Enclosure 2

AGENCY ANNUAL SELF-INSPECTION PROGRAM DATA: FY 2013

(Submissions must be unclassified.)

PART A: Identifying Information

1. Enter the agency name.	1.Central Intelligence Agency

2. Enter the date of this report.	**2.November 22, 2013**

3. Enter the name, title, address, phone, fax, and e-mail address of the **Senior Agency Official** (SAO) (as defined in E.O. 13526, section 5.4(d)) responsible for this report.	3. Joseph W. Lambert Director Information Management Services (IMS) CIA, Washington, DC 20505	(b)(3)
4. Enter the name, title, phone, fax, and e-mail address of the **individual or office** responsible for conducting self-inspections and reporting findings.	4. Harry P. Cooper Chief, Classification Management & Collaboration Group (CMCG) CIA, Washington, DC 20505	(b)(3)
5. Enter the name, title, phone, fax, and e-mail address for the **point-of-contact** responsible for answering questions regarding this report.	5. Harry P. Cooper Chief, Classification Management & Collaboration Group CIA, Washington, DC 20505	(b)(3)

PART B: Classified National Security Information (CNSI) Program Profile Information

6. Has your agency been designated/delegated as an original classification authority (OCA)?	6.	O YES O
7. Does your agency perform original classification activity?	7.	O YES O
8. Does your agency perform derivative classification activity?	8.	O YES O
9. Does your agency have an approved declassification guide and declassify CNSI?	9.	O YES O

PART C: Description of the Program

A description of the agency's self-inspection program to include activities assessed, program areas covered, and methodology utilized. The description must demonstrate how the self-inspection program provides the SAO with information necessary to assess the effectiveness of the CNSI program within individual agency activities and the agency as a whole.

Responsibility

10. How is the SAO involved in the self-inspection program? (Describe his or her involvement with the self-inspection program.)

The Senior Agency Official delegates responsibility to CMCG for self-inspection program, approves annual self-inspection plan, receives briefing on results and recommendations, and approves follow-on actions.

11. How is the self-inspection program structured to provide the SAO with information necessary to assess the agency's CNSI program in order to fulfill his or her responsibilities under section 5.4(d) of E.O. 13526?

The self inspection program is designed to cover compliance with all of 5.4(d) areas of responsibility, to identify best practices and areas for improvement so that training and education can be improved, errors and problems can be addressed, and any needed policy changes can be implemented.

12. Whom has the SAO designated to assist in directing and administering the self-inspection program? Who conducts the self-inspections?
    (If the SAO conducts the self-inspections, which may be the case in smaller agencies, indicate this.)

The Chief/IMS/CMCG, an SES-level officer, is designated to assist in directing and administering the self inspection program. Three classification specialists in CMCG conduct the self-inspections. In addition two representatives from the Agency Publications Review Board observed and conducted in-person interviews in tandem with CMCG staff.

Approach

13. What means and methods are employed in conducting self-inspections? *(For example: interviews, surveys, data calls, checklists, analysis, etc.)*

An audit plan was prepared to identify components that would provide a representative sample of Agency work. An interview methodology was prepared, and document review checklists were developed to cover all necessary aspects of classification review. There was a data call followed by CMCG in-person interviews and a review of documents classified by employees in each of those components. In addition, we collaborated on data collection with the component Information Management Officer and interviewed the component Security Officer. Results were analyzed, and findings and recommendations prepared.

INFORMATION SECURITY OVERSIGHT OFFICE

AUTHORIZED FOR LOCAL REPRODUCTION
32 CFR 2001 E.O. 13526

14. If your agency performs different types of inspections (e.g., component self-inspections, command inspections, compliance reviews, etc.), describe each of them and explain how they are used. If not, indicate NA.

There was an Inspector General Evaluation, Component Self-Inspections, Classification Count and Analysis, and Compliance Review of Mandatory Original and Derivative Classification Training, as required by EO 13526. All of these inspections were considered in the overall evaluation as reflected in this report

15. Do your agency's self-inspections evaluate adherence to the principles and requirements of E.O. 13526 and its implementing directive and the effectiveness of agency programs covering the following areas? *(Select all that apply.)*

☐ √ Original classification ☐ √ Security violations ☐ √ Safeguarding ☐ √ Management and oversight
☐ √ Derivative classification ☐ √ Declassification ☐ √ Security education and training

16. Do your self-inspections include a review of relevant security directives and instructions?	16. O YES O
17. Do your self-inspections include interviews with producers (where applicable) and users of classified information?	17. O YES O

Approach: Representative Sample
(If your agency does not classify information, indicate NA.)

