Description of document:	National Reconnaissance Office (NRO) Inspector General (OIG) report (due September 30, 2013) on reducing over-classification required in Section 6 of the Reducing Over-Classification Act (H.R. 553)
Requested date:	08-October-2013
Released date:	03-February-2014
Posted date:	24-February-2014
Title of document	National Reconnaissance Office Office of Inspector General Final Report (U) Evaluation of the National Reconnaissance Office Classification Management under Public Law 111-258, the Reducing Over-Classification Act (Project Number 2013-001 S) 30 September 2013
Source of document:	National Reconnaissance Office MS&O/Information Access and Release Team 14675 Lee Road Chantilly, VA 20151-1715 Fax: (703) 227-9198 Email: foia@nro.mil Online Request Form

NATIONAL RECONNAISSANCE OFFICE
14675 Lee Road
Chantilly, VA 20151-1715

3 February 2014

This is in response to your request dated 8 October 2013, received in the Information Management Services Office of the (NRO) on 17 October 2013. Pursuant to the Freedom of Information Act (FOIA), you are requesting "a copy of the NRO Inspector General report (due September 30, 2013) on reducing over-classification required in Section 6 of the Reducing Over-Classification Act (H.R. 553)."

Your request has been processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. A thorough search of our files and databases located thirty-three (33) pages responsive to your request. These pages are being released to you in part.

Material redacted is denied pursuant to FOIA exemption (b)(6) which applies to records which, if released, would constitute a clearly unwarranted invasion of the personal privacy of individuals; and exemption (b)(3), which applies to information exempt from disclosure by statute. The relevant withholding statute is 10 U.S.C. §424, which provides (except as required by the President or for information provided to Congress), that "no provision of law shall be construed to require the disclosure" of the organization or any function of NRO, including the function of protecting intelligence sources and methods from unauthorized disclosure, or the name, official title, occupational series, grade, salary or numbers of persons employed by or assigned or detailed to the NRO.

The FOIA authorizes federal agencies to assess fees for record services. Based upon the information provided, you have been placed in the "other" category of requesters, which means you are responsible for the cost of search time exceeding two hours ($44.00/hour) and reproduction fees (.15 per page) exceeding 100 pages. In this case, no assessable fees were incurred in processing your request. Additional information about fees can be found on our website at www.nro.gov.

You have the right to appeal this determination by addressing your appeal to the NRO Appeal Authority, 14675 Lee Road, Chantilly, VA 20151-1715 within 60 days of the date of this letter. Should you decide to do so, please explain the basis of your appeal.

If you have any questions, please call the Requester Service Center at (703) 227-9326 and reference case number **F14-0004.**

Sincerely,

Kimberley W. Condas
(Acting) Chief, Information Review
and Release Group

Enclosure: NRO Office of Inspector General Final Report: Evaluation of NRO Classification Management, 30 September 2013

NATIONAL RECONNAISSANCE OFFICE

OFFICE OF INSPECTOR GENERAL

FINAL REPORT

(U) Evaluation of the National Reconnaissance Office Classification Management under Public Law 111-258, the *Reducing Over-Classification Act*

(Project Number 2013-001 S)

30 September 2013

THIS PAGE INTENTIONALLY LEFT BLANK

NATIONAL RECONNAISSANCE OFFICE
Office of Inspector General
14675 Lee Road
Chantilly, VA 20151-1715

30 September 2013

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: (U) Final Report: Evaluation of the National Reconnaissance Office Classification Management under Public Law 111-258, the *Reducing Over-Classification Act* (Project Number 2013-001 S)

(U) The National Reconnaissance Office (NRO) Office of Inspector General (OIG) has conducted the Evaluation of the NRO's Classification Management Program in compliance with the *Reducing Over-Classification Act*. The Public Law 111-258 requires the OIG to complete a second evaluation by 30 September 2016. For the second evaluation, we will follow-up on the recommendations outlined in this report.

(U//FOUO) I appreciate the courtesies extended to my staff during this evaluation. Please direct any questions you may have regarding this evaluation to (b)(3) 10 U S C. 424, (b)(6) Deputy Assistant Inspector General for Acquisition Audits, at (b)(3) 10 U.S.C. (secure).

Lanie D'Alessandro
Inspector General

Attachment:
(U) Final Report
(Project Number 2013-001 S)
(U//FOUO)

THIS PAGE INTENTIONALLY LEFT BLANK

SUBJECT: (U) Final Report: Evaluation of the National Reconnaissance Office Classification Management under Public Law 111-258, the *Reducing Over-Classification Act* (Project Number 2013-001 S)

DISTRIBUTION:

Hardcopy:

Internal:
Director, National Reconnaissance Office
Principal Deputy Director, National Reconnaissance Office
Deputy Director, National Reconnaissance Office
Director, Office of Security and Counterintelligence
Assistant Inspector General for Audits, (b)(3) 10 U.S.C. 424, (b
Evaluation Lead, (b)(3) 10 U.S.C. 424, (for official file)
OIG Follow-up Administrator (b)(3) 10 U.S.C. 424, (b
OIG Chrono file

External:
Senate Committee on Homeland Security and Governmental Affairs
Senate Select Committee on Intelligence
House Committee on Homeland Security
House Committee on Oversight and Government Reform
House Permanent Select Committee on Intelligence
Director, Information Security Oversight Office, National Archives and Records Administration

Softcopy:
action-ig (TIER)

THIS PAGE INTENTIONALLY LEFT BLANK

NRO APPROVED FOR RELEASE 3 FEBRUARY 2014

(U) NATIONAL RECONNAISSANCE OFFICE
OFFICE OF INSPECTOR GENERAL

(U) Evaluation of the NRO's Classification Management under Public Law 111-258, the *Reducing Over-Classification Act* (Project Number 2013-001 S)

(U) EXECUTIVE SUMMARY

(U) INTRODUCTION

(U) The National Reconnaissance Office (NRO) Office of Inspector General (OIG) conducted this evaluation of the NRO's classification management as required by Public Law 111-258, the *Reducing Over-Classification Act*, October 2010. The objectives of the evaluation were to

- assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered;
- identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification; and
- coordinate with other Inspectors General and with the Information Security Oversight Office (ISOO) to ensure that evaluations follow a consistent methodology that allows for cross-agency comparisons.

