Central Intelligence Agency

Washington, D.C. 20505

22 February 2022

Martin Peck
MuckRock News
DEPT MR 21361
411A Highland Avenue
Somerville, MA 02144
21361-80067878@requests.muckrock.com

Reference: F-2015-02655

Dear Requester:

This letter is a final response to your 19 September 2015 Freedom of Information Act (FOIA) request for **records associated with self-inspection of classified materials handling pursuant to Executive Order (EO) 13526 and E.O. 13587 performed by the Agency for the last ten (10) years. Please include results of inspection and especially guidance resulting from analysis of reviewed activities and materials. Inspection records associated with effectiveness or original classification, effectiveness of derivative classification, safeguarding material, security training, security violations, and auditing/oversight are specifically requested**. We processed your request in accordance with the FOIA (5 U.S.C. § 552, as amended, and the CIA Information Act, 50 U.S.C. § 3141, as amended).

We completed a thorough search for records responsive to your request and located one enclosed document which we determined can be released in its entirety. We also determined that the other enclosed six documents be released in segregable form with deletions made on the basis of FOIA exemptions (b)(3) and (b)(6). Additional material was located and must be denied in its entirety on the basis of FOIA exemptions (b)(1), (b)(3), (b)(5), and (b)(6).

Please note that exemption (b)(3) pertains to information exempt from disclosure by statute. The relevant statutes are Section 6 of the Central Intelligence Agency Act of 1949, as amended, and Section 102A(i)(l) of the National Security Act of 1947, as amended.

As the CIA Information and Privacy Coordinator, I am the CIA official responsible for this determination. You have the right to appeal this response to the Agency Release Panel, in my care, within 90 days from the date of this letter. Please explain the basis for your appeal.

In the course of processing your request, we also located material originating with another agency. We have referred that material to the originating agency for review and direct response to you.

Please be advised that you may also seek dispute-resolution services from the CIA FOIA Public Liaison or from the Office of Government Information Services (OGIS) of the National Archives

and Records Administration. OGIS offers mediation services to help resolve disputes between FOIA requesters and Federal agencies.

To contact **CIA** directly with questions or to appeal the CIA's response to the Agency Release Panel:	To contact the **Office of Government Information Services (OGIS)** for mediation or with questions:
Information and Privacy Coordinator Central Intelligence Agency Washington, DC 20505 TEL: (703) 613-1287 FAX: (703) 613-3007	Office of Government Information Services National Archives and Records Administration 8601 Adelphi Road – OGIS College Park, MD 20740-6001 TEL: (202) 741-5770 FAX: (202) 741-5769 / ogis@nara.gov

Sincerely,

Andra Barker
Acting Information and Privacy Coordinator

Enclosures

C06896739

Approved for Release: 2022/01/27 C06896739

19 December 2011

Mr. John P. Fitzpatrick, Director
Information Security Oversight Office
National Archives and Records Administration
Washington, D.C. 20408-0001

Dear Mr. Fitzpatrick:

(U//FOUO) I have enclosed the Central Intelligence Agency's (CIA) 2011 report on its self-inspection as required by Executive Order 13526 § 5.4 (d)(4). This is in response to a letter signed by Mr. William Cira on April 05, 2011 that was never received by CIA and only brought to our attention several days ago. We have nevertheless completed the report on our annual self-inspection.

(U//FOUO) The CIA's report this year is classified, because we chose in 2011 to inspect an operational element of the CIA that requires protection. We have adopted an inspection process that will look very closely at a different CIA business area each year. We have chosen this approach as I believe it will give us a much better opportunity to focus our corrective actions on specific weaknesses. Otherwise, a very broad inspection could only be met with some very generalized policy refinement or training.

(U) Should you have any questions regarding this report, please call me at [redacted] or contact Harry Cooper at [redacted]. (b)(3) (b)(3)

Joseph W. Lambert
Director, Information Management Services

Enclosure

[redacted] (b)(3)

Upon removal of attachment(s), this document is UNCLASSIFIED//FOUO

Approved for Release: 2022/01/27 C06896739

Mr. John P. Fitzpatrick (b)(3)

D/IMS/JWLambert [redacted] (19 Dec 11) CIO-IMS-2011-169
[redacted] 20111219 Ltr to (b)(3)
ISOO re 2011 Annual Report on Classification Self-
Inspection.docx

Distribution:
Orig - Addressee
1 - CIO
2 - D/IMS
1 - C/CMCG
1 - [redacted] (b)(3)
(b)(6)

C06896965

Approved for Release: 2022/01/27 C06896965

2014 Classification Self Audit – Declassification

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.*

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.