18. Do your self-inspections include reviews of representative samples of original and derivative classification actions to evaluate the appropriateness of classification and the proper application of document markings?	18. O YES O O
19. Do these reviews encompass all agency activities that generate classified information? ***Yes – over time.**	19. O YES ⊙ O

20. Describe below how the agency identifies activities and offices whose documents are to be included in the sample of classification actions. (Indicate if NA.)

Each year CMCG determines an appropriate set of components and activities to sample with the goal of reviewing, over time, all agency components and activities. This year, CMCG partnered with Information Management Officers in each of our major functional areas to identify representative components to enable CMCG to review C, S, & TS material from a wide range of CIA activities. CMCG also examined Office of Security guidelines and procedures, and Agency representatives accompanied the ISOO team when it examined the 25 year declassification program.

21. Do the reviews include a sampling of various types of classified information in document and electronic formats?	21. O YES O O

22. How do you ensure that the materials reviewed provide a representative sample of the agency's classified information? (Indicate if NA.)

CMCG asked the Information Management Officer in each selected component to identify a sample office and a random group of component personnel for interviews and document review. Each of the interviewees was asked to provide a random sample of paper, email, and other electronic documents that they produced on four specific days for CMCG representatives to examine.

23. How do you determine that the sample is proportionally sufficient to enable a credible assessment of your agency's classified product? (Indicate if NA.)

CMCG works with the Information Management Officers to identify a variety of Agency functions ranging from administrative to mission critical and then target Offices and officers in each of these specific areas. Based upon the results of prior annual audits, and questions received by our Classification Help Desk, we determine if there are areas that need increased attention in subsequent audits.

24. Who conducts the review of the classified product? (Indicate if NA.)

Chief/CMCG forms inspection teams of 2-3 persons who are classification experts.

25. Are the personnel who conduct the reviews knowledgeable of the classification and marking requirements of E.O. 13526 and its implementing directive?	25. O YES O O
26. Do they have access to pertinent security classification guides? (Indicate if NA.)	26. O YES O O
27. Have appropriate personnel been designated to correct misclassification actions? (Indicate if NA.) If so, identify below.	27. O YES O O

The Chief and all the members of CMCG.

Frequency

28. How frequently are self-inspections conducted?

Annually over the course of approximately four months.

29. Describe the factors that were considered in establishing this time period?

The four-month period gives CMCG sufficient time to plan the audit, brief component management and do a data call, complete the interviews and analysis, brief management on the results, integrate the results into revised training, and make regulatory or policy changes, as necessary.

Coverage
30. How do you determine what offices, activities, divisions, etc., are covered by your self-inspection program? What agency activities are assessed?
As noted in the response to question 20, CMCG's goal, over time, is to audit all agency components and activities. Thus, far, our efforts have been directed toward establishing a benchmark to guide future audits. This year, in support of our goal, CMCG audited one component from each of the Agency's major functional areas. The sample included documents and perspectives that varied from administrative and support to mission-critical matters. As we identify additional Agency issues, we will focus on those components and activities that are most likely to confront those issues.
31. How is the self-inspection program structured to assess individual agency activities and the agency as a whole?
As CMCG plans the audit of each specific component, we review the type of functions performed in that component and the type of documents received and produced. We also take into account any classification questions that have been asked by personnel in that component. This guides the development of our checklists, data calls, and interviews. Our analysis of each audit in terms of deficiencies and best practices helps us to identify specific areas we should focus on in training and in subsequent audits.