(U) RESULTS IN BRIEF

(U//FOUO) Overall, the NRO has not fully adopted, followed, or effectively administered federally required classification policies, procedures, rules, and regulations. While the NRO complies with federal reporting and original classification authority (OCA) designation requirements, we found that NRO classification management practices and procedures do not comply with applicable federal laws and guidance. Specifically, we found that the

- NRO classification policies do not fully capture the federal classification requirements, and the NRO is not adhering to its classification policies;
- NRO classification training is not compliant in all aspects with federal laws;
- NRO OCAs and derivative classifiers are not consistently classifying in accordance with the federal laws and guidance;
- NRO OCAs and derivative classifiers lack sufficient knowledge of their classification responsibilities; and
- NRO does not have a classification management self-inspection program in line with the requirements of the federal laws and guidance.

NRO APPROVED FOR RELEASE 3 FEBRUARY 2014

(U) SUMMARY OF RECOMMENDATIONS

(U//FOUO) In order to strengthen the management and oversight of the NRO's classification management program, the NRO needs to adopt, follow, and effectively administer federal classification standards and procedures. Accordingly, we recommend that the Director, Office of Security and Counterintelligence (D/OS&CI) establish NRO classification management policies that comply with the collective requirements of federal laws and guidance. We also recommend that the D/OS&CI establish proper classification oversight activities to include mandatory training and ensure that classification policies are clearly communicated, implemented, and followed.

(U) MANAGEMENT COMMENTS

(U//FOUO) The D/OS&CI non-concurred with the report as written but did not provide specific comments on the recommendations. OS&CI agreed there is room for improvement in various aspects of the NRO's classification management activities, but strongly disagreed with the primary conclusions documented in the report. A complete copy of their comments can be found in Appendix C. Based on the comments we received, we have updated the final report where appropriate.

(U//FOUO) The Public Law 111-258 requires the OIG to perform a second evaluation by 30 September 2016 where we will assess the progress made by the NRO to be fully compliant with federal laws and guidance.

(U) TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

NRO APPROVED FOR RELEASE 3 FEBRUARY 2014

(U) NATIONAL RECONNAISSANCE OFFICE
OFFICE OF INSPECTOR GENERAL

(U) Evaluation of the NRO's Classification Management under Public Law 111-258, the *Reducing Over-Classification Act* (Project Number 2013-001 S)

(U) INTRODUCTION

(U) The National Reconnaissance Office (NRO) Office of Inspector General (OIG) conducted this evaluation of the NRO classification management as required by Public Law 111-258, the *Reducing Over-Classification Act*, October 2010 (the Act). Section 6(b) of the Act requires the Inspector General (IG) of each department or agency with an officer or employee who is authorized to make original classifications, in consultation with the Information Security Oversight Office (ISOO),[1] to

- assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered;
- identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification; and
- coordinate with other IGs and with the ISOO to ensure that evaluations follow a consistent methodology that allows for cross-agency comparisons.

(U) The Act requires the OIG to complete the initial evaluation by 30 September 2013. In addition, the Act requires the OIG to complete a second evaluation by 30 September 2016. For the second evaluation, we will follow-up on the recommendations outlined in this report.

(U) BACKGROUND

(U) In an intelligence environment seeking to balance the need to share and the need to know, accurately classified information is critical. By classifying correctly, the NRO lessens the potential compromise of sources and methods, and protects its assets and the lives of its personnel. In addition, by classifying appropriately, the NRO rightfully permits information sharing with those mission partners who have the authority and the need to know that information.

(U) If information is not properly classified (e.g., classified at too high or too restrictive a level), the NRO cannot share the information with others in the NRO, the Intelligence Community (IC), or even mission partners who need that information to help fulfill the NRO and overall IC mission. If information is classified at too low a level, the NRO risks classified information being compromised or shared with those not intended to receive it. Either way,

[1] (U) The ISOO is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program. The ISOO is a component of the National Archives and Records Administration and receives policy and program guidance from the National Security Council.

mission, resources, and possibly lives are at risk. Accordingly, the NRO needs to adopt, follow, and effectively administer federal classification standards and procedures.

(U) Federal Classification Standards and Procedures

(U) Congress created the Act to address issues highlighted by The National Commission on Terrorist Attacks Upon the United States (commonly known as the "9/11 Commission") concerning over-classification and excessive compartmentalization of national security information. The Act promotes sharing information as prescribed by Federal guidelines.

(U) In addition to the Act, the federal government has directed government-wide classification standards and procedures. In 2009, the President signed Executive Order (E.O.) 13526, *Classified National Security Information* (the Order). The Order establishes the current principles, policies, and procedures for classification and prescribes a "uniform system for classifying, safeguarding, and declassifying national security information." 32 Code of Federal Regulations (CFR) Part 2001, *Classified National Security Information* (the Directive), "sets forth guidance to agencies on original and derivative classification, downgrading, declassification, and safeguarding of classified national security information."

(U) According to the Order, information may be classified originally or derivatively. Original Classification Authorities (OCAs) are individuals authorized in writing, either by the President, the Vice President, or agency heads or other officials designated by the President, to initially classify information. Original classification means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Derivative classifiers incorporate, paraphrase, restate, or generate in a new form information that is already classified, and mark the newly-developed material consistent with the classification markings that apply to the sourced information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(U) Pursuant to the Order and Directive, classified information that is determined to require protection against unauthorized disclosure to prevent damage to national security must be marked appropriately to indicate its classified status. The three United States classification levels are

- Top Secret – shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage* to the national security that the OCA is able to identify or describe.
- Secret – shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *serious damage* to the national security that the OCA is able to identify or describe.
- Confidential – shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *damage* to the national security that the OCA is able to identify or describe.

(U) Office of Director National Intelligence Policies

(U) The Office of the Director of National Intelligence (ODNI) publishes the Controlled Access Program Coordination Office (CAPCO) Register and Manual as well as Intelligence Community Directives (ICDs) on classification management and control markings. The CAPCO is the authority for standard markings and portion markings throughout the Intelligence Community (IC).