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

Approved for Release: 2022/01/27 C06896965

Approved for Release: 2022/01/27 C06896965

comparisons with earlier reporting periods. It can be used to support assertions about the successes and strengths of an agency's program.

53. Declassification:

We continued our declassification program improvements with the establishment of an automated digital dashboard to help us better manage our Freedom of Information (FOIA) Privacy Act (PA) and Mandatory Declassification Review (MDR) declassification efforts. In FY2014 we achieved a FOIA/PA backlog reduction of 3%, and a MDR backlog reduction of 38%. We reduced our FOIA/PA appeals backlog by 13% and closed the ten oldest FOIA/PA appeals. In FY2014 our automatic declassification program again released over one million pages of information and for the first time 20,000 pages of President's Daily Briefs were reviewed for declassification.

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

Agency use of metrics to track its declassification efforts is a best practice. It allows managers to monitor, on a real time basis, progress toward our declassification review goals and ensure review accuracy. In an environment of high researcher demand and resource constraints, such monitoring is critical to identify bottlenecks and inefficiencies, spot trends, and redeploy resources to improve review accuracy and most efficiently manage our production workload to meet required deadlines.

Approved for Release: 2022/01/27 C06896965

C06896970

Approved for Release: 2022/01/27 C06896970

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.

Approved for Release: 2022/01/27 C06896970

C06896970

Approved for Release: 2022/01/27 C06896970

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. ○ YES ○
17. Do your self-inspections include interviews with producers (where applicable) and users of classified information?	17. ○ YES ○

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. ○ YES ○ ○
19. Do these reviews encompass all agency activities that generate classified information? ***Yes – over time.**	19. ○ YES ◔ ○

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. ○ YES ○ ○

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. ○ YES ○ ○
26. Do they have access to pertinent security classification guides? (Indicate if NA.)	26. ○ YES ○ ○
27. Have appropriate personnel been designated to correct misclassification actions? (Indicate if NA.) If so, identify below.	27. ○ YES ○ ○

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.

Approved for Release: 2022/01/27 C06896970

C06896970

Approved for Release: 2022/01/27 C06896970

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

Approved for Release: 2022/01/27 C06896970

C06896970

Approved for Release: 2022/01/27 C06896970

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

Approved for Release: 2022/01/27 C06896970

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.

Approved for Release: 2022/01/27 C06896970

C06896970

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

Approved for Release: 2022/01/27 C06896970

C06896970

Approved for Release: 2022/01/27 C06896970

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

Approved for Release: 2022/01/27 C06896970

C06896970

Approved for Release: 2022/01/27 C06896970

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.

Approved for Release: 2022/01/27 C06896970

Approved for Release: 2022/01/27 C06896970

Enclosure 2

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

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

Approved for Release: 2022/01/27 C06896970

C06896969

Approved for Release: 2022/01/27 C06896969

Central Intelligence Agency

Washington, D.C. 20505

17 December 2012

Mr. John P. Fitzpatrick
Information Security Oversight Office
700 Pennsylvania Avenue, N.W.
Washington, D.C. 20408-0001

Dear Mr. Fitzpatrick:

(U) In response to the Information Security Oversight Office's (ISOO) 23 August 2012 request, the Central Intelligence Agency (CIA) has completed an inspection of its classification practices and our report is attached.

(U//FOUO) Since the publication of EO 13526, CIA has endeavored to design an audit methodology and survey instrument that would best capture employees' classification and marking decisions and provide data that CIA could use to better tailor policies and training. We plan to audit several components across our agency each year so that we are able to obtain classification data from employees working in each of our mission and support areas.

(U//FOUO) This year's reporting cycle was focused on the audit of our headquarters based staff. We selected an administrative component that is engaged in the formulation and implementation of policy and on the development and delivery of training to our agency's employees. This unit is comprised of employees with a range of experience including some who have recently entered on duty and others with twenty or more years of experience.