Special Access Programs (SAP) (If your agency does not have the authority to create SAPs, indicate NA.)			
32. If your agency has any special access programs, are self-inspections of the SAP programs conducted annually?	32.	O YES O	O
33. Do the self-inspections confirm that the agency head or principal deputy has reviewed each special access program annually to determine if it continues to meet the requirements of E.O. 13526?	33.	O YES O	O
34. Do the self-inspections determine if officers and employees are aware of the prohibitions and sanctions for creating or continuing a special access program contrary to the requirements of E.O. 13526?	34.	O YES O	O

Reporting
35. What is the format for documenting self-inspections in your agency?
CMCG documentation includes document analysis worksheets, interview report forms, data aggregation spreadsheets, audit analysis with findings and recommendations, the ISOO "Agency Annual Self-Inspection Program Data" form report, D/IMS briefing, and memoranda on self-inspection audit findings for the CIA/CIO and Executive Director.
36. Who receives the reports?
The Senior Agency Official (D/IMS), the Chief Information Officer, the Executive Director, and the Information Security Oversight Office, as well as feedback to the audited components Information Management Officers.
37. Who compiles/analyzes the reports?
The CMCG audit team.
38. How are the findings analyzed to determine if there are problems of a systemic nature?
CMCG scores the data in the document analysis worksheets and identifies trends from the interview report forms to discover patterns both within specific audited components and across the various components we have audited. We also analyze the classification questions we are asked over the course of the year to spot areas where additional training is needed.
39. How and when are the results of the self-inspections reported to the Senior Agency Official (SAO)?
CMCG briefs the SAO when the data analysis is completed and when we have a set of draft findings and recommendations. The ISOO "Agency Annual Self-Inspection Program Data" form report is completed and sent to the SAO before being released. The SAO approves the findings and recommendations, which are then implemented.
40. How is it determined if corrective actions are required?
CMCG seeks to correct all errors and inadequacies in areas where action is needed. Where these seem to be unique, they may be used as examples in training courses or referenced in the Agency's Classification Website's "Frequently Asked Questions." Where errors occur more frequently or there seems to be a pattern, CMCG will make them a focus area in its training, issue an employee notice, and examine if Agency guidance and regulations need further clarification.
41. Who takes the corrective actions?
CMCG.
42. How are the findings from your agency's self-inspection program distilled for the annual report to the Director of ISOO?
They are summarized in Parts D, E, H and I of this document.

43. Has the SAO formally endorsed this self-inspection report?	43. O YES O

PART D: A summary of the findings of your agency's self-inspection program

The **summary** should present specific, concise findings from your self-inspection program for each of the required program areas below. It is not a description of the requirements of the agency's CNSI program. Rather, the summary outlines the essential self-inspection findings based on the compilation and/or distillation of the information contained in the agency's internal self-inspection reports, checklists, etc. In large agencies where findings are drawn from multiple agency offices and activities, the findings that are reported here may be the most significant or most frequently occurring.

44. Original Classification:

The self inspection determined that the number of original classifiers has been kept at the lowest possible level, that annual original classifier training has been given, and that original classifiers understand their original classification authority (OCA) is only to be exercised in the rare case when the Agency classification guide does not provide guidance, and there appears to be a need for the information to be classified. In the last five years, the only CIA officer to exercise OCA was C/CMCG. Typically there have been less than 5 OCA decisions each year as reported on the SF311. This year there were no OCA decisions.

45. Derivative Classification: The review found that 17.4% of the sample was over-classified. More specifically, 1.4 % of the TOP SECRET docs should have been SECRET and 0.6% CONFDENTIAL; 0.8% of the S docs should have been C, and 7.7% should have been U//AIUO or U//FOUO; 5.8% of the C documents should have been AIUO or FOUO; and 1.1% of the S or C docs should have been U. In addition, 2.8% of the sample as under-classified – 1.1% were AIUO or FOUO but should have been C or S and 1.7 % marked C should have been S.
Apart from discrepancies involving classification levels, we identified four additional areas for improvement: 62% of the sample was incorrectly portion marked, 8% inappropriately used the ORCON/NOFORN caveat, and 9% did not list a personal identifier. In addition, we found a failure to list source documents when multiple sources were used.

46. Declassification:

The review of the automatic declassification program looked at both process and substantive issues, and encountered no examples of missed equities, improper exemptions, or inappropriate referrals.

