Description of document: Report No. OIGE-13-09 National Geospatial-Intelligence Agency (NGA) Office of Inspector General (OIG) Implementation of the Reducing Over-Classification Act, 2013

Request date: 2014

Released date: 14-May-2014

Posted date: 30-June-2014

Source of document: National Geospatial-Intelligence Agency
FOIA Requester Service Center
7500 GEOINT Drive, MS S01-EGM
Springfield, Virginia 22150-7500
Fax: 571-558-3130

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
7500 GEOINT Drive
Springfield, Virginia 22150

U-099-14/OIG

May 14, 2014

SUBJECT: Freedom of Information Act Request for Report No. OIGE-13-09
(FOIA 20140104F)

This is in response to your request for Report No. OIGE-13-09 (NGA's Implementation of the Reducing Over-Classification Act) closed by the National Geospatial-Intelligence Agency (NGA), Office of Inspector General.

Attached is a redacted copy of the NGA OIGE Report dated September 2013. Note, the identities of any individuals who may have been identified in the Report along with any information that might identify an organization within NGA were redacted in accordance with FOIA exemption (3) (material exempted from disclosure by statute); specifically 10 U.S.C. § 424 (limiting the release of NGA organizational and personnel information).

You may appeal these redactions in writing to the NGA Inspector General, the appellate authority, within 60 days from the date of this letter. The appeal, which should reference the above FOIA request number, may be sent to the Inspector General, National Geospatial-Intelligence Agency, Mail Stop N75-OIGC, 7500 GEOINT Drive, Springfield, VA 22150. Please include a copy of this letter with your appeal.

Fees associated with processing your FOIA request have been waived.

Sincerely,

Lenore N. Guthrie
Assistant Inspector General
for Plans and Programs
Initial Denial Authority

Enclosure as stated

cc:
SISCC

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

Know the Earth... Show the Way... Understand the World

Office of Inspector General

Inspections Division

(U) NGA's Implementation of the Reducing Over-Classification Act

Report No. OIGE-13-09

September 2013

(U) Questions, Copies, Suggestions

(U) The Inspections Division, Office of Inspector General, NGA, prepared this report. If you have questions about the report or want to obtain additional copies, contact the Office of Inspector General, NGA.

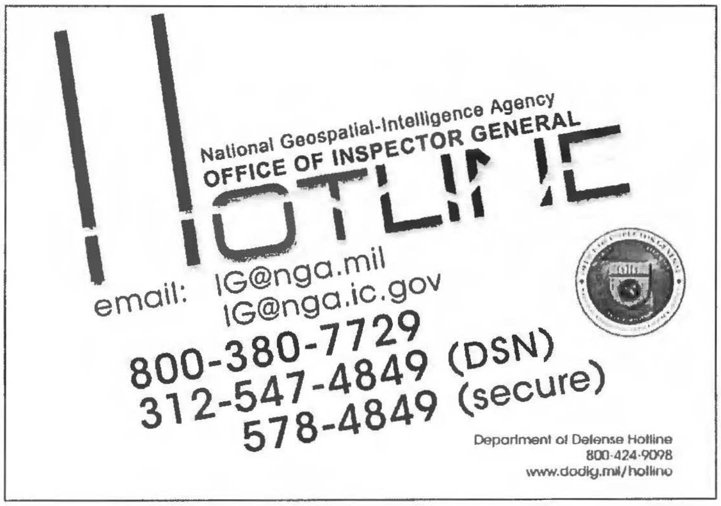
(U) To suggest ideas for or request future inspections of NGA issues, contact the Office of Inspector General, NGA:

Telephone: 571-557-7500 • (DSN 547-7500)

Fax (unclassified): 571-558-3273 • (DSN 547-3273) • (secure) 571-558-1035

e-mail: ig@nga.mil

Mail: National Geospatial-Intelligence Agency
Attention: Inspector General
Mail Stop N-75
7500 GEOINT Drive
Springfield, VA 22150



National Geospatial-Intelligence Agency
OFFICE OF INSPECTOR GENERAL
HOTLINE

email: IG@nga.mil
IG@nga.ic.gov

800-380-7729
312-547-4849 (DSN)
578-4849 (secure)

Department of Defense Hotline
800-424-9098
www.dodig.mil/hotline

(U) This is a National Geospatial-Intelligence Agency, Office of Inspector General, document. It may contain information that is restricted from public release by Federal law. Recipients of this document cannot further release it or its contents to anyone not having an official need to know without the express consent of the NGA Inspector General.

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
7500 GEOINT Drive
Springfield, Virginia 22150

SEP 27 2013

MEMORANDUM FOR [redacted]

SUBJECT: (U) Final Inspection Report, Implementation of the Reducing Over-Classification Act (Report No. OIGE-13-09)

1. (U) Enclosed is the NGA Office of Inspector General report on NGA's Implementation of the Reducing Over-Classification Act. The objective of this inspection was to review NGA's classification management policies, procedures and practices, to determine the agency's compliance with Executive Order 13526 and Title 32 CFR as mandated in PL 111-258.

2. (U//~~FOUO)~~ We determined that NGA has not adopted all applicable policies, procedures, rules, and regulations. While many of the policies have been followed, the agency has not implemented all the changes required to meet the new standards, and the program is not effectively administered. We identified opportunities for improvement and provided 14 recommendations to facilitate those improvements.

3. (U//~~FOUO)~~ We request that management provide a detailed plan of action and milestones (POA&M) for implementing each recommendation no later than 30 December 2013. The POA&M will provide the basis for quarterly follow-up on management actions.

4. (U//~~FOUO)~~ We appreciate the courtesies extended to the OIG staff. If you have questions or concerns, please contact [redacted]

Dawn R Eilenberger
Dawn R. Eilenberger
Inspector General

Results in Brief: Review of NGA's Implementation of the Reducing Over-Classification Act

(U) What We Did

(U//~~FOUO~~) We reviewed NGA's classification management policies, procedures and practices to determine the agency's compliance with EO 13526 and Title 32 CFR as mandated in PL 111-258. The team had two objectives: (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within NGA, and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within NGA.

(U) What We Found

- (U//~~FOUO~~) NGA's Security Education and Training Program does not effectively train all personnel authorized to handle classified information in accordance with established requirements.
- (U//~~FOUO~~) NGA's Original Classification Authority Program lacks rigor.
- (U//~~FOUO~~) NGA does not have a formal process for challenging original classification decisions.
- (U//~~FOUO~~) NGA-produced security classification guides do not incorporate all required classification guidelines.
- (U//~~FOUO~~) NGA does not have a fully established self-inspection program.

(U) What We Recommend

(U) On the basis of the inspection results, we made the following recommendations:

(U) For the [redacted]

(U//~~FOUO~~) Restructure initial security training, including all required training areas.

(U//~~FOUO~~) In coordination with the [redacted] conduct a resource assessment of the initial security training to determine the length of time required to sufficiently instruct new employees on required security policies, principles and practices. Consider creating a separate block of instruction focused specifically on classification management-related requirements.

(U//~~FOUO~~) Establish training for the derivative classification authority separate from the annual security refresher training. Include clear objectives and instruction on the principles of derivative classification and incorporate all mandatory minimum topic areas.

(U//~~FOUO~~) Incorporate and track the biennial DCA training requirement as a separate entry in the current PeopleSoft tracking system.

(U//~~FOUO~~) Develop and implement a security education and training program incorporating all requirements for individuals who have significant duties in managing and overseeing classified information.

(U//~~FOUO~~) Review the current OCA training plan and develop a more comprehensive briefing outlining the step-by-step duties and responsibilities of OCAs. Expand the 30-minute OCA training window to allow for more detailed training and discussions.

(U//~~FOUO~~) Establish a verifiable mechanism to monitor and track OCA annual training through PeopleSoft.

(U//~~FOUO~~) Develop and implement a process to hold personnel accountable for noncompliance with mandated training requirements and suspend classification authorities when appropriate.

(U//~~FOUO~~) Establish a classification challenge system for processing, tracking and recording formal classification challenges. Promulgate the procedures to all OCAs and include in their required annual training.

(U//~~FOUO~~) Insert a Change Request Form in all security classification guides. Include a brief instruction on how to challenge a classification decision.

(U//~~FOUO~~) Incorporate the classification challenge process into the initial security classification and derivative classification training curricula.

(U//~~FOUO~~) Review and update all security classification guides and implement a quality control mechanism to ensure every guide contains mandatory elements.

(U//~~FOUO~~) Fully establish and implement a self-inspection program in accordance with EO 13526, 32 CFR, and ISOO directives.

(U//~~FOUO~~) Establish procedures to document the annual self-inspection process, including a methodology for analyzing, measuring and validating data.

(U) CONTENTS

(U) Introduction

(U) Appendixes

(U) This page intentionally left blank.

(U) INTRODUCTION

(U//~~FOUO~~) We reviewed NGA's classification management policies and practices to determine whether they ensure proper classification and marking of classified national security information (CNSI). We focused on two objectives as described below. Based on the inspection results, we made 14 recommendations (see appendix A). The scope and methodology are presented in appendix B.

(U) Background

(U) Context of the Inspection

(U) The NGA Inspector General (IG) initiated this inspection based on a Congressionally Directed Action. In October 2010, the President signed Public Law 111-258, Reducing Over-Classification Act. The act was designed to address issues that the National Commission on Terrorist Acts Upon the United States (9/11 Commission) highlighted regarding the over-classification of national security information and to promote information sharing across the Federal Government and with state, local, tribal, and private sector entities. The act also mandated that the IG of each Federal department or agency with officers or employees who are authorized to make original classification decisions review classification management policies and practices within their agency and assess whether they ensure the proper classification and marking of information. The act established specific reporting deadlines. The first evaluation is to be completed by 30 September 2013, and the second by 30 September 2016. The evaluation reports will be distributed to the Congressional committees listed in appendix F.

(U//~~FOUO~~) The Intelligence Community Inspector General (IC IG) initiated a joint effort to coordinate with the IGs executing evaluations under PL 111-258 and with the Information Security Oversight Office (ISOO) to ensure the evaluations follow a consistent methodology that allows for cross-agency comparisons.[1] The IC IG coordinated several meetings to discuss progress and solicit ideas on standards.

(U) The Issue

(U) Executive Order (EO) 13526, Classified National Security Information, December 29, 2009, prescribes a uniform system for classifying, safeguarding, and declassifying national security information. It also expresses the President's belief that this nation's progress depends on the free flow of information, both within the government and to the American people. Accordingly, protecting information critical to national security, demonstrating a commitment to open government through accurate and accountable application of classification standards, and routine, secure, and effective declassification are equally important priorities.

[1] (U) The ISOO is a component of the National Archives and Records Administration and receives policy and program guidance from the National Security Council.

(U) Classification management and use of dissemination control markings are high-risk subjects that have drawn significant concern from Congressional oversight committees, the media, and public interest groups. Though proper classification and control of information is vital to safeguarding the nation, over-classification, as the 9/11 Commission found, jeopardizes national security by inhibiting information sharing. Over-classification or over-control of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholders' and the public's access to information. The commission also observed that over-classification is likely to increase without strong management practices, clear implementing regulations that are consistent with the policy and procedures established by EO 13526, and staff who are adequately trained on the classification process.

(U) Classification Management Program

(U//~~FOUO~~) Classification management is the management of classified national security information through its life cycle, from original classification to declassification. It includes developing classification guides that provide instructions from an original classifying authority (OCA)[2] to derivative classifiers who identify elements of information regarding specific topics that must be classified and the level and duration of classification of each element. The overall administration of the NGA Classification Management Program is the responsibility of the [redacted] The mission of the [redacted] is to ensure that information is properly labeled to allow for appropriate dissemination and protection. [redacted] serves as the classification management office for the National System for Geospatial-Intelligence (NSG) and NGA, develops security classification guides, conducts classification reviews, and manage the original classification authority program. The [redacted] manages information security performance measurement, assessment, and reporting programs. It collaborates with the classification management, counterintelligence, and security disciplines to protect critical information associated with sensitive and classified operations and activities. [redacted] also provides security education and awareness training to the NGA work force.