(U//FOUO) At the start of the audit these employees were given a survey which asked a range of questions about their classification practices including what types of training they had received, their awareness of classification policies and tools, their safeguarding practices, and types of documents they typically classify. The audit staff then reviewed documents

Approved for Release: 2022/01/27 C06896969

Approved for Release: 2022/01/27 C06896969

Mr. John P. Fitzpatrick

The audit staff then reviewed documents created and classified by each person against a checklist that contained elements focused on the use of guidance, the classification level, the block, banner, and portion marking. The audit revealed that a percentage of documents lacked consistent portion marking but the level of classification was correct on the vast majority of documents evaluated.

(U) In order to provide a report that is unclassified, we focused on the outcome and did not discuss any classified details regarding the work, the organizational specifics, or examples of issues found.

(U) Please contact Mr. Harry Cooper, Chief, Classification Management and Collaboration Group, at 703- [redacted] if you have any questions regarding the FY 2011 submission. (b)(3)

(b)(6)

[redacted]

Joseph W. Lambert
Director, Information Management Services

Enclosure

Approved for Release: 2022/01/27 C06896969

C06896969

Approved for Release: 2022/01/27 C06896969

Executive Order 13526
2012 CIA Self Inspection Report

I. Introduction:

a. (U) In accordance with E.O. 13526 § 5.4 (d)(4) as implemented by 32 C.F.R. 2001.60, the Central Intelligence Agency (CIA) has established an ongoing self-inspection program which includes a regular review of a sample of CIA classification decisions. The 2012 CIA self-inspection report is provided to CIA's Senior Agency Official who is appointed in accordance with § 5.4 (d) of the Order and is authorized to correct misclassification actions identified during the self-inspection process. While CIA has had an ongoing self-inspection program under predecessor Orders, it is noted that the revised language in EO 13526 brings a greater level of formality to the self-inspection process and has changed the CIA's overall methodology from a distributed process where Classification Management Specialists deployed to CIA elements each conducted several annual informal inspections, to a more formal annual process where one or more components within the CIA are chosen and teams deployed to review classification of that component. The results of these formal "Classification Assistance Visits" will be synthesized into a single report to the Information Security Oversight Office (ISOO).

II. (U) Program Description:

a. In the intelligence business, classification of information is a more integral part of each employee's daily work than in perhaps any other governmental function in the United States. The CIA makes extensive use of email on classified networks, collects intelligence information that is classified upon collection, and has innumerable issues related to association of CIA with many people, places and things that often make the mere fact of association classified.

b. (U) We have relied more on the expertise of our officers in the intelligence business than we have on extensive classification guides due to the nuanced nature of our business. As part of the required fundamental classification guidance review we completed under EO 13526 § 1.9 the CIA has embarked on an significant program to re-write classification guidance on all aspects of the CIA mission. Some new guidance is now available, but work is in progress on the largest portion of the changes in guidance.

c. (U) In the 2012 self-inspection cycle we looked at a HQ based component with a largely administrative role. This element provides policy support, customer service, and training. We chose an element with a wide variety of classified documents ranging from email to formal reports to electronic messages. This unit supports sensitive compartmented programs and has a reach across the entire agency, so we believe its work is uniquely representative of a broad swath of administrative support for the agency mission. Unlike the review we made in

Approved for Release: 2022/01/27 C06896969

C06896969

Approved for Release: 2022/01/27 C06896969

2011 of an operational component, officers in this element are more steeped in corporate policy and typically are not on short duration assignments or experience a significant operational tempo in their daily work.

d. (U) In 2012 we worked to improve and standardize our self-inspection program. We utilized a standard format for data collection (see attachment "A") to ensure that each officer we reviewed and each document we inspected would be viewed under the same standards While the data collected suggests some minor changes to the form may be needed, we believe that overall this strategy for collecting information on our classification practices will work well.

e. (U) In 2013 we anticipate a blended approach including both operational components and HQ elements. We recognize that our visits to our mission elements must be equally evaluative and helpful. We will utilize these visits as opportunity for mission-specific classification training. Our goal is for employees to welcome our visits as a means to improve performance rather than as some kind of "inspection" oriented at finding problems.

III. Summary of Findings:

a. (U) Overall classification at CIA is good. In our inspection of a representative sample of documents we generally found that the classification levels assigned by the derivative classifiers were correct. A breakdown of areas we focused on includes the following:

1. **(U) Original Classification Decisions:** CIA will only report 4 OCA decisions for 2012. We did not review these decisions as they were all made by the manager of the classification management program at CIA and should reasonably be consistent with requirements of the Order.