47. Safeguarding:

The review determined that the Agency's policies and accompanying procedures related to safeguarding as outlined in Executive Order 13526 are in alignment with the EO, and with existing Federal statutes and other pertinent Executive Branch issuances. Specifically, while adhering to EO 13526, the Agency adheres to the governing requirements outlined in ICD 503 for information technology, ICD 704 for personnel security, ICD 705 for physical and technical security, and EO 12829 and the NISPOM for industrial security, all of which build upon the requirements listed in EO 13526.

48. Security Violations:

The review determined that the Agency's policies and accompanying procedures related to the reporting and investigation of security violations are in alignment with Executive Order 13526 and with procedures established by the Department of Justice and the Federal Bureau of Investigation. The review also found that the Agency recently added additional resources to increase its ability to investigate leaks to the media. Additionally, the Agency has a strong insider threat program that incorporates the reporting, investigation, and adjudication of all security violations.

49. Security Education and Training:

The review determined that the Agency's policies and accompanying procedures provide the appropriate level of security training and education commensurate with the EO, and other applicable Executive Branch issuances. Specifically, the review found that the Agency's security training and education program extends for the lifecycle of a cleared individual's association with the Agency, and covers initial education and training indoctrination, annual refresher training and mandatory training, exit debriefing, and pre-publication reviews. Training received is recorded in personnel records.

50. Management and Oversight:
CMCG is a year-round resource for classification assistance to mission partners. This includes courses intended for professional training of classification specialists, training for new personnel in the fundamentals of classification and as well as more specialized training for various components, including training on compartmentation principles. It continues with regular original and derivative classification refresher training, and a classification help desk that provides real-time assistance to Agency personnel. These functions provide insight into the types of problems that are being encountered and factors into the content of the training we provide, the employee publications we issue, and the regulatory policy adjustments we suggest. Issues are brought by CMCG to the attention of the SAO, who consults with the CIO and Executive Director and others as appropriate.

Approved for Release: 2022/01/27 C06896970

Enclosure 2

PART E: An assessment of the findings of your agency's self-inspection program

The assessment discerns what the findings mean. The assessment is an evaluation of the state of each element of your agency's CNSI program based on an analysis of the specific, concise findings of the self-inspection program. It reports what you have determined the findings indicate about the state of your agency's CNSI program.

The assessment should inform the SAO and other decision makers of significant issues that impact the CNSI program. It should be used to determine how security programs can be improved, whether the agency regulation or other policies and procedures must be updated, and if necessary resources are committed to the effective implementation of the CNSI program. The assessment should report trends that were identified during the reporting period across the agency or in particular activities, as well as trends detected by making comparisons with earlier reporting periods. It can be used to support assertions about the successes and strengths of an agency's program.

51. Original Classification:

The self-inspection found that our original classification system is working well, and that no additional changes or improvements are needed to our regulations, policies or procedures. No additional resources are needed at this time.

52. Derivative Classification: A 20% over- and –under-classification rate is not acceptable, and we need to further enhance our classification training. It was noted, however, that the vast majority of the documents classified each year are internal Agency email. Appropriately 81% of the sample was internal email where the misclassified documents would not affect either information sharing or public access. Similarly the lack of portion marking was generally on internal email. CMCG needs to focus more of its training on the requirement to portion mark documents, including classified email. New guidance on the use of ORCON/NOFORN has already been issued but additional training is needed to reduce the misuse of this caveat from the current 8%. Finally, it was found that the lack of a personal identifier generally does not mean a lack of traceability to the classifier, but the Agency needs to work on procedures to fix the issue.

53. Declassification:

The ISOO assessment this year found that CIA has followed the recommendations of previous ISOO declassification assessments and made significant improvements in its declassification program. The Agency automatic declassification program received a green rating, the highest, with a score of 100 out of 100 points.

54. Safeguarding:

The Agency's safeguarding measures are meeting mission needs. The Agency continually evaluates and tests its existing safeguarding measures. With the recent national trends in media leaks and focus on insider threat, the Agency is deploying improvements made to its information technology systems, increasing deployment of a technical security system, and updating both facility access and compartmentation policy and procedures.

55. Security Violations:

The self-inspection determined that Agency personnel appropriately report security violations. With the recent increase of leaks of classified information to the media, the Agency decided to add resources to its investigation capabilities. These resources are focusing special attention on media leaks. Additionally, the Agency is currently updating its policy and procedures related to protecting classified information, which will provide Agency personnel with greater detailed guidance.