(U) The *NGA Security Classification Guide* is the NGA document that implements PL 111-258 in accordance with EO 13526 and Title 32 Code of Federal Regulations (32 CFR). The guide establishes procedures for classifying, downgrading, and declassifying information and for safeguarding information. It also establishes uniform classification procedures for geospatial intelligence (GEOINT)-produced national security information. NGA classifiers are responsible and accountable for the accuracy of the classification and markings they assign, whether by original or derivative classification authority.[3]

[2] (U) An OCA is an individual authorized in writing by the President, Vice President, agency heads, or other officials designated by the President to classify information in the first instance.

[3] (U) Classifiers are every NGA employee who has met the standards for access to classified information. Classifiers have the authority to apply original or derivative classification markings.

(U) Objectives

(U//~~FOUO~~) The overall purpose of the inspection was to assess NGA's classification management program and efforts to ensure compliance with applicable laws and regulations and reduce over-classification of information. Specific objectives as defined in PL 111-258 were to:

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

(U) Prior Evaluation Coverage

(U) None.

(U) Criteria

- 32 CFR § 2001 *Classified National Security Information*, Government-wide Implementation Directive for EO 13526, June 28, 2010
- DoD 5200.1-H, *DoD Handbook for Writing Security Classification Guidance*, November 1999
- DoDD 5205.07, *Special Access Program Policy*, July 1 2010
- DoD Manual 5200.01, *DoD Information Security Program: Overview: Classification, and Declassification,* February 24, 2012, vol. 1
- DoDM 5200.01, *DoD Information Security Program: Marking of Classified Information,* February 24, 2012, vol. 2
- DoDM 5200.01-V3, *DoD Information Security Program: Protection of Classified Information,* February 24, 2012, vol. 3
- DoDM 5230.30, *DoD Mandatory Declassification Review (MDR) Program*, December 22, 2011
- Executive Order 12951, *Release Of Imagery Acquired By Space-Based National Intelligence Reconnaissance Systems,* February 24, 1995
- Executive Order 13526, *Classified National Security Information*, December 29, 2009
- Intelligence Community Classification and Control Markings Implementation Manual, ver. 3.1, May 7, 2010
- Intelligence Community Authorized Classification and Control Markings - Register and Manual, ver. 6.0 February 28, 2013

- Intelligence Community Policy Guidance 710.1, *Application of Dissemination Controls: Original Controls*, July 25, 2012
- ISOO Booklet, *Marking Classified National Security Information*, January 1, 2012
- ISOO Memorandum, *Annual Senior Agency Official Self-Inspection Program Report*, 29 June 2012
- NSGM CS 9300.02, ver. 1.3, *National System for Geospatial Intelligence GEOINT Marking and Dissemination Guidance*, May 13, 2013
- Presidential Order, *Original Classification Authority*, December 29, 2009
- Public Law 111-258, *Reducing Over-Classification Act*, October 7, 2010
- U.S. Department of State Foreign Affairs Manual, 5 FAM 480, *Classifying and Declassifying National Security Information—Executive Order 13526*, June 16, 2011

(U) INSPECTION RESULTS

(U//~~FOUO~~) We found that NGA has not adopted all applicable classification policies, procedures, rules, and regulations mandated in PL 111-258, and outlined in EO 13526 and 32 CFR. While many of the policies have been followed, the agency has not implemented all of the changes required to meet the new standards. We assessed that NGA's security classification management program, while functional, is not effectively administered. We identified issues with training, including initial, OCA, and derivative classification authority (DCA);[4] compliance with OCA annual training requirements and a penalty for noncompliance; the classification challenge process; security classification guides; and the self-inspection program. In several cases, there were gaps between what the classification management team said was happening and how things actually worked. For example, compliance with all training requirements, management of the OCA program, information contained in the security classification guides, and numerous documents were said to exist but could not be produced. Therefore, we were unable to determine if agency procedures and management practices contributed to persistent misclassification of information. A small sampling of original and derivative classification actions revealed that classification marking issues exist, and many classification actions did not fully comply with 32 CFR (see appendixes C and D).[5] However, a more in-depth review is required to determine the extent and impact. The follow-on 2016 report will present an extensive review of actions and a determination of the magnitude of misclassifications.

(U//~~FOUO~~) Finding 1. NGA's Security Education and Training Program does not effectively train all personnel authorized to handle classified information in accordance with established requirements

(U//~~FOUO~~) NGA's security education and training program provides mandatory initial and refresher training for all personnel with derivative classification authority (DCA). The initial training does not, however, cover all of the required topic areas, and the annual refresher training does not meet the requirements for DCA training. Mandatory declassification authority training is not conducted, and classification management personnel do not receive specialized training as required when they assume their duties.

(U) Criteria

- EO 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Part 2 outlines the use of derivative classifications and mandates that persons who apply derivative classification

[4] (U) A derivative classification authority is an individual who reproduces, extracts, or summarizes classified information or who applies classification markings derived from source material or as directed by a classification guide.

[5] (U//~~FOUO~~) OCA sample = 27 actions; DCA sample = 54 actions.

markings receive training in the proper application of the derivative classification principles with an emphasis on avoiding over-classification.

- 32 CFR § 2001.70 sets standards for agency security education and training programs. The frequency of the training varies with the needs of the agency's security classification program, subject to the following requirements:

  (a) Initial training shall be provided to every person who has met the standards for access to classified information in accordance with applicable guidelines;

  (b) Original Classification Authorities shall receive training in proper classification and declassification prior to originally classifying information and at least annually thereafter;

  (c) Persons who apply derivative classification markings shall receive training in the proper application of the derivative principles of the executive order prior to derivatively classifying information and at least every two years;

  (d) Each agency shall provide some form of refresher security education and training at least annually for all personnel who handle or generate classified information.

- DoDM 5200.1, vol. 3, encl. 5, establishes security education and training requirements for DoD components for initial orientation, special training, OCA training and annual refresher training. It provides detailed training requirements on security policies and principles and derivative classification practices. It also dictates the minimum training requirements for declassification authorities to be completed at least once every two years and specifies additional training for individuals who are significantly involved in managing and overseeing classified information.

(U//~~FOUO~~) The Initial Security Classification Training of New Employees Does Not Incorporate All of the Required Topic Areas

(U//~~FOUO~~) The initial security training in the New Employee Orientation Seminar is neither tailored to the needs of the agency nor sufficiently addresses the basics of classification processes and requirements. The training lacks several requirements listed in the DODM 5200.1, such as an explanation of a security classification guide and how to use and obtain it, how to downgrade or declassify information, how to challenge classification decisions, and an explanation of derivative classification. Furthermore, although the training lists derivative classification authority once as a type of classifier, it falls short in clearly delineating who DCAs are, their associated responsibilities, and the principles of derivative classification. The stated objective of the training is to provide a basic understanding of procedures and methods involved with the proper handling and safeguarding of classified information.

(U//~~FOUO~~) In addition, the time allotted for the training block was reduced from 70 to 55 minutes. The security personnel we interviewed told us the time frame for the initial security training is not sufficient to meet the training needs of new employees so that they would effectively comprehend and retain the large quantity and types of data presented. Several individuals stated that the time frame is too short; there is not enough basic classification training; the minimum NGA requirement is not enough for employees; and NGA does not mentor new employees well in classification, especially analysts.

(U//~~FOUO~~) Because the initial security training does not meet the needs of the agency and most analysts work with a complex set of rules and require a great deal more classification training than that offered, the [redacted] developed its own classification training program to better prepare its employees to make classification decisions, mark, and handle classified information. The supplemental training provides a comprehensive review of classification, sourcing, declassification and markings. This training is intended to enhance, not replace, current initial security training. [redacted] is aware of the effort, but has not formally approved [redacted] specialized analytical security training.

(U//~~FOUO~~) NGA's Annual Security Computer-Based Training Does Not Meet the Requirement for DCA Training

(U//~~FOUO~~) NGA's Annual Security Refresher Training, administered via computer based-training (CBT), is the mechanism the [redacted] uses to satisfy the biennial DCA training requirement. While this CBT meets the minimum requirement for annual refresher security education and training, it does not adequately satisfy the requirement for DCA training. The current training lacks several requirements listed in 32 CFR. These include training for derivative classifiers that covers duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

(U//~~FOUO~~) All NGA employees are required to complete the security refresher training annually, and the NGA [redacted] tracks compliance through the [redacted] PeopleSoft system. The security CBT does not mention or clarify that the training fulfills the biennial derivative classification training requirement. In fact, numerous personnel interviewed did not realize the annual CBT served as their required derivative classifier training and initially thought they had not received refresher DCA training. In the CBT, the first information specifically relating to classification processes does not appear until midway through the training. The CBT does not include any standards, methods, or procedures for declassifying information. Although a security classification guide is mentioned twice, the training does not provide any details on where to find the guides or how to properly mark classified national security information. The information simply refers the employee to the Security Study Hall, which is not mandatory training. In addition, the CBT title, stated objectives, and summary do not provide definitive statements about classification management, such as classification markings, derivative classification, or declassification.

(U//~~FOUO~~) Multiple personnel we interviewed stated that the current derivative classification training is ineffective or inadequate because it covers too many security-related topics, and the classification management information is buried among other security training requirements. Many view the training as general security training. Interviewees also opined that the training is not sufficient for an agency that produces classified information on a daily basis. Several individuals stated that CBT is not the right tool for this type of training. One interviewee also stated that NGA has taken several shortcuts pertaining to classification training, education, and awareness and these are reflected in the inability of its work force to properly classify and mark documents. Other supplemental security training, such as the Security 101 and the Security Study Hall, are available but not mandatory.

(U//~~FOUO~~) NGA Does Not Adhere to the Minimum Requirements for Declassification Authority Training

((U//~~FOUO~~) NGA does not have any formal or standardized training for declassification authorities or reviewers. Required training for declassification authorities should include the standards, methods, and procedures for declassifying information; the standards for creating, maintaining, and using security classification guides; the information contained in NGA's declassification plan; NGA's responsibility for creating and maintaining a declassification database; and the referral process and requirements. Minimum training requirements for declassification authorities must be completed at least once every two years. Criteria documents do not specify minimum training requirements for declassification reviewers.

(U//~~FOUO~~) According to several personnel interviewed, declassification authorities become proficient in their jobs through on-the-job training and the knowledge gained through previous experience. As mentioned, the annual security refresher CBT required for all employees does not meet the minimum training requirements for declassification authorities.

(U//~~FOUO~~) In addition, we observed that declassification responsibilities among NGA personnel charged with oversight and management of the program are not clearly defined and understood. Some of the responsibilities are unclear, and several personnel we interviewed did not know who had responsibility for specific actions. For example, we were unable to determine the person responsible for oversight and approval of declassification recommendations made by designated declassification reviewers. We were given several names and spoke with those individuals. We found confusion and lack of awareness of who is responsible for this function. Due to time constraints, we were unable to determine or verify the declassification reviewer's evaluation and submission process.