(U) NRO Classification Structure and Authorities

(U) On 15 September 2010, the Director of National Intelligence (DNI) delegated authority for original Top Secret classification to the Director, NRO (DNRO) and the incumbents of 12 NRO senior positions.[2]

(U) The DNRO assigned to the Director, Office of Security and Counterintelligence (D/OS&CI) responsibility to manage the NRO program for protecting national intelligence and intelligence sources and methods, thereby fostering a culture of information sharing, and effectively responding to evolving critical threats through proactive and integrated policies. In addition, the D/OS&CI oversees NRO activities to protect NRO's intelligence information, including Sensitive Compartmented Information and special access program information. The D/OS&CI also manages and directs the NRO's Program Security Officer (PSO) Program.

(U) NRO Adoption of Federal and ODNI Guidance

(U) The NRO has promulgated regulations to implement its classified national security information programs in accordance with the Order and Directive. The NRO OS&CI provided the following NRO regulations used for classification management:

- ***Integrated NRO Classification Guide*** **(INCG)** – is the primary source document for classification of NRO systems and resources.
- **INCG Annex A** – is the primary classification guide for NRO information not releasable to foreign nationals (NOFORN)
- ***The NRO Security Manual*** **(NSM) v3** – is the overall guide for how security is executed within the NRO
- **NRO Directive (ND) for the Reserve (RSV) program, ND 100-35** ***NRO RESERVE Control System*** – the directive hosts the processes for the reviews and de-confliction of all RESERVE compartment documentation (e.g., Program Protection Plans, Classification Guides, etc.)

---

[2] (U) The 12 NRO OCA positions are Principal Deputy Director (PDDNRO); Deputy Director (DDNRO); Director, Imagery Intelligence Systems Acquisition Directorate (D/IMINT); Director, Signals Intelligence Systems Acquisition Directorate (D/SIGINT); Director, Communications Systems Directorate (D/COMM); Director, Advanced Systems and Technology Directorate (D/AS&T); Director, Mission Operations Directorate (D/MOD); Director, Special Communications Office (D/SCO); Director, Ground Enterprise Directorate (D/GED); Director, Office of Security and Counterintelligence (D/OS&CI); Director, Office of Space Launch (D/OSL); and Director, Mission Support Directorate (D/MSD).

- **OS&CI Policy Note 2011-04, "Implementation Policy for Executive Order 13526, Classified National Security Information"** – provides the implementation guidance to the NRO for E.O. 13526

(U) Previous Classification Review

(U) In August and September of 2009, the ISOO performed a classification review of 15 agencies that generated 10,000 or more classification decisions in fiscal year (FY) 2008. The NRO was included as part of the classification review. The ISOO reviewed 96 NRO classified documents and found a total of 114 discrepancies in 61 documents.

(U) SCOPE AND METHODOLOGY

(U) We conducted this evaluation from May through September 2013 in accordance with Quality Standards for Inspections and Evaluations issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The evidence obtained provides a reasonable basis for our findings and conclusions.

(U) To accomplish our evaluation, we used an evaluation guide prepared on behalf of CIGIE by a working group of IG offices participating in this government-wide effort. The evaluation guide was intended to meet the requirements of the Act regarding the classification responsibilities of each participating department and agency. The IG offices formed the working group to ensure consistency in the evaluative process, comparable reporting, and the ability to compare results across agencies. As directed by the Act, we consulted with the ISOO and coordinated throughout the evaluation with other IG offices with the objective of ensuring that all evaluations followed a consistent methodology to allow for cross-agency comparisons. The evaluation focused on eight areas:

1. General program management responsibilities
2. Security education and training
3. Original classification
4. Derivative classification
5. Self-inspections
6. Original classification authority
7. Reporting and definitions
8. Intelligence Community crosscutting issues

(U) We examined whether NRO policies and practices were consistent with the Order and Directive and applied the ISOO evaluation tools including

- an agency implementing regulation assessment tool (See Appendix A);
- methodology for determining the appropriateness of original classification and derivative classification decisions;
- original classification authority interview coverage; and
- derivative classifier interview coverage.

(U) In addition, we interviewed OCAs, derivative classifiers, and selected a non-statistical sample[3] of classified documents to assess the level that applicable classification policies, procedures, rules, and regulations have been adopted, followed, and administered (See Appendix B for the detailed sampling methodology). To accomplish this objective, we reviewed NRO classification policies, procedures, rules, and regulations. Additionally, we interviewed NRO officials responsible for related policy development, implementation, and classification training of OCAs, and derivative classifiers. Finally, we examined

- the results of the fundamental classification guidance review and the self-inspection program; and
- the reporting results of ICD 710 and Standard Form (SF) 311, "Agency Security Classification Management Program Data" for FYs 2010 to 2012.[4]

(U) EVALUATION RESULTS

(U//FOUO) Overall, the NRO has not fully adopted, followed, or effectively administered federally required classification policies, procedures, rules, and regulations. While the NRO complies with federal reporting and OCA designation requirements, we found that NRO classification management practices and procedures did not comply with applicable federal laws and guidance. Specifically, we found that the

- NRO classification policies do not fully capture the federal classification, requirements, and the NRO is not adhering to its classification policies;
- NRO classification training is not compliant in all aspects with federal laws;
- NRO OCAs and derivative classifiers are not consistently classifying in accordance with the Order and Directive;
- NRO OCAs and derivative classifiers lack sufficient knowledge of their classification responsibilities; and
- NRO does not have a classification management self-inspection program in line with the requirements of the Order and Directive.

(U//FOUO) Because of the lack of compliance in multiple areas, the NRO is susceptible to the risk of persistent misclassification of NRO documents and information. The NRO would benefit from a comprehensive review of its policies and procedures to ensure that it complies with the federal classification requirements. In addition, the NRO would benefit from improved enforcement and monitoring of classification activities, such as OCA and derivative classification training. Increased vigilance over NRO policies, procedures, rules, regulations, and management practices would reduce the NRO exposure to persistent misclassification.

[3] (U) When non-statistical sampling is used, the sample size is not determined mathematically. We used our judgment in determining a representative sample of documents and we evaluated the selected documents against the cited federal and NRO criteria.

[4] (U) We noted the 2013 ICD 710, which applies to the Order guidelines for the IC, was not released until 21 June 2013 three years after the Order was effective.

