act or process by which information is determined to be classified information. Declassification means the authorized change in the status of information from classified information to unclassified information.

² “Reducing Over-Classification Act” of 2010, Public Law 111-258, 111th Congress (October 7, 2010).

training requirements that were not met, and self-inspections that were not fully implemented. Although these deficiencies were relatively minor in nature, failure to comply with these requirements increases the risk that personnel may inadvertently misclassify material.

Management Action

We recommended that the NASA Assistant Administrator for Protective Services revise NASA's classification implementing policy so it is consistent with the Order. In addition, we recommended the Assistant Administrator ensure that persons with classification authority receive all required training and the Agency's self-inspection program identifies and mitigates future occurrences of marking and training deficiencies.

In response to our draft report, the Assistant Administrator for Protective Services concurred with our recommendations. Specifically, the Office of Protective Services (OPS) agreed to revise NASA policy to clarify that individuals who apply derivative classification markings must receive the required training prior to classifying any information. Additionally, the Assistant Administrator will issue an interim policy to all Centers containing the revised mandatory requirements. Further, to improve the Agency's self-inspection program OPS will formalize criteria for annual Center self-inspections, provide self-inspection sheets for tracking purposes, and measure the Centers' progress as part of the Integrated Security Functional Reviews. We consider the proposed actions to be responsive and will close the recommendations upon completion and verification of the corrective actions. Management's full response is reprinted in Appendix B.

CONTENTS

INTRODUCTION

Background _____	1
Objectives _____	3

RESULTS

NASA's Policies Comply with Requirements of Executive Order 13526 _____	4
NASA Does Not Consistently Follow Federal Requirements for Classifying National Security Information _____	6

APPENDIX A

Scope and Methodology _____	11
Review of Internal Controls _____	12
Prior Coverage _____	12

APPENDIX B

Management Comments _____	13
---------------------------	----

APPENDIX C

Report Distribution _____	15
---------------------------	----

INTRODUCTION

Background

The over-classification of information can interfere with accurate, actionable, and timely information sharing; increase the cost of information security; and needlessly limit stakeholder and public access to information. Executive Order 13526, “Classified National Security Information” (Order), was intended to ensure greater openness and transparency in Federal classification and declassification programs while maintaining the legitimate interests of the United States in protecting certain information from unauthorized disclosure. In June 2010, the Information Security Oversight Office (Oversight Office) published guidance to assist agencies in implementing the Order and to provide direction related to classifying, downgrading, declassifying, and safeguarding national security information.³ This guidance included rules for:

- classification, declassification, and marking principles;
- safeguarding classified information;
- agency security education and training programs;
- agency self-inspection programs; and
- reporting requirements.⁴

Classified information must be marked appropriately to indicate its status. The three classification levels are:

- *Top Secret* – as determined by the original classification authority, the unauthorized disclosure of such information could reasonably be expected to cause *exceptionally grave damage* to national security.
- *Secret* – as determined by the original classification authority, the unauthorized disclosure of such information could reasonably be expected to cause *serious damage* to national security.

³ The Oversight Office, a component of the National Archives and Records Administration, is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program. Specifically, the Oversight Office’s Classification Management Staff develops security classification policies for classifying, declassifying, and safeguarding national security information.

⁴ 32 Code of Federal Regulations (CFR) Parts 2001 and 2003, “Classified National Security Information: Final Rule” (2010).

- *Confidential* – as determined by the original classification authority, the unauthorized disclosure of such information could reasonably be expected to cause *damage* to national security.

Over-Classification. The Order defines over-classification as classification of information that does not meet one or more of the following standards:

- an original classification authority (OCA) has classified the information;⁵
- the information is owned by, produced by or for, or under the control of the U.S. Government;
- the information falls within one or more of seven categories of information;⁶ and
- the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to national security and the original classification authority is able to identify or describe the damage.

Original and Derivative Classification Actions. Information may be classified either originally or derivatively. Original classification means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure. Derivative classification means incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Persons who reproduce, extract, or summarize classified information or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. Information may be derivatively classified from a source document or documents or based on a classification guide.⁷

⁵ Original classification authority means an individual authorized in writing by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

⁶ These categories are: (1) military plans, weapons systems, or operations; (2) foreign government information; (3) intelligence activities; (4) foreign relations or foreign activities of the United States; (5) scientific, technological, or economic matters relating to the national security; (6) U.S. Government programs for safeguarding nuclear materials or facilities; (7) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or (8) the development, production, or use of weapons of mass destruction.