(U//~~FOUO~~) NGA Classification Management Personnel Do Not Receive Specialized Security and Education Training Upon Assumption of Duties

(U//~~FOUO~~) Title 32 CFR § 2001.71 directs that personnel who have significant duties in creating or handling classified information receive more detailed or additional training no later than six months after assumption of duties. These positions include classification management officers, security managers, security specialists, and declassification authorities. NGA does not have a method to implement and manage the specialized security education and training required for individuals with significant duties in handling and overseeing classified information. We found no specific training identified or established to meet this requirement. According to classification management personnel, current training, when taken, is ad hoc and not standardized. Mandated training requirements for declassification authorities are nonexistent and not effectively communicated. The [redacted] indicated that classification security managers need about two years to get trained and "up to speed" in the position.

(U//~~FOUO~~) Inadequate and ineffective training has the potential to result in over-classification of information and could lead to persistent misclassification of data. Employees may not fully understand the requirements or their responsibilities in marking and handling classified data. Most personnel we interviewed stated that current training is inadequate and leads to misclassification of NGA documents, especially in e-mails. In addition, an OIG review of classified actions revealed consistent errors in areas such as classification authority, identity of derivative classifiers, and portion markings.

(U) Recommendations

(U) For the [redacted]

(U//~~FOUO~~) Recommendation 1. Restructure initial security training, including all required training areas.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] in collaboration with [redacted] began a security training restructure initiative in early 2013, specifically requesting the additional time needed to address all required areas. [redacted] will provide a plan addressing actions already taken and the way forward within 60 days following the release of the final OIG report. This plan will be responsive to recommendations 1, 2, 3, 4, and 5.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Recommendation 2. In coordination with the [redacted] conduct a resource assessment of the initial security training to determine the length of time needed to sufficiently instruct new employees on required security policies, principles, and practices. Consider creating a separate block of instruction focusing specifically on classification management-related requirements.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] in coordination with [redacted] will conduct a resource assessment of the initial security training to determine the length of time needed to sufficiently instruct new employees on security policies, principles, and practices and additional personnel needed to implement the training. This assessment will also address the inclusion of a separate block of instruction focused on classification management-related requirements.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Recommendation 3. Establish training for derivative classification authority separate from the annual security refresher training. Include clear objectives and instruction on the principles of derivative classification and incorporate all mandatory minimum topic areas.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] will coordinate with [redacted] to develop biennial mandatory training for DCAs that is separate from the annual security refresher training. DCA training will include clear objectives, step-by-step instructions on the principles of derivative classification, and all mandatory minimum topics.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Recommendation 4. Incorporate and track the biennial training requirement on derivative classification authority as a separate entry in the PeopleSoft tracking system.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] will incorporate and track the biennial training as a separate entry in the PeopleSoft tracking system.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Recommendation 5. Develop and implement a security education and training program incorporating all requirements for individuals who have significant duties in managing and overseeing classified information.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] will develop and implement specialized training for individuals with significant duties in managing and overseeing classified information. This specialized training will address the role and responsibilities of classification managers, declassification specialists, original classification authorities (OCAs), remotely assigned personnel, analysts, international desk officers, and other personnel identified.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Finding 2. NGA's original classification authority program lacks rigor

(U//~~FOUO~~) The original classification authority training program does not prepare all OCAs to execute their authorities. According to one OCA, the training does not instruct them on how to determine an original classification decision and only briefly explains the information provided in the OCA handbook. Although OCA training is required annually, not all OCAs have met this requirement. In addition, NGA does not have a process to hold personnel accountable and suspend classification authorities for noncompliance with mandatory training.

(U) Criteria

- EO 13526, part 1, defines the original classification principles through several sections including:
    - Classification Standards
    - Classification Levels
    - Classification Authority
    - Classification Categories
    - Duration of Classification
    - Identification and Markings
    - Classification Prohibitions and Limitations
    - Classification Challenges
    - Fundamental Classification Guidance Review
- 32 CFR § 2001.1 provides requirements for agencies with original classification authority, including training, establishment of classification guides, duration of classification, and limitations.
- EO 13526, 32 CFR § 2001.71, and DoDM 5200.1, vol. 3 state that OCAs who do not receive OCA mandatory training at least once a calendar year shall have their classification authority suspended until such training has occurred.

(U//~~FOUO~~) NGA's Security and Education Training Program Does Not Fully Meet the Needs of All OCAs

(U//~~FOUO~~) The ability to originally classify information is the cornerstone of the classification management system. The ability to classify Top Secret information is passed down by the President, through the Undersecretary of Defense for Intelligence to the Director, NGA. Prior to 29 July 2013, the Director, NGA, with approval, further delegated OCA at the Secret level to four NGA Key Component (KC) directors. Those directors were: [redacted]. Effective 29 July 2013, NGA was granted additional OCA designations at the Top Secret level. This inspection focused solely on the OCAs in place and involved in the process prior to 29 July 2013.

(U//~~FOUO~~) NGA's [redacted] has established an OCA training program consisting of a handbook and an in-person, 30-minute PowerPoint briefing. The handbook provides information on delegation authorities, national security information, marking, the classification decision process, explanations of what is and is not classified, and an explanation of information security. OCA training is required at least once every calendar year.

(U//~~FOUO~~) On the surface, the established OCA training program appears to be adequate and meets the directed requirements, but interviews and a review of available documentation and process reveal otherwise. At least one OCA stated that the training does not satisfy OCAs' needs or adequately prepare them to execute their original classification authorities. They told us that they rarely perform these functions; therefore, when a decision is needed, they have to relearn the information and process. Also, the 30-minute training does not teach OCAs how to make an original classification decision. The training briefly explains the information, but does not provide original classifiers a thorough step-by-step process. Another OCA was not aware of their designation as an OCA until contacted by the OIG for an interview in support of this inspection. Some OCAs require assistance and rely heavily on their subordinates to work through the OCA decision process. In addition, none of the OCAs interviewed were aware of the existence of a classification challenge process or what role the OCA would play in such a scenario.[6] Upon further review of [redacted] training material, we found no mention of a classification challenge process. These issues further expose the inadequacies of the OCA training program.

(U//~~FOUO~~) All OCAs Have Not Met the Annual Training Requirement and They Are Not Held Accountable for Noncompliance

(U//~~FOUO~~) All OCAs designated prior to 29 July 2013 are not in compliance with the annual training requirement. According to EO 13526, OCAs are required to receive original classification training every year and certify that fact in writing. [redacted] claims to abide by this rule; however, we were unable to verify this assertion. On several occasions, we requested documentation confirming compliance with the annual training requirement. [redacted] provided current certification forms for two of the five OCAs. The others did not exist or fell outside of the one-year required time frame. In addition, the [redacted] has operated without a trained OCA for five months. [redacted] informed us that the decision was made not to train the then acting [redacted] even though he

[6] (U) A classification challenge process establishes procedures under which authorized holders of information are encouraged and expected to challenge the classification of information they believe is improperly classified or unclassified.

served in the position for three months. We noted that this decision contrasted with DoD guidance and OCA training materials, which state that deputies of an OCA are empowered to exercise OCA authority when they officially assume the OCA position in an acting capacity. They, too, must certify, in writing, receipt of OCA training. As of 14 August 2013, [redacted] had not contacted the new [redacted] regarding his OCA responsibilities or the required training.

(U//~~FOUO~~) Mandatory training for all NGA employees is listed and tracked within the PeopleSoft system. The annual OCA training requirement is not listed in PeopleSoft and therefore not easily tracked. Classification management personnel were unable to provide updated training records or verification for all OCAs.

(U//~~FOUO~~) NGA does not have a process to hold personnel accountable or to suspend classification authorities for noncompliance with mandatory training in accordance with EO 13526 and 32 CFR. There are also no checks and balances for holding OCAs accountable and suspending access to classified information when appropriate. According to several individuals interviewed, multiple attempts to implement accountability procedures have failed. Personnel involved with management of the program would like to see more stringent penalties for noncompliance with mandatory training.

(U//~~FOUO~~) Based on our analysis of NGA's OCA program, training shortfalls could be attributed to noncompliance with mandated training requirements, the short time frame allotted for OCA training, the infrequency of OCAs' classification decisions, the absence of accountability mechanisms for noncompliance, and the lack of an established relationship between the OCAs themselves and [redacted] All OCAs we interviewed indicated they do not interact or work directly with [redacted] personnel regarding original or derivative classification actions. This is a potential issue since all classification challenges and the review and signature of security classification guides are supposed to be coordinated between the [redacted] and the OCAs.

(U) Recommendations

(U) For the [redacted]

(U//~~FOUO~~) Recommendation 6. Review the current OCA training plan and develop a more comprehensive briefing outlining the step-by-step duties and responsibilities of OCAs. Expand the 30-minute OCA training window to allow for more detailed training and discussions.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] has expanded the existing 30 minute training to include ample time for OCA questions. The existing OCA briefing, NGA OCA Manual, and handouts are currently under review for content. Step-by-step duties and responsibilities of OCAs will be included in the briefing and reiterated in the accompanying training documents. In 2013, NGA was authorized 10 Top Secret OCAs by the Deputy Secretary of Defense. [redacted] is currently providing robust initial training to the new Top Secret OCAs, including all recommendations provided in this report. [redacted] will provide a plan addressing actions already taken and the way forward within 90 days following the release of the final OIG report. This plan will be responsive to recommendations 6, 7, and 8.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Recommendation 7. Establish a verifiable mechanism to monitor and track OCA annual training through PeopleSoft.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] will immediately begin action to complete this recommendation and will provide a plan with actual deliverable dates within 90 days following the release of the final OIG report.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Recommendation 8. Develop and implement a process to hold personnel accountable for noncompliance with mandated training requirements and suspend classification authorities, when appropriate.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] will develop and implement a process to hold OCAs accountable for noncompliance with mandatory training requirements and suspend classification authorities, when appropriate. Details of the process will be included in the NGA Security Classification Guide, NGA OCA Manual, and made available during the OCA training.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Finding 3. NGA does not have a formal process for challenging original classification decisions

(U//~~FOUO~~) NGA does not have a classification challenge process that meets specified Federal guidelines. The current procedure lacks basic requirements and accountability. Most personnel interviewed, including the OCAs, were unaware of NGA's process for challenging classification decisions or the requirement to have a process.

(U) Criteria

- EO 13526, part 1, states that an agency head or senior agency official shall establish procedures to challenge improper classification.

- 32 CFR § 2001.14 states that agencies shall establish a system for processing, tracking, and recording formal classification challenges made by the authorized holders. Agencies shall consider challenges separately from Freedom of Information Act requests and shall not process such challenges in turn with pending access requests. It also states that a formal challenge must be in writing but need not be any more specific than to question why information is or is not classified; and the agency shall provide an initial written response to a challenge within 60 days.

- DoDM 5200.01, vol. 1, encl. 4, states the need for an established Classification Challenge process.

(U) Title 32 CFR sets the standard for agency classification challenge procedures and outlines the basic set of requirements for this process. The basic requirements include the following: the challenge process must be in writing; the agency must track and record all formal challenges; and the agency shall provide a written response to a challenge within 60 days. The challenge can be made by any authorized holder and shall be presented to an OCA with jurisdiction over the information.[7]

(U//~~FOUO~~) NGA's classification challenge process lacks the basic requirements outlined in 32 CFR. Most of the personnel interviewed, including all OCAs, were not aware of the existence of a classification challenge process. NGA's solution to this requirement is to include a Change Request Form in all security classification guides. The intent is for the individual challenging the OCA decision to annotate the challenge and rationale on the form and forward it to the [redacted] A review of NGA's 29 completed security classification guides, however, revealed only eight of the 25 guides classified above U//FOUO contain the form. We were unable to determine if [redacted] tracks and records all formal challenges or provides written responses within 60 days of a challenge. Our own written request for procedures regarding classification challenges yielded no results. In addition, of the two classification challenges mentioned during the interview process, we were unable to determine if the applicable OCA was involved or if NGA responded to these challenges in writing within the 60-day timeline.