(U) NRO Annual Reporting and OCA Designations Meet Federal Requirements

(U) We found that the NRO complies with specific federal classification management annual reporting and OCA designation and delegation requirements. For example, the Directive requires that agencies report statistical data related to their security classification programs to the ISOO each year. Agencies use the SF 311 for inclusion in a report to the President. The OS&CI submitted the NRO's SF 311 to the Under Secretary of Defense for Intelligence (USD(I)) for fiscal years 2010, 2011, and 2012. We confirmed that the USD(I) incorporated the NRO's information into a consolidated SF 311 report of Department of Defense (DoD) components and submitted a final report to ISOO. For the same fiscal years, the NRO also submitted to ISOO an SF 716, *Agency Security Classification Cost Estimates* to document the NRO's accounting for cost of implementing the Order. Still, we observed that the NRO did not include these reporting requirements into the NRO governing manuals, guides, or policies. Incorporating the reporting requirements would provide better assurance that the NRO will remain compliant with these reporting requirements.

(U) In addition, the NRO is compliant with the original classification authority designation and delegation requirements of the Order and Directive. The NRO has requested and received original classification authority from the ODNI, and the NRO satisfied all designation requirements found within the Order and Directive. We confirmed that the NRO met all criteria and reporting requirements for the 13 OCA delegation positions.

(U//FOUO) NRO Classification Policies and Procedures do not Fully Capture Federal Requirements and the NRO does not Adhere to Its Policies

(U//FOUO) We found that the NRO classification policies and procedures do not fully capture the Order, Directive, or ODNI guidance. Moreover, the NRO classification and security officials were not adhering to the Order, Directive, or ODNI guidance as they were incorporated into the NRO policies.

(U//FOUO) While the NRO policies and regulations align with several of the Order, Directive, and ODNI policy requirements, as shown in Table 1 (below), not all of the requirements have been incorporated.

Table 1: (U) NRO Policy Alignment with the Order, Directive, and ODNI Guidance

(U) Incorporated in NRO Policies	(U) Not Incorporated in NRO Policies
▪ Original Classification Authority designation and delegation ▪ Derivative classification training ▪ Suspension of OCA authorities ▪ The rating of personnel on the performance of duties relating to the designation and management of classified information ▪ Designation of a senior agency official to direct and administer the program ▪ Establishment of a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper classification as needed ▪ Coordination for preparing the ODNI's Annual Review of Controlled Access Programs report, the USD(I)'s Annual Special Access Program (SAP) report	▪ Working paper guidance ▪ Prohibitions and limitations ▪ Safeguarding classified information originated by non-OCAs ▪ Incentives for accurate classification ▪ Reporting elements ▪ NRO inclusive self-inspection program

(U) This table is Unclassified

(U//~~FOUO~~) Our assessment found that the NRO classification and security officials were not adhering to the policy requirements. For example, NRO has not conducted timely reviews or updates of the NRO's Review and Redaction Guide (RRG) or its security classification guides (SCGs). The Directive states, "Agency declassification guides shall be reviewed and updated as circumstances require, but at least once every five years. Each agency shall maintain a list of its declassification guides in use." Additionally, the NRO is not meeting its own requirement under the D/OS&CI Policy Note 2011-04 (Rev 1), "Implementation Policy for Executive Order 13526," which requires five-year reviews for all SCGs. The previous NRO RRG, dated 2005, and three of the 62 SCGs had not been reviewed within five years. SCGs that are significantly overdue for review are at risk of providing invalid classification determinations guidance resulting in derivative classifiers misclassifying documents.

(U//~~FOUO~~) Furthermore, OS&CI does not maintain an inventory of all the SCGs used by the NRO, nor does it enforce the requirement for originating offices to provide soft copies of their SCGs to OS&CI as described within the policy note. Consequently, the OS&CI lacks insight and control over the SCGs the NRO workforce and IC partners are using to classify documents. Moreover, the NRO has not adhered to the Order's requirement to disseminate its implementing regulations—Policy Note 2011-04 (Rev 1) "Implementation Policy for E.O. 13526"—in the Federal Register for public knowledge. OS&CI Policy Branch could not provide

any documentation as to why the policy note was not pertinent to the public and did not require being published in the Federal Register.

(U//FOUO) As a part of this evaluation, we found the following cases of inadequate monitoring and adherence to classification policies, procedures, rules, and regulations.

- The Order requires that NRO security professionals and the NRO workforce have classification management as a rated performance area. None of the PSOs we interviewed had classification management as a performance element for themselves or their security staffs. The OS&CI provided no evidence of compliance with this requirement.

- The OS&CI has not addressed inaccuracies in the NRO's Classification Management Tool (CMT). According to OS&CI, the CAPCO requested that the NRO identify a solution for the CMT since the tool had a technical issue and could not properly support the use of RRG within the classification block. The OS&CI requested a change from the ISOO, who in-turn approved deleting RRG from the classification block for the NRO. The OS&CI was to initiate actions to remove the RRG from the classification block in the CMT, so that all electronically developed documents were correctly marked. To date, the CMT still incorrectly inserts the RRG line and all classified documents created since 3 April 2013 have incorrect classification block information.

- The OS&CI provided incorrect NRO classification block guidance between the years of 2005-2012. The NRO OCAs did not have the authority to grant automatic declassification at 50 years during this time. In 2012, the ISOO/Interagency Security Classification Appeals Panel (ISCAP) approved the NRO's authority to exempt information from automatic declassification at 25 and 50 years. NRO OCA and derivative classifiers did not have the authority to mark NRO documents referring to the 2005 RRG with a 50-year exemption. Consequently, NRO classification blocks from 2005 to 2012 have incorrect declassification exemption determinations.

- The NRO self imposed more restrictive timeline requirements for annual OCA training. The Order requires annual OCA training be completed by the end of the calendar year (CY). D/OS&CI Policy Note 2011-04 (Rev 1) states all OCA training will be completed by 1 June of each CY. The 2013 OCA Training briefing states that the ODNI requires OCA training to be completed by 30 June. As a result, only two of the 13 NRO OCAs met the NRO and ODNI requirement in 2012. Noncompliance with the NRO and ODNI policies requires the DNRO or PDDNRO to suspend OCA delegation; however, according to OS&CI, no suspensions were enacted.