⁷ Source document means an existing document containing classified information that is incorporated, paraphrased, restated, or generated in new form into a new document. Classification guide means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Objectives

Pursuant to the “Reducing Over-Classification Act” of 2010, the NASA Office of Inspector (OIG) evaluated NASA’s system for classifying, safeguarding, and declassifying national security information. Our objectives were to:

- assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within NASA; and;
- identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within NASA.

See Appendix A for details of the evaluation’s scope and methodology, our review of internal controls, and a list of prior coverage.

NASA'S POLICIES COMPLY WITH REQUIREMENTS OF EXECUTIVE ORDER 13526

NASA has adopted classification policies and issued regulations that comply with the requirements of Federal security classification reform requirements. Specifically, NASA Procedural Requirements (NPR) 1600.2, "NASA Classified National Security Information," establishes Agency procedures for the proper implementation and management of a uniform system for classifying, accounting, safeguarding, and declassifying national security information generated by or in the possession of NASA. Based on our review of NPR 1600.2, we concluded that NASA complied with Executive Order 13526 and the Oversight Office's implementing directive, 32 CFR Part 2001. The Order sets forth criteria agencies must meet to comply, and, as illustrated in Table 1, NASA met all applicable criteria.

Table 1: Compliance Summary	
Criteria for Compliance	Criteria Met?
Does the NPR cite Executive Order 13526 and 32 CFR, Part 2001 for authorizing NASA Classified National Security Information Program?	Yes
Does the NPR require the senior agency official to direct and administer the program?	Yes
Does the NPR cite the classification standards?	Yes
Are the classification levels provided and only the three levels authorized for use?	Yes
Does the NPR emphasize the 25-year automatic declassification and downgrading of NASA Classified National Security Information?	Yes
Does the NPR require the agency to establish a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency?	Yes
Does the agency submit annual Standard Form 311 to Information Security Oversight Office?	Yes

Source: NASA OIG's review of NPR 1600.2

The Assistant Administrator for Protective Services is the Senior Agency Official responsible for providing direction, oversight, and implementation guidance for NASA's information security program.⁸ Further, individual Center Directors are responsible, through their respective Center Chief of Security, for ensuring proper planning and implementation of the Order and managing classified information and material under the jurisdiction and custody of their respective Centers.

NASA's Classification Activity. As required by the Order and the implementing directive, NASA submits annual reports on original and derivative classification decisions made by its personnel, declassification activities, and any classification guides it creates or uses.⁹ Four positions at NASA possess original classification authority: the Administrator, Deputy Administrator, Associate Administrator, and Assistant Administrator for Protective Services.

For fiscal years (FY) 2010 through 2012, NASA reported making no original classification decisions. However, during that period, 59,284 derivative classification decisions were made Agency-wide – 390 Top Secret, 58,795 Secret, and 99 Confidential.¹⁰ NASA Office of Protective Services (OPS) officials told us that the majority of the 59,284 classification decisions made across the Agency for FYs 2010, 2011, and 2012 related to Sensitive Compartmented Information or Special Access Program documents.¹¹ In addition, the Agency reported declassifying 938 pages of information as a result of mandatory declassification reviews, 40,872 pages by automatic declassification, and 200 pages as a result of systematic declassification reviews.¹²

⁸ Aeronautics and Space Information Security Program, 14 CFR Part 1203-Information Security Program, Executive Order 13526.

⁹ *Agency Security Classification Management Program Data* (Standard Form 311).

¹⁰ Approximately 98 percent of these decisions were made by personnel assigned to NASA Headquarters.

¹¹ Sensitive Compartmented Information is a classification level for information, generally intelligence-related, requiring security clearances and physical or procedural security measures above those established for collateral classified information or Special Access Program information. Special Access Program means any program established and approved under Executive Order Number 13526 that imposes need-to-know or access controls beyond those normally required for access to collateral Top Secret, Secret, or Confidential information.