(U//~~FOUO~~) Because NGA has not established a standardized formal classification challenge process, the agency is not in compliance with mandated regulations. Not having an established and publicized process could cause confusion among NGA employees and NSG partners. Many employees are unaware of the requirement or unsure of the procedures to launch a challenge. In addition, without an established records file and retention process, management may not be able to produce records of classification challenges to show compliance.

(U) Recommendations

(U) For [redacted]

[7] (U) An authorized holder is any individual who has been granted access to specific classified information in accordance with the provisions of EO 13526.

(U//~~FOUO~~) Recommendation 9. Establish a classification challenge system for processing, tracking, and recording formal classification challenges. Promulgate the procedures to all OCAs and include in their required annual training.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] will establish a formal classification challenge system for processing, tracking and recording formal classification challenges. The system will be consistent with direction provided in EO 13526 and 32 CFR. Details of the classification challenge system will be explained in the NGA SCG and annexes, NGA OCA Manual and DCA briefings. [redacted] will provide OIG with a plan within 90 days following the release of the final OIG report. This plan will be responsive to recommendations 9, 10, and 11.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Recommendation 10. Insert a Change Request Form in all security classification guides. Include a brief instruction on how to challenge a classification decision.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] will include a Change Request Form in all SCGs that provide instructions on how to challenge a classification decision.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Recommendation 11. Incorporate the classification challenge process into the initial security classification and derivative classification training curricula.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] will incorporate the classification challenges process into all initial, annual, and biennial security training for OCAs and DCAs.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Finding 4. NGA-produced security classification guides do not incorporate all of the required classification guidelines

(U//~~FOUO~~) The *NGA Security Classification Guide*, which implements PL 111-258, does not include specific guidance on detailed requirements as delineated in Federal regulations. Other NGA security classification guides have similar issues and are inconsistent with required guidelines.

(U) Criteria

- EO 13526, part 2, provides general requirements and standards concerning the issuance of security classification guides. It states that each classification guide shall be approved personally and in writing by an official who:

  - Has program or supervisory responsibility over the information or is the senior agency official.

  - Is authorized to classify information originally at the highest level of classification prescribed in the guide.

  The executive order also states that agencies shall establish procedures to ensure security guides are reviewed, updated and incorporate original classification decisions on a timely basis.

- 32 CFR §§ 2001.15, 2001.21, and 2001.25 state the security classification guides at a minimum need to identify the OCA by name and position or personnel identifier. Also, the security classification guide must contain declassification instructions.

- DoDM 5200.01, vol. 3, encl. 5, stipulates that required training contain explanations on authorized types of sources that could be used for derivative classifications. Topics should cover security classification guide specifics, including purpose, components, and approval and signature by the cognizant OCA.

- DoD 5200.1-H provides direction for writing security classification guidance, discusses classification and declassification principles, gives administrative requirements for security classification guides, and offers a recommended format.

(U//~~FOUO~~) The *NGA Security Classification Guide*, as the Implementing Directive, Does Not Incorporate All Classification Mandates

(U//~~FOUO~~) The *NGA Security Classification Guide* is NGA's primary guidance for classification management. The guide implements EO 13526, which became effective on 29 December 2009. The guide's date reflects its most recent administrative update as of 25 March 2008. Although the guide predates the executive order, it references EO 13526 several times. NGA does not have a separate implementing instruction or directive specifically addressing classified national security information and the implementation of PL 111-258. The classification management personnel we interviewed stated they did not need a separate document.

(U//~~FOUO~~) A thorough review of the *NGA Security Classification Guide* revealed that specific guidance on the detailed requirements in EO 13526 and 32 CFR is absent and has not been incorporated. The guide references the executive order, lists the NGA OCAs, states that all other NGA employees are derivative classifiers, and provides a few definitions. It does not, however, provide detailed instruction about or the processes for executing classification authority decisions, markings, fundamental classification guidance review, declassification, self-inspection, training, and other responsibilities stipulated in 32 CFR and the DoD Handbook. [redacted] is in the process of updating the *NGA Security Classification Guide*. However, the current draft is similar to the existing document and does not go far enough in addressing national and DoD classification guidance and training requirements.

(U//~~FOUO~~) NGA Security Classification Guides Are Not Consistent with Specific Guidelines

(U//~~FOUO~~) The OCAs issue security classification guides and identify the elements of information for a specific subject that must be classified. These guides provide direction for determining security levels, control systems, and duration of classifications. They are used by OCAs as a tool to communicate with the work force. NGA has approximately 60 security classification guides, of which at least half are in draft. Criteria references listed above provide guidance on writing the guides and specify required elements or contents, as well as associated training. In addition to the required OCA signature of approval, other required content for security classification guides includes identity of the subject matter, OCA's name and position or personal identifier, agency point of contact, date of issuance or last review, reason for classification, and specific date or event for declassification. The classification management personnel we interviewed confirmed that all of the security classification guides are required to have an OCA signature and informed us that all NGA guides include a statement on derivative classification and a form for classification challenges. Although EO 13526 does not require the derivative classifications section to be included in security classification guides, the classification management program officer stated every NGA guide contained a derivative section to assist users in properly making classification decisions. Title 32 CFR also levied requirements for an initial, fundamental classification review of all security classification guides. NGA reported completion of the initial review of all of its security classification guides in 2012.

(U//~~FOUO~~) A review of the 29 completed security classification guides revealed several inconsistencies with required guidelines. Specifically, 21 of 29 guides did not contain an OCA signature of approval. One guide was classified by an NGA nonsupervisory employee not designated as an OCA, contrary to EO 13526. Seventeen guides did not identify the OCA by name and position or personal identifier. One did not include declassification instructions, and another had an incomplete declassification date. Of the 25 security classification guides classified above U//FOUO , 22 did not include or mention derivative classification, and 17 did not contain the form for challenging a classification decision. Of note, the NGA guide used as the implementing directive for PL 111-258 did not include an approval signature; the current draft *NGA Security Classification Guide* does include an OCA signature block.

(U//~~FOUO~~) The NGA security classification guides contain many of the required content; however, numerous critical elements are missing from many of them. Omission of required data has the potential to result in over-classification of information and lead to persistent misclassification of data within NGA.

(U) Recommendation

(U) For the [redacted]

(U//~~FOUO~~) Recommendation 12. Review and update all security classification guides and implement a quality control mechanism to ensure every guide contains mandatory elements.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] will begin an immediate review of all published and in-draft SCGs to ensure every guide contains mandatory elements. In addition, [redacted] will implement a quality control mechanism to ensure the review and updates are being accomplished. A plan to address this recommendation will be provided within 90 days following the release of the final OIG report.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Finding 5. NGA does not have a fully established self-inspection program

(U//~~FOUO~~) NGA's self-inspection process is not fully established based on the ISOO criteria used in 2012 self-inspection annual report. We were unable to verify the findings NGA reported in 2012 to the ISOO and compliance with established security standards.

(U) Criteria

- EO 13526, part 5, establishes the need for agencies to report annually to the Director of Information Security Oversight Office (ISSO) on their self-inspections programs.

- 32 CFR § 2001.60 sets standards for establishing and maintaining an ongoing agency self-inspection program. These standards include, but are not limited to:
    - A regular review of representative samples of the agency's original and derivative classification actions encompassing all activities that generate classified information.
    - Documenting self-inspection findings internally and reporting the findings annually to the Director of ISOO.
    - Specifying in the report to ISSO the agency's classification decisions and programs in the areas of:

  - Original and derivative classification
  - Declassification program
  - Safeguarding
  - Security violations
  - Security education and training
  - Management oversight

- ISOO 2012 Memorandum, *Annual Senior Agency Official Self-Inspection Program Report*
  - Enclosure 1 details elements to include in the agency annual report.
  - Enclosure 2 provides details to include in the annual report for agencies that have not fully established their self-inspection program.

(U//~~FOUO~~) We were unable to validate the findings in the NGA 2012 self-inspection report. The ISOO provides annual guidance for agency use in assessing the effectiveness of their classified national security information program through a self-inspection. The guidance provides two reporting formats, listed above under ISOO memorandum as enclosures 1 and 2. NGA's 2012 self-inspection report signed by the [redacted] followed the ISSO reporting format in enclosure 2, for agencies that have not fully established a self-inspection program.

(U//~~FOUO~~) The [redacted] complied with the ISOO requirements by using a self-inspection questionnaire, presented in an online format, and supplemented by a review of electronic records and GEOINT products. The questionnaire used yes and no questions to determine employees' understanding of the mandated security elements. Because a yes/no format limits measurement of employees' overall understanding of a particular topic, we requested documentation to verify the number of participants who answered the questionnaire and the methodology used in analyzing the data. We did not receive any additional applicable documents. The information received during the data call consisted of one document with a percentage breakdown of responses to the security elements listed in the 2012 self-inspection report. For an explanation of the data, we made two inquiries to members of the classification management team involved with the self-inspection. However, neither person was able to explain the information. [redacted] also used an ISOO-provided self-inspection checklist to determine security information requirements. According to [redacted] personnel, the checklist contained outdated information, and numerous questions were not applicable to NGA. During interviews, [redacted] personnel stated they were updating the checklist to more accurately reflect the needs of NGA.

(U//~~FOUO~~) NGA reported in its self-inspection memorandum to the ISOO that in FY 2012 the agency made [redacted] original classification decisions and [redacted] derivative classification decisions. According to [redacted] provided documentation and information confirmed during the interviews, the number of derivative classification decisions was usually determined by gathering two weeks of derivative classification actions across the agency four times a year. A mathematical algorithm applied to the data produced an agency total. In FY 2012, however, [redacted] used only one two-week sample period. The two-week sum was then multiplied by 26 to obtain the yearly total reported in the final report. Upon further analysis of the information, we determined that eight of the 17 agency KCs—including [redacted] which had more than [redacted] personnel—reported zero derivative classification decisions during the sample period. This resulted in no contributions from those eight KCs to the total annual numbers reported. [redacted] failure to follow its own processes and to not question seemingly inaccurate data calls into question the validity of the procedures used and the numbers provided in the final report.

(U//~~FOUO~~) The NGA 2012 report also stated that personnel reviewed and assessed a five percent representative sample of the agency's original and derivative classification actions, activities, and program areas. We were unable to verify the accuracy of the representative sample reviewed and process used to obtain the information because inquiries to obtain documentation on the "representative" sample numbers, type, and other associated procedures showing the results of the review were not provided for our evaluation.

(U//~~FOUO~~) NGA does not have specific implementation guidance for self-inspections. The *NGA Security Classification Guide*, which serves as the implementing directive for PL 111-258 and EO 13526, does not address self-inspection procedures. We were unable to verify an established [redacted] process to question the accuracy of the data or validate the collective information gathered during the self-inspection review. We were also unable to verify compliance with established security standards. For example, we could not determine the sample size of personnel. We could not determine if a representative sample of classification actions and program areas was reviewed. We could not verify how [redacted] concluded, as reported, that a majority of the documents were properly classified and marked in accordance with Federal standards and directives. We could not determine how and by whom the stated best practices were identified, and we could not verify the accuracy of the number of original and derivative classification decisions provided in the annual self-inspection report. Finally, we were unable to assess the self-inspection process in totality. All of these factors limited our ability to determine the effectiveness of the program. Without using a representative sampling of classified actions throughout the entire year and questioning the validity of the data received, management may be unable to assess the effectiveness of NGA's classified national security information program.

(U) Recommendations

(U) For [redacted]

(U//~~FOUO~~) Recommendation 13. Fully establish and implement a self-inspection program in accordance with EO 13526, 32 CFR, and ISOO directives.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] continues efforts to establish, document and implement a self-inspection program in accordance with EO 13526, 32 CFR and ISOO directives. [redacted] will document the self-inspection program in a NGA Self-Inspection Program Manual. [redacted] will provide a plan within 90 days following the release of the final OIG report. This plan will be responsive to recommendations 13 and 14.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U//~~FOUO~~) Recommendation 14. Establish procedures to document the annual self-inspection process, including a methodology for analyzing, measuring and validating data.