56. Security Education and Training:

The Agency's security education and training program meets the needs of the Agency's mission. To build upon the Agency's existing base of security training and education, and as a result of recent leaks to the media, the Agency has initiated two programs designed to increase security awareness. One program is addressing the obligation that all Agency personnel have in protecting classified information from unauthorized disclosure. The other program is designed to assist Agency personnel in preventing security violations. The Agency also has added training that addresses the use of the ORCON designator.

57. Management and Oversight:

The self-inspection revealed a need for greater personnel outreach and CMCG brand awareness so that Agency derivative classifiers are better able to avail themselves of classification assistance. There is a need for CMCG to partner with Information Management Officers and other stakeholders to direct customers to the classification website email and telephone resources. CMCG needs to continue to issue more specific guidance to address issues identified in this self-inspection.

INFORMATION SECURITY OVERSIGHT OFFICE

AUTHORIZED FOR LOCAL REPRODUCTION
32 CFR 2001 E.O. 13526

Approved for Release: 2022/01/27 C06896970

PART F: Focus Questions
Answer the questions below. If the response identifies a deficiency, it should be explained in Part D, Summary of Findings, under the relevant program area, and should be addressed in Part H, Corrective Actions.

Training for Original Classification Authorities

Original classification authorities are required to receive training in proper classification and declassification each calendar year. (Section 1.3(d) of E.O. 13526 and § 2001.70(c) of 32 C.F.R. Part 2001) (Indicate NA if your agency does not have original classification authority.)

58. Does agency policy require training for original classifiers?	58. ⦿YES ○　　○
59. Has the agency validated that this training has been received?	59. ⦿YES ○　　○
60. What percentage of the original classification authorities at your agency has received this training?	60. 80%
	○ Actual ○
61. Have any waivers to this requirement been granted?	61. ○　　○No ○

Persons who Apply Derivative Classification Markings

Persons who apply derivative classification markings are required to receive training in the proper application of the derivative classification principles of E.O. 13526, prior to derivatively classifying information and at least once every two years thereafter. (Section 2.1(d) of E.O. 13526 and § 2001.70(d) of 32 C.F.R. Part 2001) (Indicate NA if your agency does not have any personnel who derivatively classify information.)

62. Does agency policy require training for derivative classifiers?	62. ⦿YES ○　　○
63. Has the agency validated that this training has been received?	63. ⦿YES ○　　○
64. What percentage of the derivative classifiers at your agency has received this training?	64. 67%
	○ Estimated
65. Have any waivers to this requirement been granted?	65. ⦿No ○　　○

Initial Training

All cleared agency personnel are required to receive initial training on basic security policies, principles, practices, and criminal, civil, and administrative penalties. (§ 2001.70(b) of 32 C.F.R. Part 2001)

66. Does agency policy require initial training? For all Agency employees, not industrial contractors	66. ⦿YES ○
67. Has the agency validated that this training has been received?	67. ⦿YES ○
68. What percentage of cleared personnel at your agency has received this training?	68. 100%
	○ Actual ○

Annual Refresher Training

Agencies are required to provide annual refresher training to all employees who create, process, or handle classified information. (§ 2001.70(f) of 32 C.F.R. Part 2001)

69. Does agency policy require annual refresher training?	69. ○ YES⦿
70. Has the agency validated that this training has been received?	70. ○ YES⦿
71. What percentage of the cleared employees at your agency has received this training?	71. 67%
	○ Estimated

Identification of Derivative Classifiers on Derivatively Classified Documents

Derivative classifiers must be identified by name and position, or by personal identifier on each classified document. (Section 2.1(b)(1) of E.O. 13526 and § 2001.22(b) of 32 C.F.R. Part 2001) (Indicate NA if your agency does not derivatively classify information.)