2. (U) **Overall Classification Levels:** We have determined that the identification of classification levels using our guide has been very good. We do not believe the majority of classified documents are either under or over classified.

3. (U) **Use of Classification Guidance:** In our headquarters environment, employees use an automated tool to mark documents and that tool includes a feature allowing the employee to go directly to the guidance and review it as they make the derivative decision. We find this works well when the employee has a good understanding of the information, but the limited detail in our guidance needs improvement. We found a 5.5% error rate in using the appropriate guidance.

4. (U) **Security Violations:** The number of violations by CIA employees continues to be relatively low. Like any large organization we do have a number of simple mistakes or errors of omission (such as failing to secure a lock or transporting classified information in an unapproved

Approved for Release: 2022/01/27 C06896969

manner). As part of the required annual training for derivative classifiers we have included instruction in safeguarding that should help reduce the number of violations.

5. (U) **Portion Marking:** This remains the weakest area among CIA employees. The use of email in government is beginning to mimic its use outside of the work environment. As a result these often cryptic communications lack the formality usually associated with portion marking. We found that in 20.8% of the documents we reviewed portion marking errors (or omissions) were identified.

6. (U) **Overall Classification Quality:** In addition to the 5.5% errors in selecting the correct use of guidance and 20.8% portion marking errors we found that 2.7% also had issues with markings showing the classification of an attachment or transmittal document without the attachment. None of the reviewed documents were classified at the incorrect level. Overall about 29% of documents reviewed had some kind of error, but those errors were generally minor and procedural rather than over or under classification.

7. (U) **Declassification**: We did not evaluate declassification during this self-inspection cycle. The CIA programs, however, remain a best practice in government.

8. (U//FOUO) **Safeguarding:** Safeguarding of classified information is greatly enhanced at the CIA where virtually all work areas are Sensitive Compartmented Information Facilities (SCIFs). Regular security inspections of facilities and security equipment are provided by our Office of Security, and all deficiencies are handled as quickly as possible.

9. (U//FOUO) **Security Education and Training:** Employees are required to complete a classification management Computer Based Training (CBT) program that is revised each year, and as a condition of access to classified computer systems and networks employees must also complete a CBT annually that is focused on information systems security. Additionally, classification management professionals placed directly within agency components also provide many ad hoc training sessions or briefings to ensure employees remain continually focused on issues related to classification management and safeguarding of classified information.

10. (U//FOUO) **Management and Oversight:** Within the area of responsibility of the Chief Information Officer for CIA, the office of Information Management Services (IMS) maintains responsibility for classification management. The Director of IMS is the Senior Agency Official (SAO) under § 5.4 of the Executive Order. To facilitate his role

C06896969

Approved for Release: 2022/01/27 C06896969

as SAO, the D/IMS has established a senior level component (Classification Management and Collaboration Group) led by an SIS/SES level officer to ensure that all classification management requirements established by the Executive Order, implementing directive, or implemented by the Director of National Intelligence (DNI) have been fully complied with at the CIA. The Chief of the Classification Management Group is responsible for classification counts, self inspections and many ongoing CIA programs to ensure the protection of classified information.

IV. (U//FOUO) **Completed or Planned Corrective Actions:** Classification guidance in the form of accurate detailed guides is essential in getting classification right. The CIA has embarked on a Fundamental Classification Guidance Review as required by the Order that when completed will provide significantly better guidance to employees. Work has also begun to institutionalize the requirement for biennial training of derivative classifiers and annual training of original classifiers. This training will also go a long way toward improving employee understanding of the classification process.

V. (U) **Identified Best Practices:**

a. As discussed above, declassification at the CIA is clearly a best practice.

b. We also noted no issues with classification blocks or banner markings. This is due to a large degree to our use of an automated marking tool created by CIA that operates with every application our users create documents with. The tool applies the CAPCO register markings exactly as prescribed by ISOO and CAPCO and no mistakes are ever present in the blocks or banners with regard to format or completeness of markings. This is clearly a CIA best practice.

VI. (U) **Conclusions:**

a. Overall classification is good, but areas for improvement do exist.