(U//~~FOUO~~) Management Comments. [redacted] concurred with the recommendation. [redacted] continues ongoing efforts to document the annual self-inspection process, including methodology for analyzing, measuring and validating data. The methodology will be coordinated with USD(I) and ISOO to ensure consistency with standards provided by them.

(U//~~FOUO~~) OIG Response. Management's comments were responsive to the intent of the recommendation.

(U) Appendix A. List of Recommendations, Status, and Benefits

Recommendation	Management Response	Status	Description of Benefits
(U) For the [redacted]			
(U//~~FOUO~~) Restructure initial security training, including all required training areas.	[redacted] concurred with the recommendation. [redacted] in collaboration with [redacted] began a security training restructure initiative in early 2013, specifically requesting the additional time needed to address all required areas. [redacted] will provide a plan addressing actions already taken and the way forward within 60 days following the release of the final OIG report. This plan will be responsive to recommendations 1, 2, 3, 4, and 5.	Open	Nonmonetary. Improve program results. Ensures NGA is compliant with Federal directives, rules and regulations.
(U//~~FOUO~~) In coordination with the [redacted] conduct a resource assessment of the initial security training to determine the length of time needed to sufficiently instruct new employees on required security policies, principles, and practices. Consider creating a separate block of instruction focusing specifically on classification management-related requirements.	[redacted] concurred with the recommendation. [redacted] in coordination with [redacted], will conduct a resource assessment of the initial security training to determine the length of time needed to sufficiently instruct new employees on security policies, principles, and practices and additional personnel needed to implement the training. This assessment will also address the inclusion of a separate block of instruction focused on classification management-related requirements.	Open	Nonmonetary. Improve program results. Improves retention of classification training information among the workforce.

Recommendation	Management Response	Status	Description of Benefits
(U//~~FOUO~~) Establish training for derivative classification authority separate from the annual security refresher training. Include clear objectives and instruction on the principles of derivative classification and incorporate all mandatory minimum topic areas.	[redacted] concurred with the recommendation. [redacted] will coordinate with [redacted] to develop biennial mandatory training for DCAs that is separate from the annual security refresher training. DCA training will include clear objectives, step-by-step instructions on the principles of derivative classification, and all mandatory minimum topics.	Open	Nonmonetary. Improve program results. Ensures NGA is compliant with Federal directives, rules and regulations.
(U//~~FOUO~~) Incorporate and track the biennial training requirement on derivative classification authority as a separate entry in the PeopleSoft tracking system.	[redacted] concurred with the recommendation. [redacted] will incorporate and track the biennial training as a separate entry in the PeopleSoft tracking system.	Open	Nonmonetary. Improve program results. Utilizes existing infrastructure to ensure employee compliance with mandated training.
(U//~~FOUO~~) Develop and implement a security education and training program incorporating all requirements for individuals who have significant duties in managing and overseeing classified information.	[redacted] concurred with the recommendation. [redacted] will develop and implement specialized training for individuals with significant duties in managing and overseeing classified information. This specialized training will address the role and responsibilities of classification managers, declassification specialists, original classification authorities (OCAs), remotely assigned personnel, analysts, international desk officers, and other personnel identified.	Open	Nonmonetary. Improve program results. Improves the agency's current process and ensures compliance with mandated directives.

Recommendation	Management Response	Status	Description of Benefits
(U//~~FOUO~~) Review the current OCA training plan and develop a more comprehensive briefing outlining the step-by-step duties and responsibilities of OCAs. Expand the 30-minute OCA training window to allow for more detailed training and discussions.	[redacted] concurred with the recommendation. [redacted] has expanded the existing 30 minute training to include ample time for OCA questions. The existing OCA briefing, NGA OCA Manual, and handouts are currently under review for content. Step-by-step duties and responsibilities of OCAs will be included in the briefing and reiterated in the accompanying training documents. In 2013, NGA was authorized 10 Top Secret OCAs by the Deputy Secretary of Defense. [redacted] is currently providing robust initial training to the new Top Secret OCAs, including all recommendations provided in this report. [redacted] will provide a plan addressing actions already taken and the way forward within 90 days following the release of the final OIG report. This plan will be responsive to recommendations 6, 7, and 8.	Open	Nonmonetary. Improve program results. Improves training retention and process efficiency of original classification authority.
(U//~~FOUO~~) Establish a verifiable mechanism to monitor and track OCA annual training through PeopleSoft.	[redacted] concurred with the recommendation. [redacted] will immediately begin action to complete this recommendation and will provide a plan with actual deliverable dates within 90 days following the release of the final OIG report.	Open	Nonmonetary. Improve program results. Utilizes existing infrastructure to ensure OCA's compliance with annual mandatory training.

Recommendation	Management Response	Status	Description of Benefits
(U//~~FOUO~~) Develop and implement a process to hold personnel accountable for noncompliance with mandated training requirements and suspend classification authorities, when appropriate.	[redacted] concurred with the recommendation. [redacted] will develop and implement a process to hold OCAs accountable for noncompliance with mandatory training requirements and suspend classification authorities, when appropriate. Details of the process will be included in the NGA Security Classification Guide, NGA OCA Manual, and made available during the OCA training.	Open	Nonmonetary. Improve program results. Ensures compliance with mandated directives.
(U//~~FOUO~~) Establish a classification challenge system for processing, tracking, and recording formal classification challenges. Promulgate the procedures to all OCAs and include in their required annual training.	[redacted] concurred with the recommendation. [redacted] will establish a formal classification challenge system for processing, tracking and recording formal classification challenges. The system will be consistent with direction provided in EO 13526 and 32 CFR. Details of the classification challenge system will be explained in the NGA SCG and annexes, NGA OCA Manual and DCA briefings. SI will provide OIG with a plan within 90 days following the release of the final OIG report. This plan will be responsive to recommendations 9, 10, and 11.	Open	Nonmonetary. Improve program results. Improves security classification process and ensures compliance with mandated directives.
(U//~~FOUO~~) Insert a Change Request Form in all security classification guides. Include a brief instruction on how to challenge a classification decision.	[redacted] concurred with the recommendation. [redacted] will include a Change Request Form in all SCGs that provide instructions on how to challenge a classification decision.	Open	Nonmonetary. Improve program results. Improves security classification process and ensures compliance with mandated directives.

Recommendation	Management Response	Status	Description of Benefits
(U//~~FOUO~~) Incorporate the classification challenge process into the initial security classification and derivative classification training curricula.	[redacted] concurred with the recommendation. [redacted] will incorporate the classification challenges process into all initial, annual, and biennial security training for OCAs and DCAs.	Open	Nonmonetary. Improve program results. Improves retention of classification training information among the workforce. Ensures compliance with mandated directives.
(U//~~FOUO~~) Review and update all security classification guides and implement a quality control mechanism to ensure every guide contains mandatory elements.	[redacted] concurred with the recommendation. [redacted] will begin an immediate review of all published and in-draft SCGs to ensure every guide contains mandatory elements. In addition, [redacted] will implement a quality control mechanism to ensure the review and updates are being accomplished. A plan to address this recommendation will be provided within 90 days following the release of the final OIG report.	Open	Nonmonetary. Improve program results. Improves the agency's current process and ensures compliance with mandated directives.
(U//~~FOUO~~) Fully establish and implement a self-inspection program in accordance with EO 13526, 32 CFR, and ISOO directives.	[redacted] concurred with the recommendation. [redacted] continues efforts to establish, document and implement a self-inspection program in accordance with EO 13526, 32 CFR and ISOO directives. [redacted] will document the self-inspection program in a NGA Self-Inspection Program Manual. [redacted] will provide a plan within 90 days following the release of the final OIG report. This plan will be responsive to recommendations 13 and 14.	Open	Nonmonetary. Improve program results. Ensures NGA is compliant with Federal directives, rules and regulations.

Recommendation	Management Response	Status	Description of Benefits
(U//~~FOUO~~) Establish procedures to document the annual self-inspection process, including a methodology for analyzing, measuring and validating data.	[redacted] concurred with the recommendation. [redacted] continues ongoing efforts to document the annual self-inspection process, including methodology for analyzing, measuring and validating data. The methodology will be coordinated with USD(I) and ISOO to ensure consistency with standards provided by them.	Open	Nonmonetary. Improve program results. Improves efficiency of current process and ensures compliance with mandated directives.

(U) Appendix B. Scope and Methodology

(U) SCOPE

(U//~~FOUO~~) The scope of this project was determined by a Congressionally Directed Action as mandated in Public Law 111-258, Reducing Over-Classification Act. The inspection team reviewed NGA classification management policies and practices and assessed whether the agency is in compliance with EO 13526 and 32 CFR § 2001. The team also evaluated classification, marking, and declassification of classified national security information. This inspection focused on over-classification, not under-classification.

(U//~~FOUO~~) The organizational scope included the [redacted] designated Original Classification Authorities, derivative classifiers, security classification guides, subject matter experts, and information security specialist and managers.

(U) METHODOLOGY

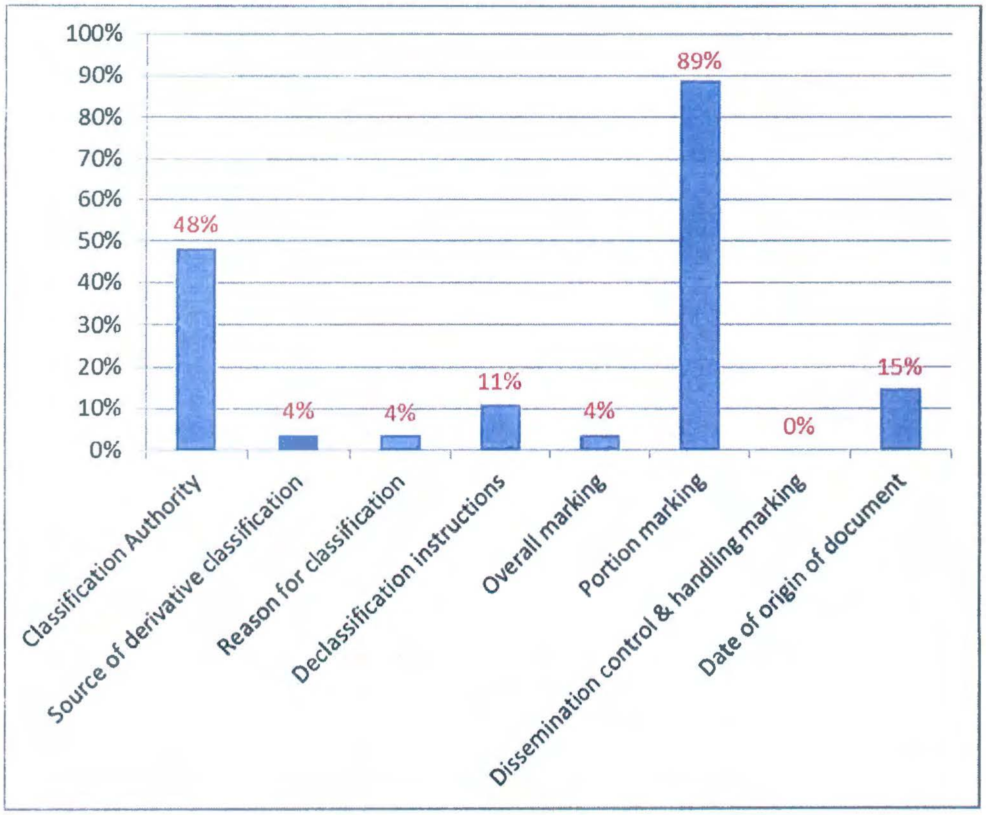
(U//~~FOUO~~) The inspection team reviewed relevant documents establishing criteria (executive orders, regulations, directives, manuals), policies, procedures, and previous OIG reports related to the classification of information. We also reviewed relevant briefings, training materials, and reports. We conducted structured interviews with the program manager and other personnel involved with the administration, execution, and oversight of NGA's classification management program.