72. Does your agency's review of classification actions evaluate if this requirement is being met?	72. ⦿YES ○　　○
73. What percentage of the documents sampled meet this requirement?	73. 91%
74. What was the number of documents reviewed for this requirement?	74. 362

List of Sources on Documents Derivatively Classified from Multiple Sources

A list of sources must be included on or attached to each derivatively classified document that is classified based on more than one source document or classification guide. (§ 2001.22c(1)(ii) of 32 C.F.R. Part 2001)

75. Does your agency's review of classification actions evaluate if this requirement is being met?	75. ⦿YES ○　　○
76. What percentage of the documents sampled meet this requirement?	76. 0%
77. What was the number of documents reviewed for this requirement?	77. 362

INFORMATION SECURITY OVERSIGHT OFFICE

AUTHORIZED FOR LOCAL REPRODUCTION
32 CFR 2001 E.O. 13526

Performance Evaluations	
The performance contract or other rating system of original classification authorities, security managers, and other personnel whose duties significantly involve the creation or handling of classified information must include a critical element to be evaluated relating to designation and management of classified information. (Section 5.4(d)(7) of E.O. 13526)	
78. Does agency policy require this critical element in the performance evaluations of personnel in the categories required by E.O. 13526?	78. ⊙YES ○
79. Has the agency validated that this critical element is included in the performance evaluations of personnel in the categories required by E.O. 13526?	79. ⊙YES ○
80. What percentage of such personnel at your agency has this element in their performance evaluations? **Being implemented Agency-wide in the 2013-2014 performance cycle**	80. **100%** ○ Actual ○

OCA Delegations	
OCA delegations shall be reported or made available by name or position to the Director of the Information Security Oversight Office. (Section 1.3(c)(5) of E.O. 13526). This can be accomplished by an initial submission followed by updates on a frequency determined by the SAO, but at least annually. (§2001.11(c) and §2001.90(a) of 32 C.F.R. Part 2001)	
81. Have there been any changes in the delegations, by name and position, of original classification authority in your agency since delegations were reported to ISOO in 2010.	81. ⊙YES ○ ○
82. Have all delegations been limited to the minimum required based on a demonstrable and continuing need to exercise this authority?	82. ⊙YES ○ ○
83. If changes have been made, have they been reported, by name or position, to ISOO?	83. ○NO ○ ○

Classification Challenges	
An agency head or SAO shall establish procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. (Section 1.8(b) of E.O. 13526) Classification challenges must be covered in the training for original classification authorities and persons who apply derivative classification markings. (§2001.71(c) and (§2001.71(d) of 32 C.F.R. Part 2001)	
84. Has your agency established procedures under which the classification of information can be challenged in accordance with section 1.8(b) of E.O. 13526 and §2001.14 of 32 C.F.R. Part 2001?	84. ⊙YES ○ ○
85. Does your agency's training for OCAs and for personnel who apply derivative classification markings cover classification challenges?	85. ⊙YES ○ ○
86. Does your agency's training for all other cleared personnel cover classification challenges?	86. ○NA* ○

PART G: Findings of the Annual Review of Agency's Original and Derivative Classification Actions

In this section provide specific information with regard to the findings of the annual review of the agency's original and derivative classification actions to include the volume of classified materials reviewed and the number and type of discrepancies identified.

87. Indicate the volume of classified materials reviewed during the annual review of agency's original and derivative classification actions. (If your agency does not classify information, indicate NA.)	87. 362 + OCA decisions

88. Indicate the number of discrepancies found during the annual review of classification actions for each category below. For additional information on marking, consult the ISOO marking guide.

88 (a) Over-classification: Information does not meet the standards for classification.	88 (a) 53
88 (b) Overgraded/Undergraded: Information classified at a higher/lower level than appropriate.	88 (b) 73
88 (c) Declassification: Improper or incomplete declassification instructions or no declassification instructions.	88 (c) 65
88 (d) Duration: a shorter duration of classification would be appropriate.	88 (d) 53
88(e) Unauthorized classifier: A classification action was taken by someone not authorized to do so.	88(e) 0
88 (f) "Classified By" line: A document does not identify the OCA or derivative classifier by name and position or by personal identifier.	88 (f) 33
88 (g) "Reason" line: an originally classified document does not cite a reason from section 1.4 of E.O. 13526.	88 (g) 0
88 (h) "Derived From" line: A document fails to cite, or cites improperly, the classification source. The line should include type of document, date of document, subject, and office/agency of origin.	88 (h) 81
88 (i) Multiple sources: A document cites "Multiple Sources" as the basis for classification, but a list of these sources is not included on or attached to the document.	88 (i) 3
88(j) Marking: A document lacks overall classification markings or has improper overall classification markings.	88 (j) 80
88 (k) Portion Marking: The document lacks some or all of the required portion markings.	88 (k) 226
88(l) Instructions from a classification guide are not properly applied.	88 (l) 73
88 (m) Other: Inappropriate application of ORCON/NOFORN caveats.	88 (m) 30

Enclosure 2

PART H: Corrective Actions

89. Describe actions that have been taken or are planned to correct identified program deficiencies, marking discrepancies, or misclassification actions, and to deter their reoccurrence.