1. Additional training in portion marking will be provided. We provide derivative classifier training annually (more frequently than the EO requires) and we will incorporate portion marking training in this annual training program. In addition we plan portion marking workshops to give employees hands-on instruction in portion marking different kinds of documents and messages that they write,

2. The work to improve guidance with more detailed classification guides will continue and as new guides are introduced we believe that the quality of decisions will improve. We have already completed several new guides and many others are in development. We are confident that richer guidance will improve the precision of derivative decisions.

Approved for Release: 2022/01/27 C06896969

3. We will increase awareness among employees that while email may facilitate information communication, it still requires all classification markings when the email is classified.

b. The increasingly informal ways that government business is conducted today using technology that includes instant messaging, email, blogs and wikis, is changing the way people create and mark classified information. We are learning that we need new tools, training and techniques to bring to our workforce the means to ensure protection of classified information without removing the extemporaneous nature of modern communication.

//end//

Approved for Release: 2022/01/27 C06896751

(U) MEMORANDUM

(U) To: Harry Cooper
(U) Fr: [redacted] (b)(3) (b)(6)
(U) Cc:
(U) Dt: 7 January 2014
(U) Re: Thursday Meeting with Jon – Approval of Email Text to Deployed IMTOs Regarding Self-Assessment Document Request

(U) Summary

(U) After our last classification self-assessment planning meeting (circa 27 Dec), we determined that revisions were needed to our proposed request message to the deployed component IMTOs. This email would ask each deployed team to provide CMCG with 100 documents per month to support the self-assessment. At present, the first proposed delivery date is 3 Mar 2014.

(U) Action Needed

- (U) C/CMCG guidance on whether or not action is needed to discuss request with C/RMTG and/or other RMTG officers.
- (U) Concurrence from C/CMCG to send the proposed text to deployed IMTOs via email.

(U) Proposed Text

(U//FOUO) Executive Order 13526, *Classified National Security Information*, establishes a requirement for agencies involved in classifying, safeguarding, and declassifying national security information to establish and maintain an ongoing self-inspection program, to include the regular reviews of representative samples of an agency's original and derivative classification actions.

(U//FOUO) [redacted] IMS/Classification Management and Collaboration Group (CMCG) is responsible for conducting the self-inspection program and for providing, on an annual basis, inspection results to the Senior Agency Official and to the Information Security Oversight Office (ISOO). (b)(3)

(U//FOUO) The quality of the Agency's report to ISOO depends upon the representative sample of documents provided for review. [redacted] component IMTOs are tasked with assisting CMCG with the self-inspection. Accordingly, beginning in January 2014, CMCG is asking for each of the Directorate IMO teams (DIR, DI, DS, DS&T, NCS) to collect a group of 100 documents per month for classification review of derivative classification actions. (b)(3)

[(U) Text continues, next page.]

Approved for Release: 2022/01/27 C06896751

- (U//FOUO) **CMCG will be responsible for all classification reviews; IMO teams will be responsible only for document selection and collection.**
  - Document review and data analysis helps CMCG to identify opportunities for better information and training in the future.
  - While documents are collected from individual employees, the data reported out to ISOO is attributed to the Agency only (not to an individual, an office, or a directorate).
  - CMCG does not penalize individuals for classification decisions.

- (U//FOUO) **CMCG asks for one group of 100 documents per directorate (DIR, DI, DS, DS&T, NCS) per month, with delivery requested on the first business day of the month.**
  - CMCG asks that the first group of documents be delivered on or before **3 MAR 2014**.
  - Documents may be collected from any office, to be determined at the discretion of the IMO team.
  - CMCG asks that these documents not come entirely from the same person(s) and/or office every month.
  - CMCG asks that the IMO teams document how they selected offices and individuals to be part of the sample and to report this information when submitting the documents.

- (U//FOUO) **A "document" can include any material on which the first classification decision was made.** Emails may be included, but they should be original messages – not forwards or replies, as these typically do not represent a classification action.
  - Virtually any document produced in FY2014 is eligible.
  - Documents do not have to be produced in the month that they are submitted to CMCG, but they should have a FY2014 date (1 OCT 2013-31 SEPT 2014).

- (U//FOUO) Since the mandated self-inspection is ongoing across fiscal years, CMCG asks that this process continue as requested above until otherwise directed.