(U//~~FOUO~~) We reviewed a small sampling of original and derivatively classified actions (documents) to determine compliance with established requirements and policies. The sample included two types of every operational product line produced by the [redacted] and presentations, reports, and Web content from other KCs. While the review of actions revealed that classification marking issues, the follow-on report will determine the extent of the problem and identify trends that may contribute to persistent misclassification of information. Last, we assessed the program to determine if persistent misclassification of information occurred.

(U//~~FOUO~~) We coordinated our assessment with other IGs and followed a consistent methodology to allow for cross-agency comparison of observations and conclusions.

(U) This inspection was conducted in accordance with the *Quality Standards for Inspections and Evaluations* of the Council of the Inspectors General for Integrity and Efficiency, January 2012.

(U) Appendix C. Errors in a Sample of NGA OCAs' Marking of Required Categories

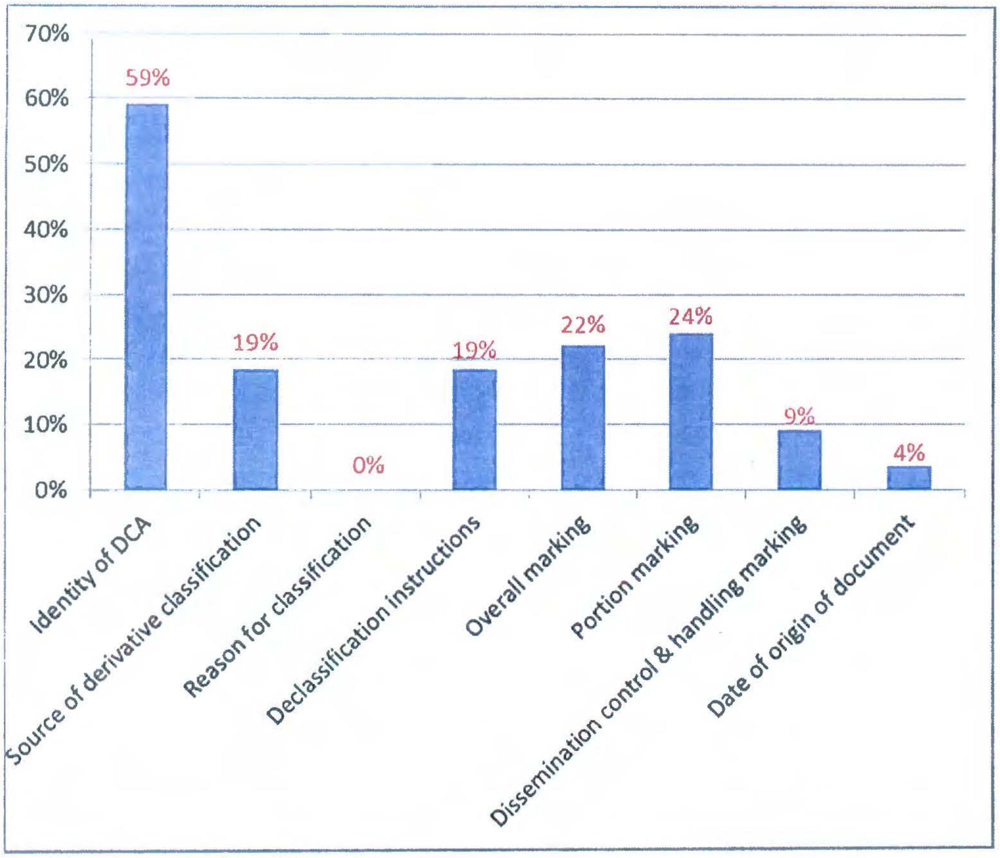


(Figure is Unclassified)

Note. This figure represents a sample of NGA OCA decisions. The review included all completed NGA security classification guides. The figure depicts the percentage of errors found in each classification category required by 32 CFR § 2001.21. The review revealed the following:

- Numerous inconsistencies in marking the original classification authority and portion marking.
- Errors in the Classified By line pertained mostly to the absence of the OCA's name and position.
- Most of the portion markings complied with the objectives of portion markings but did not fully comply with the details and intent of 32 CFR.

(U) Appendix D. Errors in a Sample of NGA DCAs' Marking of Required Categories



(Figure is Unclassified)

Note. The figure represents a small sampling of NGA DCA decisions. The review included operational products, presentations, reports and Web content. The figure depicts the percentage of error found in each classification marking category required by 32 CFR § 2001.22. The review revealed the following:

- Inconsistencies in several categories dependent on the type of classification action.
- Derivative classifier was not identified in a majority of products reviewed.
- Web design and setup contributed to errors in the source of derivative classification, declassification instructions, and overall markings categories.
- Most portion markings complied with the objectives of portion markings, but did not fully comply with the details and intent of 32 CFR.

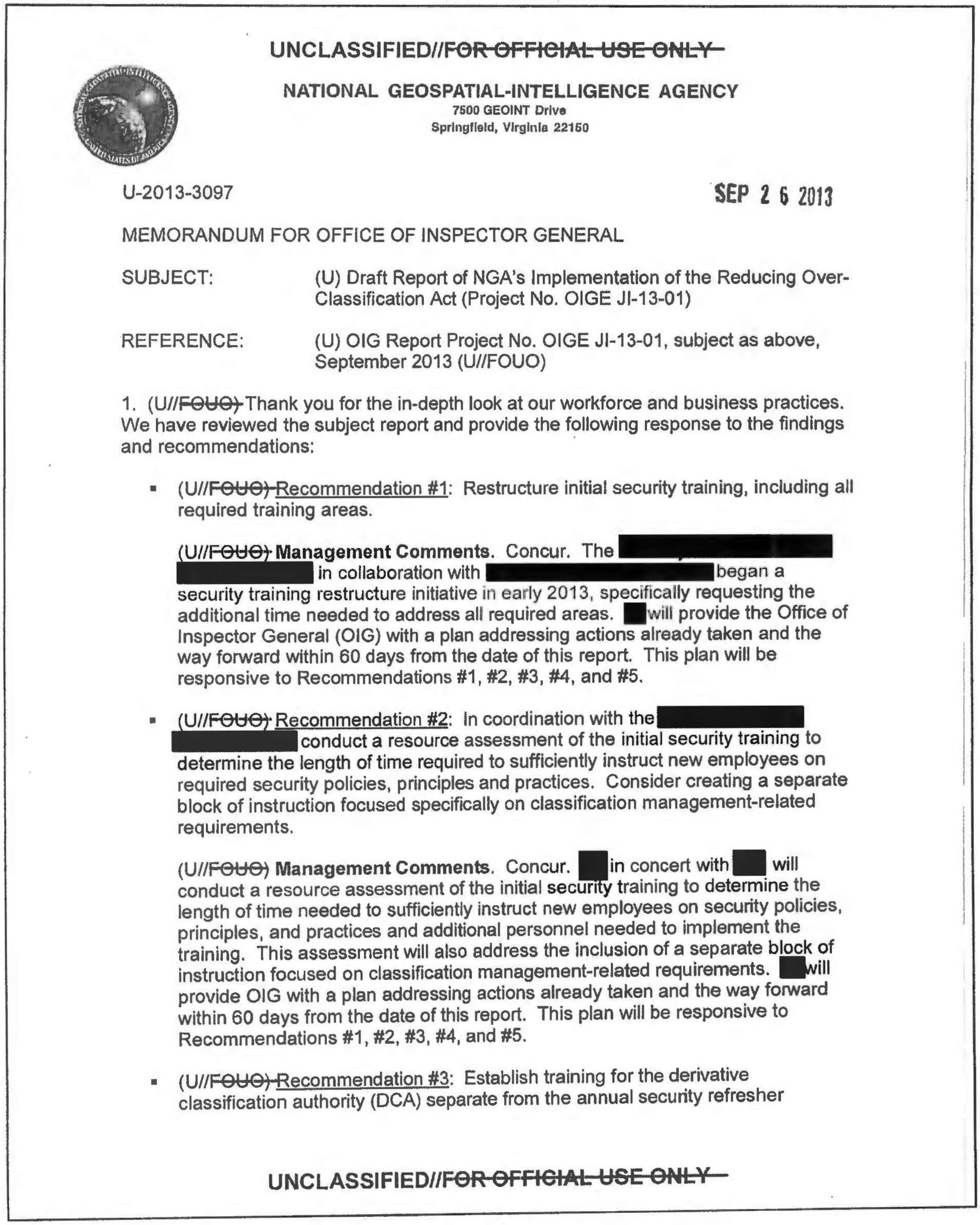
(U) Appendix E. Abbreviations

(U) CBT	computer-based training
(U) CFR	Code of Federal Regulations
(U) DoDM	DoD Manual
(U) DCA	Derivative Classification Authority
(U) EO	Executive Order
(U) FOUO	For Official Use Only
(U) GEOINT	Geospatial Intelligence
(U) IC	Intelligence Community
(U) IC IG	Intelligence Community Inspector General
(U) IG	Inspector General
(U) ISOO	Information Security Oversight Office
(U) KC	key component
(U) NGA	National Geospatial-Intelligence Agency
(U) NSG	National System for Geospatial-Intelligence
(U) NSGM	National System for Geospatial Intelligence Manual
(U) OCA	Original Classification Authority
(U) ODNI	Office of the Director of National Intelligence
[redacted]	[redacted]
(U) OIG	Office of Inspector General
[redacted]	[redacted]

(U) Appendix F. Report Distribution

(U) Senate Committee on Homeland Security and Governmental Affairs
(U) Senate Select Committee on Intelligence
(U) House Committee on Homeland Security
(U) House Committee on Oversight and Government Reform
(U) House Permanent Select Committee on Intelligence
(U) Director of National Intelligence
(U) Director, Information Security Oversight Office
(U) Deputy Inspector General Intelligence and Special Programs Assessments, Department of Defense
(U) Director, NGA
(U) Deputy Director, NGA
[redacted]

(U) Appendix G. Management Comments



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
7500 GEOINT Drive
Springfield, Virginia 22150

U-2013-3097

SEP 26 2013

MEMORANDUM FOR OFFICE OF INSPECTOR GENERAL

SUBJECT: (U) Draft Report of NGA's Implementation of the Reducing Over-Classification Act (Project No. OIGE JI-13-01)

REFERENCE: (U) OIG Report Project No. OIGE JI-13-01, subject as above, September 2013 (U//FOUO)

1. (U//~~FOUO)~~ Thank you for the in-depth look at our workforce and business practices. We have reviewed the subject report and provide the following response to the findings and recommendations:

- (U//~~FOUO)~~ Recommendation #1: Restructure initial security training, including all required training areas.