CMCG will further enhance its classification training and will focus more attention on the need to portion mark documents, including classified email. Having issued new guidance on the use of the ORCON/NOFORN caveat, CMCG will provide focused training to reduce the misuse of this caveat from the rate of 8%, as identified in this self-assessment. CMCG will add training on the need to list all source materials when using multiple sources for classification. It also will work on procedures to address the lack of a personal identifier which was found in one stream of reporting. In addition, CMCG will provide more information and conduct greater personnel outreach to make Agency derivative classifiers more aware of available classification assistance, and will partner with IMOs and other stakeholders to direct customers to the classification website email and telephone resources.

Four additional FTEs have been added to the security element responsible for the investigation of leaks of classified information to the media. The Agency also is revising its policy and updating its procedures governing protection of classified information, and has recently initiated a new security awareness and education activity targeting secrecy agreements. The Agency's security element is revising its classification guide in collaboration with CMCG.

Finally, CMCG will issue more specific guidance to address the various issues identified in this self-inspection.

PART I: Best Practices

Best practices are those actions or activities that make your self-inspection program and/or CNSI program more effective or efficient. They set your program apart through innovation or by exceeding the minimum program requirements. These are practices that may be utilized or emulated by other agencies.

90. Describe best practices that were identified during the self-inspection.

1. Agency use of automation with respect to declassification was recognized by ISOO as a best practice because it allows reviewers to enter important metadata and reference information that aids future reviewers in making determinations on records previously exempted, referred, or redacted. The practice of including box summary sheets in each box of reviewed records also was identified as a best practice because it will aid archival processing when the records are accessioned to the National Archives.

2. Embedding staff officers in the various components to provide instant classification assistance, coupled with immediate web and telephonic classification help from CMCG, to provide additional or more specialized assistance, enables classifiers to receive guidance quickly enough so that there is not a tradeoff between timely completion of priority assignments and finding the correct classification in difficult cases.

3. The Agency's management and implementation of its insider threat program.

4. A new Agency's process for ensuring that all stakeholders review and comment on regulatory issuances to ensure the appropriateness of both the policy and the classification of information.

5. The Agency's rules and practices with respect to the exercise of Original Classification Authority.

INFORMATION SECURITY OVERSIGHT OFFICE

AUTHORIZED FOR LOCAL REPRODUCTION
32 CFR 2001   E.O. 13526

PART J: Explanatory Comments

Use this space to elaborate on any section of this form. If more space is needed, provide as an attachment to this form. Provide explanations for any significant changes in trends/numbers from the previous year's report.

Re Q 15 section on Declassification: FOIA declassification decisions are subject to administrative appeal and Court review; MDR decisions are subject to appeal and ISCAP review. The self-inspection concluded that these determinations inform future declassification decisions.

Agency personnel were involved with ISOO in its review of the Agency 25 year declassification program, during which ISOO independently found to be in full compliance with EO 13526 requirements and that declassification decisions supported by the ISCAP-approved declassification guide.

Re Qs 64 and 71 on derivative and refresher training: In FY13 we had some technical issues with our web-based derivative classification training that prevented about a third of our personnel from taking this training. However the network and web based training are now fully functioning and we anticipate that our derivative classification training will meet expectations in FY 14.

Re Qs 85 and 86 classification challenges: All cleared Agency personnel are derivative classifiers and covered in the response to Q 85; there are no other cleared personnel who would require training to cover classification challenges.

~~For ISOO Use Only~~

ISOO Analyst:
Date QC

_____

_____

_____

INFORMATION SECURITY OVERSIGHT OFFICE

AUTHORIZED FOR LOCAL REPRODUCTION
32 CFR 2001 E.O. 13526