- (U) For any questions or concerns about this request, please contact CMCG by email to [redacted] (b)(3)

C06896732

Approved for Release: 2022/01/27 C06896732

Central Intelligence Agency

Washington, D.C. 20505

21 October 2014

Mr. John P. Fitzpatrick, Director
Information Security Oversight Office
National Archives and Records Administration
Washington, D.C. 20408-0001

Dear Mr. Fitzpatrick:

In response to the Information Security Oversight Office, the Central Intelligence Agency submits the enclosed FY 2014 Agency Annual Self-Inspection Program Data Report. This report covers the period from 1 October 2013 to 30 September 2014.

Please contact Mr. Harry Cooper, Chief, Classification Management and Collaboration Group, at [redacted] if you have any questions regarding the report. (b)(3)

Sincerely,

[redacted] (b)(6)

Joseph W. Lambert
Director, Information Management Services

Approved for Release: 2022/01/27 C06896732

Approved for Release: 2022/01/27 C06896732

Mr. John Fitzpatrick

CIO/IMS/JWLambert [redacted] (b)(3)

[redacted] ISOO/2014 DIMS Transmittal Letter to ISOO (b)(3)

Distribution:
Orig - Addressee
1 - CIO
2 - D/IMS
1 - C/CMCG

Approved for Release: 2022/01/27 C06896732

C06396732

Approved for Release: 2022/01/27 C06896732

Enclosure 2

AGENCY ANNUAL SELF-INSPECTION PROGRAM DATA: FY 2014

(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. 21 October 2014
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 [redacted] (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, Jr. Chief, Classification Management and Collaboration Group (CMCG) CIA, Washington, DC 20505 [redacted] (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, Jr. Chief, Classification Management and Collaboration Group (CMCG) CIA, Washington, DC 20505 [redacted] (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. ◉ Yes ○ No
7. Does your agency perform original classification activity?	7. ◉ Yes ○ No
8. Does your agency perform derivative classification activity?	8. ◉ Yes ○ No
9. Does your agency have an approved declassification guide and declassify CNSI?	9. ◉ Yes ○ No

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 SAO delegates responsibility to CMCG for the self-inspection program, approves the annual self-inspection plan, receives briefings on its results and recommendations, and approves follow-on actions. During FY14, the SAO also observed self-inspection directly through travel with CMCG to a field location.

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?

During FY14, while conducting ongoing self-inspection of documents in the Washington Metro Area (WMA), CMCG engaged field location counterparts through travel. Following each travel opportunity, the SAO received a briefing of the results. As mentioned above, the SAO also accompanied CMCG on field location travel. The self-inspection program is designed to cover compliance with all 5.4(d) areas of responsibility and to identify best practices and areas for improvement.

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 of CMCG, an SES-level officer, is designated to assist in directing and administering the self-inspection program. A number of classification specialists in CMCG conduct the self-inspections.

Approach

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

Building from success in FY13, CMCG developed a standard operating procedure to govern data collection in the WMA and from field locations. Subsequently, CMCG partnered with IMS records management colleagues to capture a substantial electronic collection of data from across the primary components of CIA, and CMCG collaborated with colleagues in field locations to ensure that documents sampled covered the depth and breadth of mission activities and support. CMCG conducted personnel interviews in field locations, performed extensive document review, and collaborated with declassification and security colleagues to obtain the necessary information. Subsequently, results were analyzed, and findings and recommendations were prepared for the SAO and ISOO.

Approved for Release: 2022/01/27 C06896732

C06896732

Approved for Release: 2022/01/27 C06896732

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.

Throughout FY14, CMCG reviewed documents across all components of CIA through document sampling and through classification assistance. In support of the self-inspection effort, CMCG engaged in nine field location visits during FY14. Additionally, CMCG conducts the annual Classification Count and analysis and a compliance review of mandatory Original and Derivative Classification Training, as required by E.O. 13526.

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
- ■ Derivative classification
- ■ Security violations
- ■ Declassification
- ■ Safeguarding
- ■ Security education and training
- ■ Management and oversight

16. Do your self-inspections include a review of relevant security directives and instructions?	16. ◉ Yes ○ No
17. Do your self-inspections include interviews with producers (where applicable) and users of classified information?	17. ◉ Yes ○ No

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. ◉ Yes ○ No ○ NA
19. Do these reviews encompass all agency activities that generate classified information?	19. ◉ Yes ○ No ○ NA

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.)