- Oversight and internal collaboration of classification management policy is limited. The NRO established a Classification Management Working Group (CWMG). However, interviews and evidence showed that the CMWG has not met for an extended period of time. As a result, NRO classification management issues, such as training and policy changes, have no dedicated forum for discussion.

(U//FOUO) The NRO OS&CI Policy Branch officials acknowledged that they have the responsibility to create classification management policies. However, even though they could not identify who was accountable for classification management, nonetheless, they maintained it is not their responsibility to ensure that the NRO is effectively classifying documents. These gaps between policy development and implementation oversight are a significant weakness. They have contributed to the NRO being susceptible to misclassification of information due to the lack of consistency in management of classification knowledge dissemination throughout the NRO population.

(U//FOUO) NRO Classification Training Does Not Comply with Federal Requirements

(U//FOUO) We found that the NRO guidance for classification training is not fully compliant with the federal classification training requirements. The Act, Order, and Directive require annual training for OCAs and training at least once every two years for all derivative classifiers. The NRO established guidance for OCA and derivative training, and the D/OS&CI policy note 2011-04 (Rev 1) complies with the federal requirements for OCAs and all derivative classifiers located at the NRO headquarters facilities. However, the guidance excludes a significant portion of the NRO workforce having derivative classification duties. The policy note requirement does not extend to NRO contractors performing derivative classification at other facilities. In the 2012 ICD 710 Report to the ODNI, the OS&CI reported that the "NRO has not made [derivative classification training for contractors] a mandatory requirement because the cost of allowing two hours of direct labor charging by each contractor individual is cost prohibitive in this time of declining budgets." Yet, the NRO Acquisition Manual (NAM) requires contractors with access to national security information to comply with IC and NRO classification and program security directives, instructions, policy guidance, and standards. In addition, the NRO Office of Contracts Policy stated that such training would be an allowable cost on NRO contracts, including NRO contractors performing derivative classification at other facilities.

(U//FOUO) In addition, the NRO's implementation of OCA and derivative training does not meet the requirements of the Order and Directive. For example, the NRO OS&CI Policy Branch develops a yearly PowerPoint presentation that is reviewed by the NRO OCAs for their annual OCA training. The 2012 and 2013 PowerPoint presentations do not include the topics of classification challenges, security classification guides, and information sharing in accordance with the Directive. The OS&CI Policy Branch relies on the Chiefs of Security and PSOs to administer the training, but the Policy Branch does not provide guidance on how to conduct the training. In addition, the Policy Branch does not perform any follow-up activities to ensure a standardized level of knowledge exists across the OCAs. When asked, the OS&CI Policy Branch stated that they were not required to provide training to government derivative classifiers. They assumed that the government derivative classifiers were taking the training available through the CAPCO. However, we found that assumption was incorrect for the majority of derivative classifiers.

(U//FOUO) Similarly, the NRO OS&CI Training Office provides a mandatory Annual Security Refresher (ASR) training to the entire NRO workforce as derivative classifiers.

The ASR focuses on several areas, including classification management. We reviewed the 2013 ASR classification questions and determined that the 2013 ASR training fell short in meeting the requirements of the Directive as it did not address required topics such as duration of classification and classification challenges. We were equally concerned that the OS&CI Policy Branch and the OS&CI Training Office do not share insights into classification management problems that could be useful in the development of the ASR training metrics.

(U//~~FOUO~~) NRO OCAs and Derivative Classifiers Are Not Properly Classifying Documents

(U//~~FOUO~~) We found that the NRO OCAs and derivative classifiers' decisions are not consistently compliant with the original and derivative classification requirements of the Order and Directive. We assessed 134 NRO originally classified and derivatively classified documents, and found that 114 of the 134 documents (85 percent) had classification errors in 18 areas of discrepancy (See Appendix B).

(U//~~FOUO~~) The Order defines original classification as "an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure" and that, "an original classification authority is classifying the information." As part of our document sample, we assessed 62 NRO OCA SCGs, documents that require an OCA classification, and we found that all but one of the 62 guides had classification errors. Derivative classifiers, not the responsible OCA, classified 26 of the 62 NRO SCGs we reviewed. The majority of the NRO SCGs had not been classified in accordance with the Directive and over-classification was evident in four of the SCGs we assessed. For example, one OCA used the overall classification of "Top Secret (TS)" and the control markings of "Signals Intelligence (SI)" with no content portion marked as TS or SI. Overall, the most common SCG errors were

- using a Derivative Classification Block instead of OCA Classification Block (45 occurrences);
- indicating inaccurate duration of declassification exemption (44 occurrences); and
- providing an unauthorized classifier of Security Classification Guide (26 occurrences).

(U//~~FOUO~~) In reviewing derivative documents, 53 of the 72 derivative sampled documents (74 percent) had classification errors and several had multiple classification block errors. Additionally, over-classification was evident in 16 of the 72 (22 percent) documents we sampled. Documents with the overall classification of TS, and the control and dissemination markings of SI, Talent Keyhole (TK), and Not Releasable to Foreign Nationals (NOFORN) contained no SI, TK, or NOFORN portion marked information. In the case of derivative classifiers, the most common errors included

- no Classification Block on the document (30 occurrences);
- over-classification (16 occurrences); and
- inaccurate duration of declassification exemptions (12 occurrences).

(U//FOUO) We observed that our evaluation findings parallel the ISOO results from 2009. This raises questions as to the effort by NRO to correct and resolve the findings of the 2009 ISOO review.

(U//FOUO) NRO OCAs and Derivative Classifiers Lack Sufficient Knowledge of Their Classification Responsibilities

(U//FOUO) We found that the OCAs and derivative classifiers lack sufficient knowledge of classification principles and procedures necessary to perform their duties. Although the Directive provides guidance on original and derivative classification to include the roles, responsibilities, and classification principles and procedures, none of the OCAs we interviewed expressed that understanding. Those interviewed did not have a full understanding of all their roles and responsibilities or the classification principles and procedures outlined within the Directive. One OCA had almost no knowledge of his responsibilities. All the OCAs stated they relied heavily on their security staff to prepare documents for them to approve as the OCA.