¹² Mandatory declassification review means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of the Order. Automatic declassification means the declassification of information based solely upon the occurrence of a specific date or event as determined by the OCA or the expiration of a maximum timeframe for duration of classification established under the Order. Systematic declassification review means the review for declassification of classified information contained in records that have been determined by the Archivist (National Archives and Records Administration) to have permanent historical value in accordance with Title 44, U.S. Code.

NASA DOES NOT CONSISTENTLY FOLLOW FEDERAL REQUIREMENTS FOR CLASSIFYING NATIONAL SECURITY INFORMATION

Although NASA's policies and procedures for managing national security information comply with Federal requirements, we found instances where Agency personnel did not consistently follow these policies. Specifically, we found classified documents that were improperly marked, training requirements for classifiers that were not met, and self-inspections that were not fully implemented. Although these deficiencies were relatively minor in nature, failure to comply with them increases the risk that personnel may inadvertently misclassify material.

Classified Documents Improperly Marked

As part of our review, we examined the classification markings on 16 documents NASA personnel derivatively classified and found several minor marking deficiencies. Federal requirements dictate that derivative classification markings shall:

- include the date of origin of the document in a manner that is immediately apparent;
- identify the derivative classifier;
- eliminate the use of the exemption markings on documents created on or after September 22, 2003, and declassify those documents 25 years from date of document creation; and
- include a listing of the source materials on, or attached to, each derivatively classified document when a document is classified derivatively on the basis of more than one source – “*Derived From: Multiple Sources.*”

For the 16 documents we examined, we found the following deficiencies:

- 2 documents had no date of origin;
- 3 documents did not identify the derivative classifier;

- 12 documents, created after September 22, 2003, contained invalid exemption markings on the “*Declassify On*” date line; and¹³
- 1 document –marked “*Derived From: Multiple Sources*” – did not include a listing of the source materials.

Training Requirements Not Fully Met

Federal regulations require that all persons with OCA must receive training on proper classification prior to originally classifying information and at least once per year thereafter. Likewise, persons who apply derivative classification markings must receive training in the proper application of the derivative classification principles before derivatively classifying any information and at least once every 2 years thereafter. The regulations state that, at a minimum, the training shall cover the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

During 2012, three of the four NASA OCAs received in-person training. The Deputy Administrator was unavailable for the training, but did not perform any original classification decisions during that period.

We spoke with two NASA employees who had derivatively classified documents during 2012. We found that while both individuals completed the mandatory annual security education training refresher, only one had received specific derivative classification training. In addition, neither individual had received the required bi-annual derivative classification training. Furthermore, we found that NASA policy does not stipulate that employees receive training on derivative classification principles before they classify any information as required by the implementing directive for the Order, the Oversight Office Directive Number 1 (32 CFR Part 2001, “Classified National Security Information”).¹⁴

Self-Inspection Requirements Not Fully Implemented

We also found that NASA has not fully implemented Federal self-inspection requirements. Federal regulations require that senior agency officials establish and maintain an ongoing self-inspection program that includes regular reviews of

¹³ NASA personnel acknowledged the use of specific exemption categories is no longer a valid declassification marking on documents created on or after September 22, 2003. NASA personnel explained that the “X1” exemption category is a default system function designed by the originators of the NASA investigative management system currently in use to comply with an earlier executive order. In response to our inquiry regarding the use of the “X1” markings, NASA personnel stated that the system administrators for the current investigative management system have been directed to take immediate action to remove the default “X1” markings from the system and comply with current guidance in the implementing directive.

¹⁴ 14 CFR Part 1203.500(d) – *Information Security Program* and NPR 1600.2, Chapter 2.3.2 require individuals who apply derivative classification markings receive training, at least once every 2 years, in the proper application of the derivative classification principles of Executive Order No. 13526, but unlike 32 CFR Part 2001.70(d)(4) do not require training prior to derivatively classifying information.

representative samples of the Agency's original and derivative classification actions. The self-inspections should evaluate adherence to the principles and requirements of the Federal regulations and the effectiveness of agency programs covering original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management oversight. The self-inspections must be regular, ongoing, and occur at least annually.¹⁵

Further, NASA policy requires Center Directors, through their Chiefs of Security, to conduct periodic reviews of NASA organizational units involved with original and derivative classification work to ensure compliance with Federal regulations.¹⁶ Specifically, each Center Protective Services Office is required to conduct audits of select Center organizations on a yearly basis to determine if they are complying with NASA policy.