In order to review a sample of documents covering all agency activities and mission support, CMCG engaged in document review and personnel interviews in field locations close to mission and performed extensive document review and data analysis in the WMA. In the WMA, CMCG deliberately sampled documents that reflect the five major business areas of the agency.

21. Do the reviews include a sampling of various types of classified information in document and electronic formats?	21. ◉ Yes ○ No ○ NA

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

In the WMA, CMCG worked with IMS records management colleagues to collect a sample of data that covered all agency components. This data collection yielded material across the spectrum of the CIA mission, from administrative matters to intelligence analysis to operational activity. CMCG supplemented its WMA review with visits to field locations, providing a sample of documents directly related to the day-to-day mission critical activities of CIA.

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.)

After receiving an initial sample of over one thousand documents, CMCG reviewed the material to ensure that all five primary business areas and their individual missions/responsibilities were present in the sample. CMCG deemed that this sample was sufficient to enable a credible assessment, based on the requirements of 32 CFR 2001.60. After reviewing the results of inspection work in nine field locations, CMCG determined that the final data sample proportionally represented the spectrum of documents associated with CIA operations.

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

In the WMA, designated CMCG full-time classification specialists conduct document reviews. For field reviews, CMCG designates teams of 2-3 individuals to conduct classification reviews, interview field personnel, and provide training on classification policies, practices, and employee obligations regarding their secrecy agreements.

25. Are the personnel who conduct the reviews knowledgeable of the classification and marking requirements of E.O. 13526 and its implementing directive?	25. ◉ Yes ○ No ○ NA
26. Do they have access to pertinent security classification guides? (Indicate if NA.)	26. ◉ Yes ○ No ○ NA
27. Have appropriate personnel been designated to correct misclassification actions? (Indicate if NA.) 27a. If so, identify below.	27. ◉ Yes ○ No ○ NA

The Chief of CMCG and all of the group's classification specialists.

Frequency

28. How frequently are self-inspections conducted?

CMCG conducts the self-inspection year-round. Nine field location visits took place over approximately five months of FY14.

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

Field location visits required extensive coordination with the respective offices to facilitate information access that would not disrupt mission-critical activities. Document inspection continued year-round in the WMA in order to allow CMCG sufficient time to identify possible data gaps within the sample and to provide the opportunity to return to IMS records management partners for additional documents.

Approved for Release: 2022/01/27 C06896732

C06896732

Approved for Release: 2022/01/27 C06896732

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 above, in order to review a sample of documents covering all agency activities and mission support, CMCG engaged in document review and personnel interviews in field locations and performed extensive document review and data analysis in the WMA. CIA has five major business areas, and CMCG deliberately sampled documents that reflect these components and their respective areas of responsibility within the broader CIA mission.	
31. How is the self-inspection program structured to assess individual agency activities and the agency as a whole?	
CMCG carefully considers the type of function performed in each component and the types of documents that each of these components produces. Classification assistance questions from the current and prior fiscal year help to shape this consideration. CMCG also considers the demanding circumstances surrounding work in the field and in high-tempo areas of CIA as it pertains to understanding how officers in field offices classify information.	
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. ◉ Yes ○ No ○ NA
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. ◉ Yes ○ No ○ NA
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. ◉ Yes ○ No ○ NA
Reporting	
35. What is the format for documenting self-inspections in your agency?	
CMCG documents its self-inspection through standardized document checklists, followed by data aggregation spreadsheets. CMCG also uses standardized forms for field personnel interviews. Following each field visit, CMCG prepares a classified trip report that analyzes findings and after-action opportunities related to classification training and practice improvements. As requested, CMCG briefs the SAO on these visits and overall progress. At the end of the self-inspection, CMCG prepares the annual report and briefing materials for the SAO and other agency senior officials, as necessary.	
36. Who receives the reports?	
The SAO; Chief of CMCG; the Chief Information Officer; other agency senior officials, as necessary; ISOO.	
37. Who compiles/analyzes the reports?	
The CMCG self-inspection staff.	
38. How are the findings analyzed to determine if there are problems of a systemic nature?	
CMCG aggregates data from the document checklists and personnel interviews in spreadsheets, then develops formulas that identify opportunities for improvement in the reporting areas required by ISOO, including: over/underclassification, overall marking requirements, and portion marking. CMCG also tracks and analyzes trends in classification derivative choices, application of dissemination controls, classification differences between WMA and field locations, and classification differences between the five major agency components. The final analysis helps CMCG identify potential areas for improvement in both customized and agency-wide original and derivative classifier training.	
39. How and when are the results of the self-inspections reported to the SAO?	
CMCG briefs the SAO after completion of data analysis and production of draft findings and recommendations. The annual self-inspection program data form is submitted to the SAO before it is released to ISOO. Once the SAO approves the findings and recommendations, CMCG submits the form to ISOO and begins implementation of recommendations, as necessary.	
40. How is it determined if corrective actions are required?	
CMCG carefully analyzes its document review and interview data for opportunities for improvement in agency-wide classification practices. If/when patterns are evident either in a particular business area or agency-wide, CMCG develops possible corrective action for consideration by the SAO.	
41. Who takes the corrective actions?	
Action depends on the finding: CMCG, IMS records management partners, field offices when necessary.	
42. How are the findings from your agency's self-inspection program distilled for the annual report to the Director of ISOO?	
CMCG relies upon spreadsheet analysis of documents and raw-answer aggregation of interview data to distill findings for the Director of ISOO. Self-inspection findings are also supported by day-to-day classification support and training provided by CMCG to CIA.	
43. Has the SAO formally endorsed this self-inspection report? If yes, please provide documentation.	43. ◉ Yes ○ No