(U//FOUO) Our interviews of derivative classifiers focused on those who were also directorate Chiefs of Security. The NRO Chiefs of Security are responsible for the classification management of their directorate. They also train the OCAs and manage the development of SCGs. None of the derivative classifiers had taken derivative classification training at the NRO. The derivative classifiers were not aware of the Act, Order, or the Directive requirement to take the derivative classification training once every two years. They were also not aware of the suspension and waivers process required if derivative classifiers do not participate in the required training. Four of the five Chiefs of Security we interviewed reported that they do not provide derivative training to their directorate. One Chief of Security stated that his office conducts an in-house ASR preparation and portion mark training. While they all train the OCAs using the OCA Training Briefing, mentioned previously, their methods of conducting the training varied greatly. Some reinforce the training with their OCA while others have the OCA read the briefing charts. As a result, many of the OCAs had limited knowledge and understanding of their roles and responsibilities. As the OS&CI classification managers for their directorates, Chiefs of Security should understand and administer the Order and the Directive requirements.

(U//FOUO) The NRO Self-Inspection Program does not Align with Federal Requirements

(U//FOUO) We found that the NRO has not established a classification self-inspection program in line with the requirements of the Order, Directive, or ISOO instructions. The Order and Directive require agencies that originate or handle classified information to establish and maintain "an ongoing self-inspection program." The self-inspection program "shall include the regular reviews of representative samples of the agency's original and derivative classification actions and shall authorize appropriate agency officials to correct misclassification actions." The Order and Directive require annual reporting to the Director of ISOO on the agency's self-inspection program. In addition, the National Archives and Records Administration/ISOO Self-Inspection Program instructions reiterate the requirements of the Order and provide the NRO with reporting instructions for a self-inspection program.

(U//~~FOUO~~) In the NRO OS&CI Policy Note 2013-04, the D/OS&CI announced compliance with Mandated Security Self-Assessment. The policy note references the NSM and the NSM provides details on the Integrated Security Assessment Program (ISAP) requirement for conducting annual self-assessments. However, the policy note is industry focused and does not include or address security self-assessments for government sites. Furthermore, the ISAP does not include regular review of representative samples of the NRO's original and derivative classification. While the NRO OS&CI provides the annual self-inspection reports to ISOO, we found that the OS&CI based the reports on information from the ISAPs at industry locations and the OS&CI Policy Branch's general knowledge of the NRO's overall classification management program. The 2012 report is not based on a self-inspection of the NRO's original and derivative classification activities, declassification, or management and oversight as required by ISOO.

(U//~~FOUO~~) We recognize that the NRO directorate classification management officers (CMOs) and PSOs review documents and briefings for accurate classification. From the classified documents we reviewed at NRO headquarters, 114 of 134 documents contained classification errors. Based on these results, the daily reviews and on-the-spot corrections made by the CMOs and PSOs do not offset the need for the NRO to establish a formal self-inspection program for government officers that meets the intent of the Order, Directive, and ISOO instructions. The NRO would benefit from a self-inspection program that is inclusive of all NRO activities generating classified information. The NRO would benefit further by incorporating written processes and procedures into the NSM to ensure regular reviews of representative samples of NROs original and derivative classification actions.

(U) RECOMMENDATIONS

(U//~~FOUO~~) The NRO has not fully adopted, followed, or effectively administered federally required classification policies, procedures, rules, and regulations. While the NRO complies with federal reporting and OCA designation requirements, the NRO classification management practices and procedures do not fully comply with applicable federal laws and guidance. Because of the lack of full compliance in multiple areas, the NRO is susceptible to the risk of persistent misclassification. With poor classification practices in place, the NRO cannot ensure that sources and methods are safeguarded and NRO resources and personnel are protected. In addition, improper classification practices and procedures may needlessly impede the NRO's sharing of information critical to mission partners meeting their mission requirements. The NRO would benefit from a comprehensive review of its OCA and derivative classification training policy and program to ensure that it meets the Order and Directive requirements. In addition, the NRO needs to establish proper classification management and oversight to increase the accuracy of classification at the NRO.

(U//~~FOUO~~) During the evaluation, NRO OCAs, directorate Chiefs of Security, and CMOs we interviewed commented that the IC could benefit significantly from an IC-wide standardized classification guide as a potential crosscutting issue. More immediately, to enable the NRO to improve its classification management and oversight, we are providing the following recommendations. Increased vigilance over NRO policies, procedures, rules, regulations, and management practices would reduce the NRO's vulnerability to persistent misclassification and the risks to National Security that may occur as a result.

(U) The Act requires the OIG to complete a follow up evaluation by 30 September 2016. We will include a follow-up on the recommendations outlined in this report as part of that review.

(U) Recommendation #1 for the D/OS&CI:

(U//FOUO) Establish NRO classification management policies that comply with the collective requirements of E.O. 13526 and 32 CFR Part 2001.

(U) Recommendation #2 for the D/OS&CI:

(U//FOUO) Establish proper classification oversight activities to include mandatory training and ensure that classification policies are clearly communicated, implemented, and followed.

(U//FOUO) Management Comments: The D/OS&CI non-concurred with the report as written but did not provide specific comments on the recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

(U) APPENDIX A: Agency Implementing Regulation Assessment Tool

(U) The purpose of the Agency Implementing Regulation Assessment Tool is to determine if the National Reconnaissance Office (NRO) has adopted the essential criteria for classification management. We reviewed the NRO's regulations against the assessment tool to ensure that the corresponding sections, as outlined in the Executive Order (E.O.) 13526 and 32 Code of Federal Regulations (CFR) Part 2001 have been adequately addressed in the NRO's implementing regulations.

(U) Original Classification Authority

- Does the agency have Original Classification Authority (OCA) and do they follow the standards for OCA designation and report delegations of OCA authority to the Director of Information Security Oversight Office (ISOO) annually?