However, based on summary data provided by OPS, 6 of 12 NASA locations did not report conducting any audits of select organizations during FY 2010 through 2012.¹⁷ Moreover, although OPS conducts functional reviews every 3 years to provide oversight of the Centers' classification activities, we found that the 2012 review did not examine important aspects of NASA's classification program, including whether classified documents were properly marked or whether classifiers were properly trained.

Conclusion

Although NASA has sound policies in place to manage its classified material, improved compliance with its policies regarding marking documents, training classification officials, and performing self-inspections would better position the Agency to ensure that classified national security information is managed in accordance with Executive Order 13526 requirements. This, in turn, would better ensure that NASA is acting in accordance with Federal guidelines that seek greater openness and transparency in agency classification and declassification programs.

¹⁵ 32 CFR Part 2001.60(a)(b)(c)(d).

¹⁶ Center Chief of Security means the senior Center official responsible for management of the Center's security program.

¹⁷ Kennedy Space Center, Glenn Research Center, Langley Research Center, Dryden Flight Research Center, Johnson Space Center, and Marshall Space Flight Center provided reports of annual audits. Conversely, Goddard Space Flight Center, Stennis Space Center, White Sands Test Facility, NASA Headquarters, Jet Propulsion Laboratory and Ames Research Center did not provide any reports of annual audits of select organizations.

Recommendations, Management's Response, and Evaluation of Management's Response

In order to ensure that NASA complies with security classification requirements, we recommended that the NASA Assistant Administrator for Protective Services take the following actions:

Recommendation 1. Revise 14 CFR 1203 and NPR 1600.2 to require that persons who apply derivative classification markings receive training in the proper application of the derivative classification principles prior to classifying any information.

Management's Response. The Assistant Administrator concurred, agreeing to revise 14 CFR 1203 and NPR 1600.2 to clarify that individuals who apply derivative classification markings must receive the required training prior to classifying any information.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the corrective actions.

Recommendation 2. Coordinate with Center Chiefs of Protective Services to ensure that persons who apply derivative classification markings receive training before classifying any information and refresher training at least every 2 years thereafter.

Management's Response. The Assistant Administrator concurred, stating that OPS will issue an interim policy letter to all Centers and revise NPR 1600.2 to clarify that individuals must complete training prior to classifying any information as well as (at a minimum) every 2 years thereafter.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the corrective actions.

Recommendation 3. Ensure that the Agency self-inspection program includes regular reviews of NASA's derivative classification actions sufficient to identify and mitigate classification marking and training deficiencies.

Management's Response. The Assistant Administrator concurred, stating that OPS will formalize criteria for annual Center self-inspections, provide self-inspection sheets for tracking purposes, and measure the Centers' progress as part of the Integrated Security Functional Reviews.

Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the corrective actions.

Scope and Methodology

We performed this audit from July 2013 through September 2013 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.

Public Law 111-258, “Reducing Over-Classification Act” of 2010, requires Inspectors General coordinate with each other and with the Oversight Office to ensure that evaluations of principles, policies, and procedures for NASA Classified National Security Information follow a consistent methodology, as appropriate, that allows for cross-agency comparisons. Accordingly, we contacted the Oversight Office and requested copies of Inspectors General reports it had received. Additionally, we reviewed the audit reports issued by two Inspectors General.

At the request of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Inspection and Evaluation Committee and with the approval of the CIGIE Executive Council, the Department of Defense (DOD) OIG led a working group consisting of other OIGs in developing detailed guidance for OIGs to use, where appropriate, in evaluating their agencies processes for following Executive Order 13526, “Classified National Security Information,” and its implementing directive, 32 CFR Part 2001, “Classified National Security Information.”¹⁸ In part, we used the DOD evaluation guide to interview with the Assistant Administrator for Protective Services, one of four NASA original classification authorities; interview two derivative classifiers; and evaluate the extent that NPR 1600.2 adequately prescribes policy and procedures that, if effectively followed, meet requirements of the Order and its implementing directive. We also requested supporting documentation, to substantiate the completion of required derivative classification training.