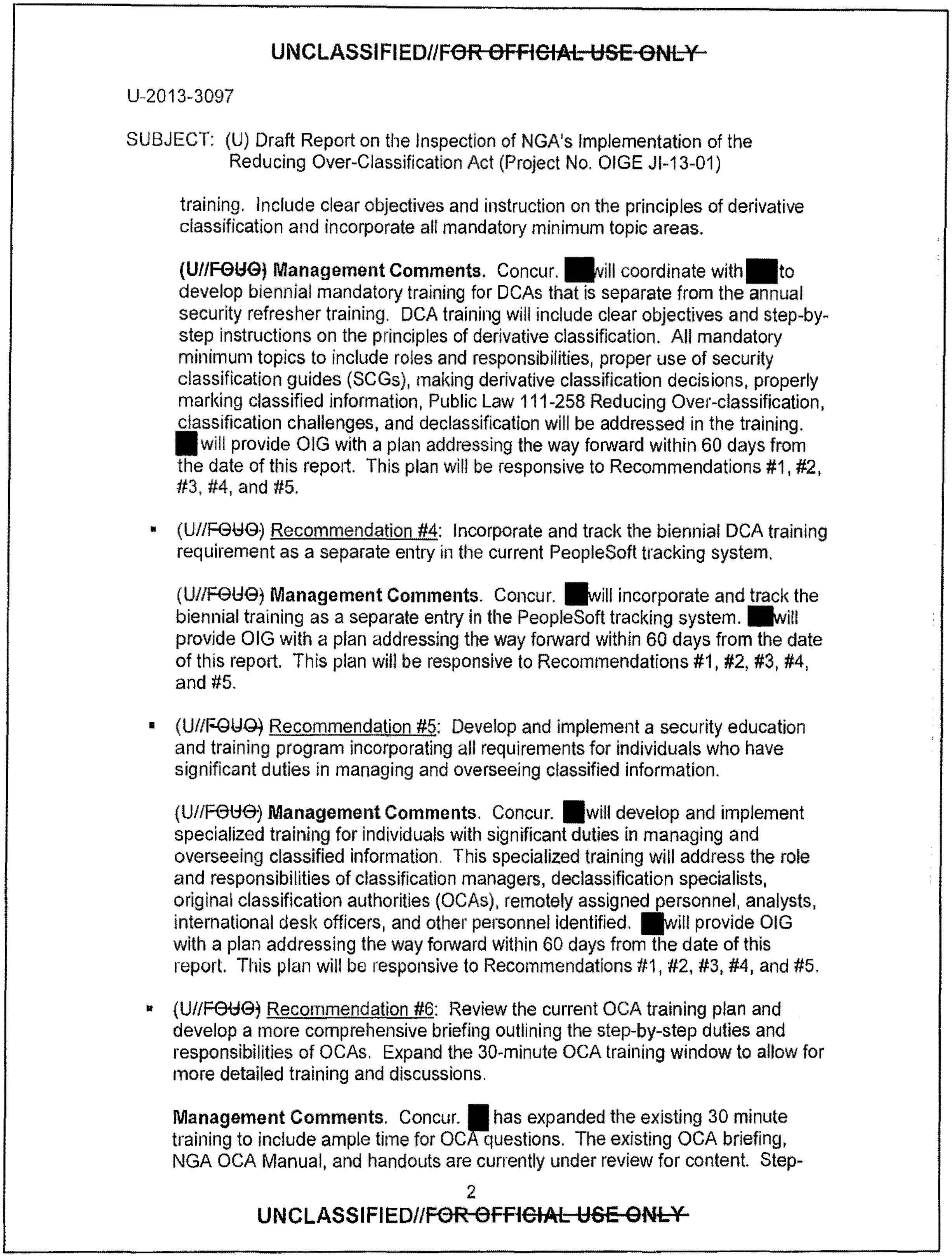
  (U//~~FOUO)~~ **Management Comments**. Concur. The [redacted] in collaboration with [redacted] began a security training restructure initiative in early 2013, specifically requesting the additional time needed to address all required areas. [redacted] will provide the Office of Inspector General (OIG) with a plan addressing actions already taken and the way forward within 60 days from the date of this report. This plan will be responsive to Recommendations #1, #2, #3, #4, and #5.

- (U//~~FOUO)~~ Recommendation #2: In coordination with the [redacted] conduct a resource assessment of the initial security training to determine the length of time required to sufficiently instruct new employees on required security policies, principles and practices. Consider creating a separate block of instruction focused specifically on classification management-related requirements.

  (U//~~FOUO)~~ **Management Comments**. Concur. [redacted] in concert with [redacted] will conduct a resource assessment of the initial security training to determine the length of time needed to sufficiently instruct new employees on security policies, principles, and practices and additional personnel needed to implement the training. This assessment will also address the inclusion of a separate block of instruction focused on classification management-related requirements. [redacted] will provide OIG with a plan addressing actions already taken and the way forward within 60 days from the date of this report. This plan will be responsive to Recommendations #1, #2, #3, #4, and #5.

- (U//~~FOUO)~~ Recommendation #3: Establish training for the derivative classification authority (DCA) separate from the annual security refresher

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



U-2013-3097

SUBJECT: (U) Draft Report on the Inspection of NGA's Implementation of the Reducing Over-Classification Act (Project No. OIGE JI-13-01)

training. Include clear objectives and instruction on the principles of derivative classification and incorporate all mandatory minimum topic areas.

(U//~~FOUO~~) Management Comments. Concur. [redacted] will coordinate with [redacted] to develop biennial mandatory training for DCAs that is separate from the annual security refresher training. DCA training will include clear objectives and step-by-step instructions on the principles of derivative classification. All mandatory minimum topics to include roles and responsibilities, proper use of security classification guides (SCGs), making derivative classification decisions, properly marking classified information, Public Law 111-258 Reducing Over-classification, classification challenges, and declassification will be addressed in the training. [redacted] will provide OIG with a plan addressing the way forward within 60 days from the date of this report. This plan will be responsive to Recommendations #1, #2, #3, #4, and #5.

- (U//~~FOUO~~) Recommendation #4: Incorporate and track the biennial DCA training requirement as a separate entry in the current PeopleSoft tracking system.

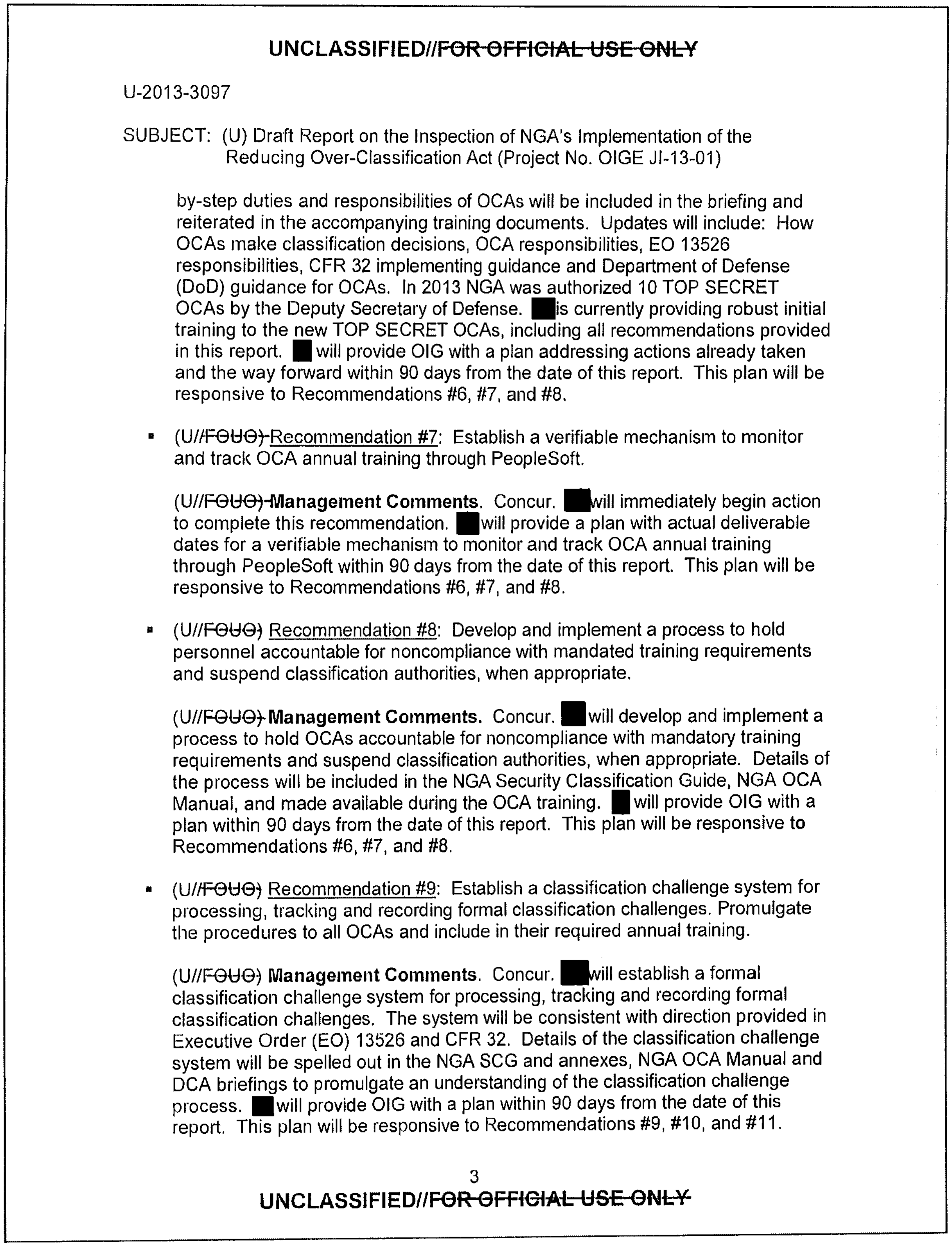
  (U//~~FOUO~~) **Management Comments**. Concur. [redacted] will incorporate and track the biennial training as a separate entry in the PeopleSoft tracking system. [redacted] will provide OIG with a plan addressing the way forward within 60 days from the date of this report. This plan will be responsive to Recommendations #1, #2, #3, #4, and #5.

- (U//~~FOUO~~) Recommendation #5: Develop and implement a security education and training program incorporating all requirements for individuals who have significant duties in managing and overseeing classified information.

  (U//~~FOUO~~) **Management Comments**. Concur. [redacted] will develop and implement specialized training for individuals with significant duties in managing and overseeing classified information. This specialized training will address the role and responsibilities of classification managers, declassification specialists, original classification authorities (OCAs), remotely assigned personnel, analysts, international desk officers, and other personnel identified. [redacted] will provide OIG with a plan addressing the way forward within 60 days from the date of this report. This plan will be responsive to Recommendations #1, #2, #3, #4, and #5.

- (U//~~FOUO~~) Recommendation #6: Review the current OCA training plan and develop a more comprehensive briefing outlining the step-by-step duties and responsibilities of OCAs. Expand the 30-minute OCA training window to allow for more detailed training and discussions.

  Management Comments. Concur. [redacted] has expanded the existing 30 minute training to include ample time for OCA questions. The existing OCA briefing, NGA OCA Manual, and handouts are currently under review for content. Step-



U-2013-3097

SUBJECT: (U) Draft Report on the Inspection of NGA's Implementation of the Reducing Over-Classification Act (Project No. OIGE JI-13-01)

by-step duties and responsibilities of OCAs will be included in the briefing and reiterated in the accompanying training documents. Updates will include: How OCAs make classification decisions, OCA responsibilities, EO 13526 responsibilities, CFR 32 implementing guidance and Department of Defense (DoD) guidance for OCAs. In 2013 NGA was authorized 10 TOP SECRET OCAs by the Deputy Secretary of Defense. [redacted] is currently providing robust initial training to the new TOP SECRET OCAs, including all recommendations provided in this report. [redacted] will provide OIG with a plan addressing actions already taken and the way forward within 90 days from the date of this report. This plan will be responsive to Recommendations #6, #7, and #8.

- (U//~~FOUO)~~ Recommendation #7: Establish a verifiable mechanism to monitor and track OCA annual training through PeopleSoft.