(U) General Program Management Responsibilities

- Do the agency's regulations cite E.O. 13526 and 32 CFR Part 2001 for authorizing the agency's classified national security information program? Does the regulation make provisions for an annual review of special access programs to determine whether it continues to meet the requirements of E.O. 13526 and is this done by the agency head or principal deputy? Did the agency promulgate implementing regulations in the Federal Register to the extent that they affect the public?
- Do the regulations require the agency to establish a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency, and to provide guidance to personnel on proper classification as needed?
- Do the regulations require the senior agency official to direct and administer the program?
- Do the regulations provide for the suspension of OCA authority for OCAs who fail to complete annual OCA training and derivative classifiers who fail to complete training on derivative classification markings at least once every two years?
- Do the regulations require the rating of personnel on the performance of duties relating to the designation and management of classified information and does the agency ensure that the system used to rate personnel performance include the designating and managing of classified information as a critical element or item to be evaluated in the rating of OCAs, security professionals, or other personnel whose duties significantly involve the handling of classified information, including derivative classifiers?

(U) Original Classification

- Does the agency have classification guides and does the regulation cite the classification standards? Does the regulation contain procedures for the publication and updating of applicable security classification guides, which meet the minimum standards of E.O. 13526 and 32 CFR Part 2001?
- Does the agency provide procedures to safeguard information originated by non-OCAs that is believed to be classified? Do the regulations discuss the principle regarding the presumption against classification when significant doubt exists and the practical use of classified addenda?

- Are classification categories provided and are they the only categories used? Are duration principles provided and is emphasis placed on the use of dates based on specific events? Are the following items included as markings for classified documents or other media at the time of original classification? Classification levels, identity of the OCA, agency or office of origin, declassification instructions, reason for classification, portion markings, foreign government information markings, dissemination control and handling markings, date of origin of the document.
- Are regulations for classification markings for the electronic environment and prohibitions and limitations in accordance with the E.O. 13526 and 32 CFR Part 2001?
- Has the agency established procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified? Do these procedures mention that individuals are not subject to retribution for such actions, an impartial official or panel is given an opportunity to review, and individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (ISCAP)? Do the procedures mention timeframes for review or appeal?

(U) Derivative Classification

- Are the following topics discussed in the agency implementation regulation regarding derivative classification: Assurance of a sufficient personal identifier, source of derivative classification to include a listing of source materials, declassification instructions, marking prohibitions, agency-prescribed special markings, transmittal documents, foreign government information, and working papers?
- Are the following items included as markings for classified documents or other media at the time of derivative classification: Identification of the derivative classifier, source of derivative classification, declassification instructions, overall markings, portion marking, dissemination controls and handling markings, and date of origin of the documents?

(U) Declassification.

- Do the regulations address the declassification of classified information once it no longer meets the standards under E.O. 13526? For file series exemptions, does a process exist to determine that the information almost invariably falls within one of the exemption categories? Are procedures established to ensure the proper processing of requests to ISCAP for exemptions from automatic declassification?
- Do the regulations address the preparation, development, use, and review of declassification guides? Do the regulations address records originated by another agency as well as restricted data and formerly restricted data (RD/FRD)?
- Do the regulations include Mandatory Declassification Review procedures and are the pertinent procedures published in the Federal Register?

(U) Self-Inspections

- Do the regulations incorporate the essential elements for self-inspections and provide for regular reviews of representative samples of original and derivative classifications and corrections of misclassifications?

(U) Reporting and Definitions

- Do the regulations incorporate the essential elements for reporting to include statistical reporting, accounting for costs, fundamental classification guidance review, self-inspections, security violations, and information declassified without proper authority? Do agency definitions conform with the E.O. 13526 and 32 CFR Part 2001?

(U) Security Education and Training

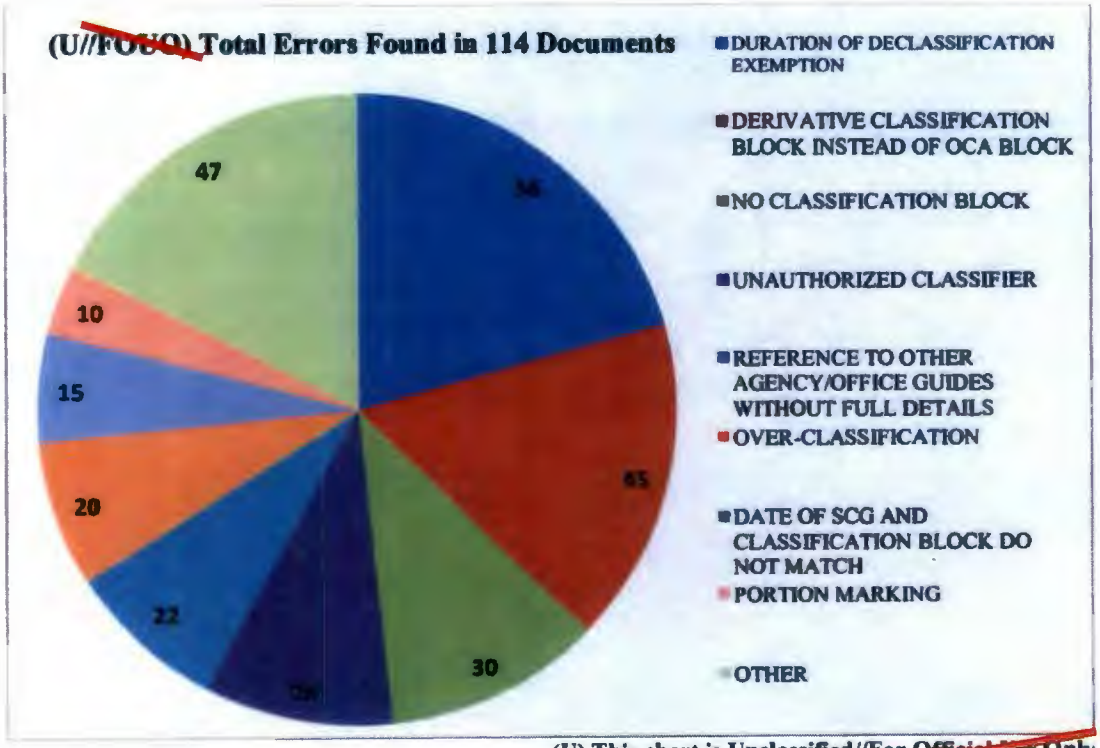
- Do the regulations incorporate the essential elements for establishing and maintaining a formal security education and training program to include initial training, annual refresher training, specialized training, and termination briefings for OCAs and derivative classifiers? How does the organization track and monitor an individual's completion of required training?
- Do the regulations provide for suspending OCA and derivative classification authority for those who fail to meet the training requirements and does it include the waiver process for delay in this training?