To identify the number of original and derivative classification decisions and declassification actions made Agency-wide, we reviewed NASA’s Standard Form 311 “Agency Security Classification Management Program Data,” that had been submitted to the Oversight Office for FYs 2010, 2011, and 2012.

NASA had no original classifications during FYs 2010, 2011, and 2012. To identify the propriety of classification markings, we reviewed 16 derivatively classified documents.

¹⁸ On behalf of CIGIE, DOD OIG issued *A Standard User’s Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the “Reducing Over-Classification Act,”* on January 22, 2013.

We reviewed the Agency-wide self-inspection reports submitted to the Oversight Office for FYs 2011 and 2012. Also, we requested copies of NASA Headquarters Center inspection reports for FYs 2010, 2011, and 2012 that had been submitted to NASA OPS.

Use of Computer-Processed Data. NASA Counterintelligence Program personnel printed and provided hard copies of 12 documents that were maintained in their electronic investigative database so that we could examine the propriety of the documents' classification markings. We did not verify the hard copy documents to the source documents, but considered the documents that we examined reliable for the purposes of the review.

Review of Internal Controls

We reviewed 14 CFR 1203 and NPR 1600.2 to determine if NASA's prescribed policy and procedures are consistent with the requirements of the Order and the implementing directive. We interviewed an original and two derivative classification authorities and determined whether they had adequate knowledge and were following the NASA Classified National Security Information requirements of NPR 1600.2, the Order, and the implementing directive. We reviewed classified documents to determine if they were properly marked and being appropriately declassified. Also, we determined if NASA personnel that classified documents were completing required training. We found that NASA needs to improve some internal controls as discussed in the body of this audit report.

Prior Coverage

During the last 5 years, the OIGs of the Department of State and the Broadcasting Board of Governors and the Department of Health and Human Services have issued three reports of particular relevance to the subject of this report. Unrestricted reports can be accessed over the Internet at <http://oig.state.gov/latest/> and <http://oig.hhs.gov/oei/reports/>.

United States Department of State and the Broadcasting Board of Governors OIG

“Evaluation of Department of State Implementation of Executive Order 13526, Classified National Security Information” (AUD-SI-13-22, March 2013)

Department of Health and Human Services OIG

“HHS Adopted, Administered, and Generally Followed Classified Information Policies” (OEI-07-12-00400, May 2013).

“Originally and Derivatively Classified Documents Met Most Federal Requirements” (OEI-07-12-00401, May 2013).

MANAGEMENT COMMENTS

National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001



September 25, 2013

Reply to Attn of: Office of Protective Services

TO: Assistant Inspector General for Audits
FROM: Assistant Administrator for Protective Services
SUBJECT: Response to OIG Draft Audit Report, "NASA's Compliance with Executive Order 13526: Classified National Security Information" (Assignment Number A-13-017-00)
REF: OIG memorandum of September 11, 2013 forwarding the subject audit report

The Office of Protective Services (OPS) appreciates the opportunity to review your draft report entitled, "NASA's Compliance with Executive Order 13526: Classified National Security Information" (Assignment No. A-13-017-00).

In the draft report, the Office of the Inspector General (OIG) articulates that although NASA has sound policies in place to manage its classified material, improved compliance with its policies regarding marking documents, training classification officials, and performing self-inspections would better position the Agency to ensure that classified national security information is managed in accordance with Executive Order 13526 requirements. NASA's response to the recommendations, including planned corrective actions, follows:

Recommendation 1: Revise 14 CFR 1203 and NPR 1600.2 to require that persons who apply derivative classification markings receive training in the proper application of the derivative classification principles prior to classifying any information.

Management's Response: NASA concurs with this recommendation. OPS concurs with the OIG recommendation to revise 14 CFR 1203 and NPR 1600.2 to clarify that individuals who apply derivative classification markings must receive the required training prior to classifying any information. As an administrative comment, 14 CFR 1203 grants its authorities mainly by reference; not by detailed, in-document descriptors. NPR 1600.2 is referenced directly in 14 CFR 1203. As a result, it should be noted that while the revision to the NPR will be more detailed, the corresponding revision to the CFR will be nominal and administrative. Estimated completion date to accomplish both the CFR revision and the NPR revision in support of the OIG recommendation is April 30, 2015.