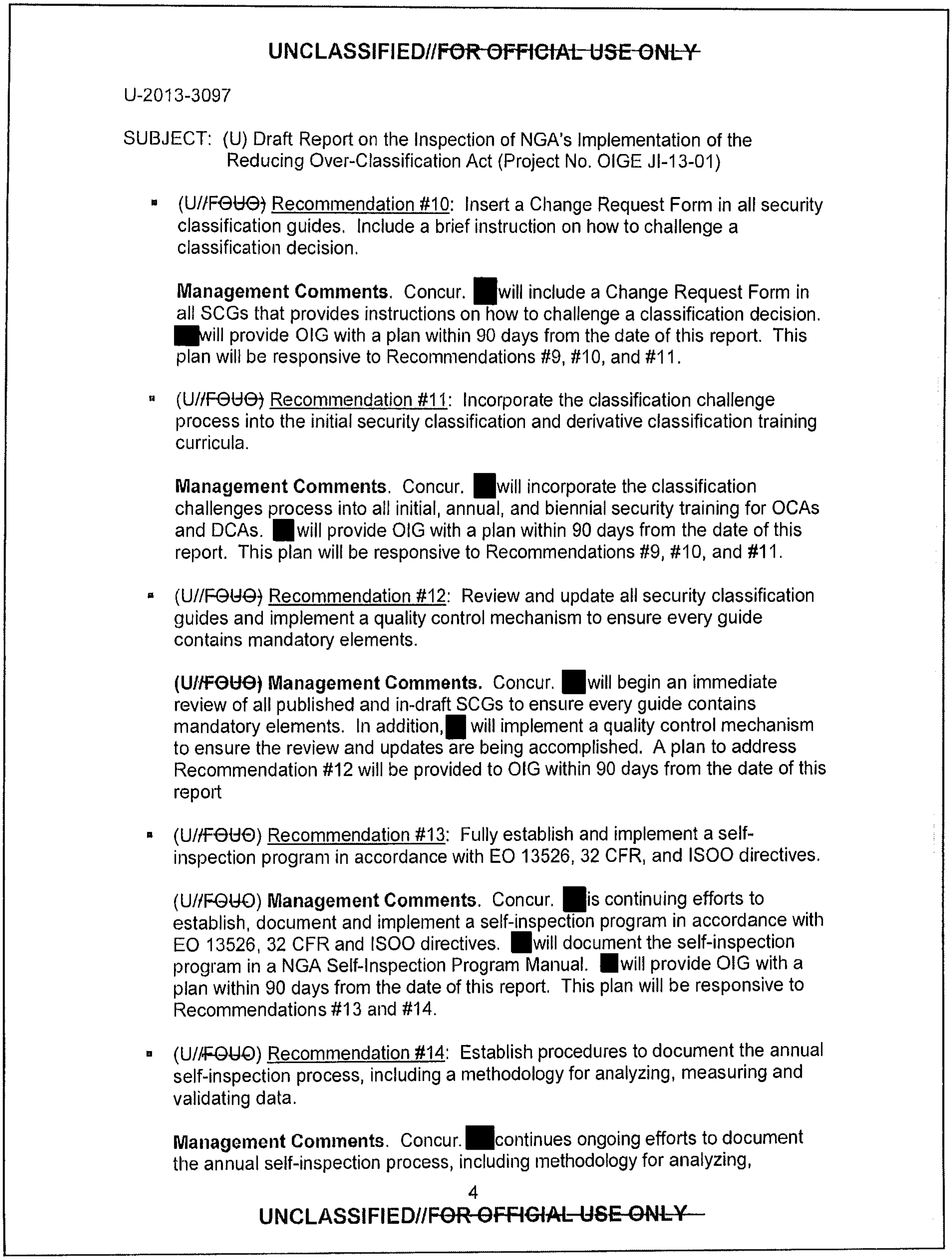
  (U//~~FOUO)~~ **Management Comments**. Concur. [redacted] will immediately begin action to complete this recommendation. [redacted] will provide a plan with actual deliverable dates for a verifiable mechanism to monitor and track OCA annual training through PeopleSoft within 90 days from the date of this report. This plan will be responsive to Recommendations #6, #7, and #8.

- (U//~~FOUO)~~ Recommendation #8: Develop and implement a process to hold personnel accountable for noncompliance with mandated training requirements and suspend classification authorities, when appropriate.

  (U//~~FOUO)~~ **Management Comments.** Concur. [redacted] will develop and implement a process to hold OCAs accountable for noncompliance with mandatory training requirements and suspend classification authorities, when appropriate. Details of the process will be included in the NGA Security Classification Guide, NGA OCA Manual, and made available during the OCA training. [redacted] will provide OIG with a plan within 90 days from the date of this report. This plan will be responsive to Recommendations #6, #7, and #8.

- (U//~~FOUO)~~ Recommendation #9: Establish a classification challenge system for processing, tracking and recording formal classification challenges. Promulgate the procedures to all OCAs and include in their required annual training.

  (U//~~FOUO)~~ **Management Comments**. Concur. [redacted] will establish a formal classification challenge system for processing, tracking and recording formal classification challenges. The system will be consistent with direction provided in Executive Order (EO) 13526 and CFR 32. Details of the classification challenge system will be spelled out in the NGA SCG and annexes, NGA OCA Manual and DCA briefings to promulgate an understanding of the classification challenge process. [redacted] will provide OIG with a plan within 90 days from the date of this report. This plan will be responsive to Recommendations #9, #10, and #11.



U-2013-3097

SUBJECT: (U) Draft Report on the Inspection of NGA's Implementation of the Reducing Over-Classification Act (Project No. OIGE JI-13-01)

- (U//~~FOUO~~) Recommendation #10: Insert a Change Request Form in all security classification guides. Include a brief instruction on how to challenge a classification decision.

  Management Comments. Concur. [redacted] will include a Change Request Form in all SCGs that provides instructions on how to challenge a classification decision. [redacted] will provide OIG with a plan within 90 days from the date of this report. This plan will be responsive to Recommendations #9, #10, and #11.

- (U//~~FOUO~~) Recommendation #11: Incorporate the classification challenge process into the initial security classification and derivative classification training curricula.

  Management Comments. Concur. [redacted] will incorporate the classification challenges process into all initial, annual, and biennial security training for OCAs and DCAs. [redacted] will provide OIG with a plan within 90 days from the date of this report. This plan will be responsive to Recommendations #9, #10, and #11.

- (U//~~FOUO~~) Recommendation #12: Review and update all security classification guides and implement a quality control mechanism to ensure every guide contains mandatory elements.

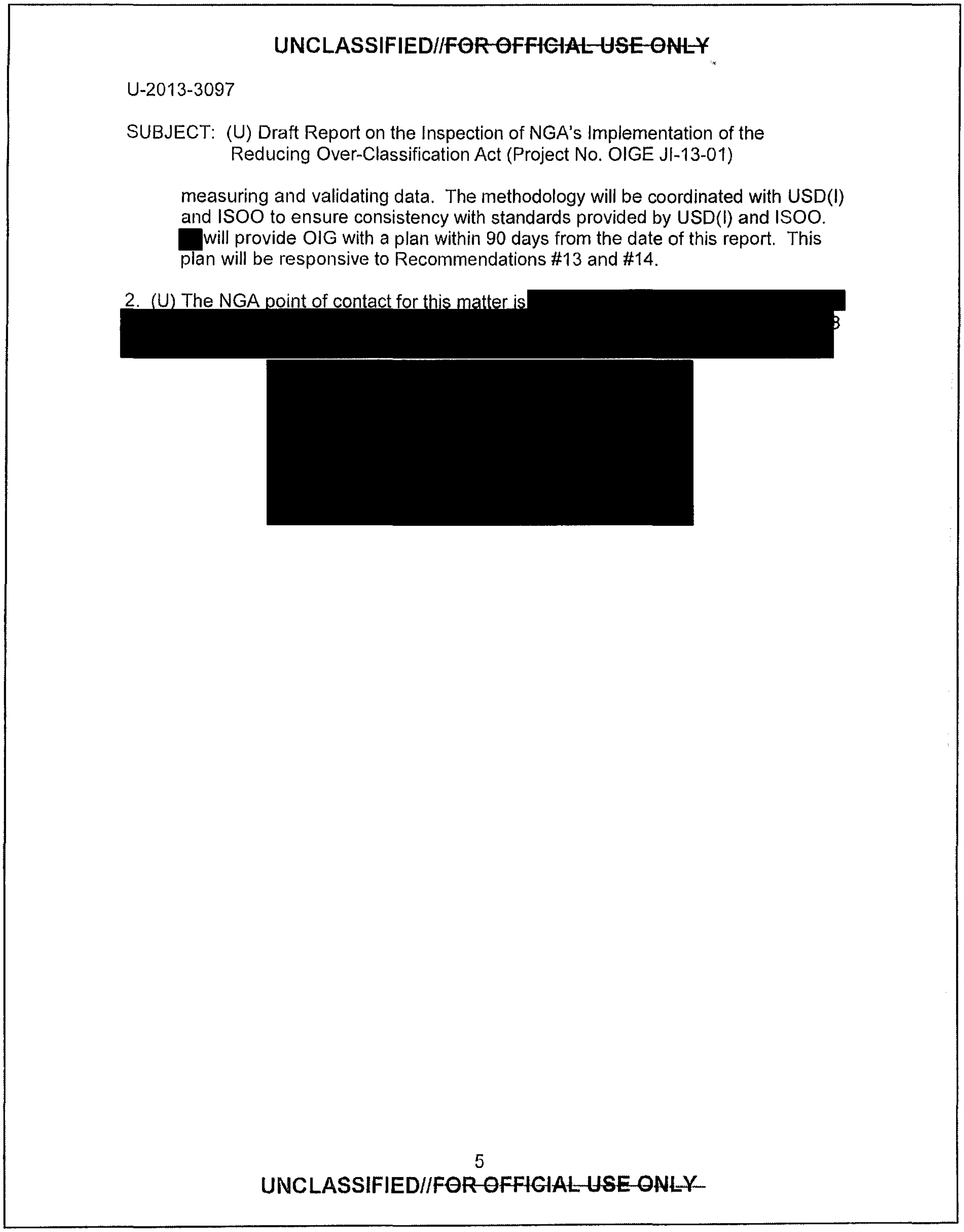
  (U//~~FOUO~~) Management Comments. Concur. [redacted] will begin an immediate review of all published and in-draft SCGs to ensure every guide contains mandatory elements. In addition, [redacted] will implement a quality control mechanism to ensure the review and updates are being accomplished. A plan to address Recommendation #12 will be provided to OIG within 90 days from the date of this report

- (U//~~FOUO~~) Recommendation #13: Fully establish and implement a self-inspection program in accordance with EO 13526, 32 CFR, and ISOO directives.

  (U//~~FOUO~~) **Management Comments**. Concur. [redacted] is continuing efforts to establish, document and implement a self-inspection program in accordance with EO 13526, 32 CFR and ISOO directives. [redacted] will document the self-inspection program in a NGA Self-Inspection Program Manual. [redacted] will provide OIG with a plan within 90 days from the date of this report. This plan will be responsive to Recommendations #13 and #14.

- (U//~~FOUO~~) Recommendation #14: Establish procedures to document the annual self-inspection process, including a methodology for analyzing, measuring and validating data.

  Management Comments. Concur. [redacted] continues ongoing efforts to document the annual self-inspection process, including methodology for analyzing,



measuring and validating data. The methodology will be coordinated with USD(I) and ISOO to ensure consistency with standards provided by USD(I) and ISOO. [redacted] will provide OIG with a plan within 90 days from the date of this report. This plan will be responsive to Recommendations #13 and #14.

2. (U) The NGA point of contact for this matter is [redacted]

[redacted]