THIS PAGE INTENTIONALLY LEFT BLANK

(U) APPENDIX B: Classified Document Sample Methodology

(U//FOUO) To test and assess whether the National Reconnaissance Office (NRO) had adopted, followed, and administered the applicable classification policies, procedures, rules, and regulations, we selected two NRO directorates: the Mission Operations Directorate (MOD) and the Signals Intelligence Systems Acquisition Directorate (SIGINT) for our document sample. We chose MOD and SIGINT because they provide a broad range of classified documents. MOD operates the NRO ground stations and interacts regularly with each of the NRO Directorates and Offices (Ds and Os). SIGINT satellites operate out [redacted] NRO ground stations, and SIGINT has mission partners in the National Geospatial Agency and National Security Agency. Therefore, a sample focused on MOD and SIGINT classified documents would provide a fairly representative sample of the NRO derivative classification decisions.

(U//FOUO) We used the NRO Tracking Information and Enterprise Response (TIER) actions assigned to MOD and SIGINT from 1 July 2012 to 1 July 2013 as the source for our sample. From these TIER actions, the team determined that an initial sample of four percent of the combined MOD and SIGINT actions that produced documents would be sufficient for our evaluation. Overall, the team tested and assessed 134 classified documents to include NRO Security Classification Guides (SCGs). Should the evaluation have required further sampling, we would have selected an additional percentage of documents. In addition, the evaluation team used a National Archives and Records Administration (NARA)/Information Security Oversight Office (ISOO) worksheet, modified to the NRO, to facilitate classified document sampling and to determine the extent that NRO classified documents and materials were appropriately classified. We found 114 documents with classification errors consisting of 18 types of discrepancy (See chart below).



(U) This chart is Unclassified//For Official Use Only

(U) The discrepancy type "OTHER" consisted of the following:

- Improper declassification instructions
- Improper or no classification ID in classification block
- No signature on SCG
- Incorrect or no overall classification marking
- Under-classification
- SCG beyond required 5 year review
- Unknown multiple sources
- Improper derived from line in classification block
- Use of ORCON

(U) APPENDIX C: Management Comments

UNCLASSIFIED

NATIONAL RECONNAISSANCE OFFICE
14675 Lee Road
Chantilly, VA 20151-1715

7 Septembe 2013

MEMORANDUM OR IRECTOR, NATIONAL RECONNAISSANCE OFFICE
PRINCIPAL DEPUTY DIRECTOR, NATIONAL
RECONNAISSANCE OFFICE
DEPUTY DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
NSPECTOR GENERAL

UBJECT: Response t the Off ce of Inspector General Draft Report:
Eva. ation of the Nat ona Reconnaissance Office
lassificatior Management under Public Law 1. 258, the
Reducing Ove -c assification Act (Project Number 2013 00
S , 23 September 2013

REFERENCE: Evaluation of the National Reconnaissance ffice
Classif.cation Management under Public Law .11-258, the
Reduc ng Over-classification Act
(Project Number 2013-001 S), 23 September 2013

The ffice of Security and Counterintelligence (OS&CI appreciates the opportunity to comment on the subject report, but nat we were not g.ven adequate ime o an appropriate response. The evaluation was conducted over a four month period; wever, OS&CI was g ven less than three days for review and comment. we were not provided adequate documentation supporting the numerous onal zed, exaggerated nd m sleading sta ements contained i he report or specific references for some requirements. OS&CI does believe the ev dence contained in the report provides a reasonable ba the Inspect General findings and conclusions. The report es not a rately ref ect the National Reconnaissance Off ce's (NRO lass fi ation Management program and th s office has no a ternat ve t n-concur wi h the repor as written.

We do agree there s room for improvement in various aspects f t NRO' lassif cat.on management act vities, but we strong y disagree w.th each of the primary conclusions documented in the report:

a. NRO classificat.on policies do not align with federal assi. tion requirements, and the NRO is not adhering o ts assi. tion po.icies;

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Response to the Office of Inspector General Draft Report: Evaluation of the National Reconnaissance Office Classification Management under Public Law 111-258, the Reducing Over-classification Act Project Number 2013-001 [illegible], 23 September 2013

b. NRO classification training is not compliant with Federal laws;

c. NRO Original Classification Authorities (OCAs) and derivative classifiers are not classifying in accordance with the Federal law and guidance;

d. NRO OCAs and derivative classifiers do not have sufficient knowledge of their classification responsibilities;

e. NRO does not have a classification management self-inspection program in accordance with federal laws and guidance.

These conclusions mischaracterize the discussion of the topics in the body of the report and the discussions themselves contain myriad errors. We agree there are cases where the NRO is not fully compliant with every aspect of the regulatory direction, but the statements and inference that the NRO does not comply with federal law and guidance is not accurate. If afforded the opportunity, OS&CI will provide details regarding factual and interpretive errors.

Please direct any questions you may have regarding this evaluation to (b)(3) 10 U.S.C. 424, (b) Chief, OS&CI Policy Branch, at (b)(3) 10 U.S.C. 424, (b)(secure).

(b)(3) 10 U.S.C. 424, (b)(

[redacted]
Director, Office of Security and Counterintelligence

UNCLASSIFIED

(U) APPENDIX D: Major Contributors to the Report

(U) (b)(3) 10 U.S.C. 424, (b)(	NRO/OIG Deputy Assistant Inspector General for Acquisition Audits
(U) (b)(3) 10 U.S.C. 424, (b)	NRO/OIG Evaluation Lead, Auditor
(U) (b)(3) 10 U.S.C. 424, (b)(6)	NRO/OIG Inspector
(U) (b)(3) 10 U.S.C. 424, (	NRO/OIG Inspector
(U) (b)(3) 10 U.S.C. 424, (b)(	NRO/OIG Independent Referencer
(U) (b)(3) 10 U.S.C. 424, (b)(6)	NRO/OIG Writing Facilitator