2

Recommendation 2: Coordinate with Center Chiefs of Protective Services to ensure persons who apply derivative classification markings receive training before classifying any information and at least once every 2 years thereafter.

Management's Response: NASA concurs with this recommendation. The OPS will revise NPR 1600.2 to clarify that individuals must complete training prior to classifying any information as well as (at a minimum) receive training once every two years thereafter. As this change to NPR 1600.2 will be included with the modification from Recommendation 1, the estimated completion date is September 30, 2014.

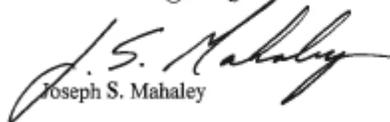
In the interim, the Assistant Administrator for Protective Services will issue a policy letter to all Centers stating the mandatory requirements that will be contained in the revised NPR 1600.2. The policy letter will be issued by October 31, 2013.

Recommendation 3: Ensure that the agency self-inspection program includes regular reviews of the agency's derivative classification actions sufficient to identify and mitigate classification marking and training deficiencies.

Management's Response: NASA concurs with this recommendation. The OPS will formalize annual self-inspection criteria for NASA Centers and provide self-inspection sheets for tracking purposes. While the Centers will be responsible for monitoring their own classification actions utilizing this new criteria, the OPS will follow up as part of the Integrated Security Functional Reviews that are conducted each Center. The metrics will appear in the final reports that are generated following the Functional Reviews. The estimated completion date for the development and issuance of the self-inspection sheets to the Centers is March 31, 2014.

As requested in the referenced OIG memorandum, the OPS performed a sensitivity review of the information contained in the draft report. This office's determination is that there is no data contained in the report that was deemed as not releasable to the public.

Again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Mr. Mark Dodd, OPS Executive Officer, at (202) 358-1255 or Mark.R.Dodd@nasa.gov.



Joseph S. Mahaley

cc:
OPS/C. Lombard
OPS/S. Peyton
OPS/M. Dodd
OPS/L. Matthews

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Associate Administrator
Chief of Staff
Assistant Administrator for Protective Services
NASA Advisory Council's Audit, Finance, and Analysis Committee

Non-NASA Organizations and Individuals

Office of Management and Budget
Deputy Associate Director, Energy and Science Division
Branch Chief, Science and Space Programs Branch
Government Accountability Office
Director, Office of Acquisition and Sourcing Management
National Archives and Records Administration
Director, Information Security Oversight Office

Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies
Senate Committee on Commerce, Science, and Transportation
Subcommittee on Science and Space
Senate Committee on Homeland Security and Governmental Affairs
Senate Select Committee on Intelligence
House Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies
House Committee on Homeland Security
House Committee on Oversight and Government Reform
Subcommittee on Government Operations
House Committee on Science, Space, and Technology
Subcommittee on Oversight
House Permanent Select Committee on Intelligence
Subcommittee on Space

Major Contributors to the Report:

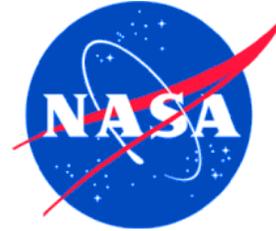
Ridge Bowman, Director, Space Operations Directorate

Kenneth Sidney, Project Manager

Ellis Lee, Lead Auditor

Gene Bauer, Auditor

Cedric Campbell, Associate Counsel to the Inspector General



OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit <http://oig.nasa.gov/audits/reports/FY13/> to obtain additional copies of this report, or contact the Assistant Inspector General for Audits at 202-358-1232.

COMMENTS ON THIS REPORT

In order to help us improve the quality of our products, if you wish to comment on the quality or usefulness of this report, please send your comments to Mr. Laurence Hawkins, Audit Operations and Quality Assurance Director, at Laurence.B.Hawkins@nasa.gov or call 202-358-1543.

SUGGESTIONS FOR FUTURE AUDITS

To suggest ideas for or to request future audits, contact the Assistant Inspector General for Audits. Ideas and requests can also be mailed to:

Assistant Inspector General for Audits
NASA Headquarters
Washington, DC 20546-0001

NASA HOTLINE

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD). You may also write to the NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026, or use <http://oig.nasa.gov/hotline.html#form>. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.