Approved for Release: 2022/01/27 C06896732

Approved for Release: 2022/01/27 C06896732

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 (OCAs) was kept at the lowest possible level, based on a demonstrable and continuing need to exercise this authority, per E.O. 13526, Sec. 1.3. This information was provided to ISOO separately via a letter signed by Director, IMS, including the positions of all current OCAs. During FY14, CIA had an estimated 18 OCA actions, which will be reported separately on the SF-311. Self-inspection found that original classifier training was provided and, in keeping with this training, OCAs understood that their authority is only to be exercised in the rare case that an Agency classification guide does not provide sufficient guidance, and there appears to be a need for classification, based on the E.O. 13526 criteria.

45. Derivative Classification:

From a sample of over 1,600 documents, the self-inspection found that 9.0% of the sample was overclassified. More specifically: 12.3% of documents classified as Top Secret (TS) were overclassified, including 11.4% that should have been Secret (S); less than 1% that should have been Confidential (C); and less than 1% that should have been For Official Use Only (FOUO). 6.3% of documents classified as S were overclassified, including 3.2% that should have been C; 1.9%, FOUO; and less than 1%, fully Unclassified (U). 16.0% of the documents classified as C were overclassified, although -- with only one exception -- the U documents would have included dissemination controls (e.g., FOUO). The self-inspection found that 14.5% of the sample was underclassified. The predominant finding was that 48.8% of documents classified as C should have been S instead. Additionally, the self-inspection noted that a majority of the sample (85.4%) lacked correct portion marking; 4.1% had an inappropriate ORCON/NOFORN caveat; 1.3% were missing all or part of the classification block; and 1.3% failed to identify the derivative classifier.

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 E.O. 13526 are in alignment with the E.O., existing Federal statutes, and other pertinent Executive Branch issuances. Specifically, while adhering to E.O. 13526, the Agency follows the governing requirements outlined in ICD 503 for information technology; ICD 704 for personnel security; ICD 705 for physical and technical security; and E.O. 12829 and the NISPOM for industrial security. All of these build upon the requirements listed in E.O. 13526. Additionally, the Agency is developing a more robust administration model for all information technology systems to provide enhanced enforcement of appropriate access and controls for users.

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 E.O. 13526 and with procedures established by the Department of Justice and the Federal Bureau of Investigation. The review confirmed that the Agency dedicates resources to ensure its ability to investigate leaks to the media and promotes enhanced internal awareness programs for employees and contractors to ensure adherence to all required security regulations involving unauthorized disclosures of classified information to the media. The Agency also has embarked on a campaign to ensure the Agency population, including cleared contractors, is made aware of their enduring obligation to protect classified information under the terms of the nondisclosure agreement. Additionally, the Agency maintains a 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 requirements of E.O. 13526 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 and mandatory training, exit debriefing, classification training, and pre-publication reviews. Training received is recorded in personnel records.

50. Management and Oversight:

CMCG provides a year-round resource for classification assistance to mission partners. This includes courses intended for the professional training of classification specialists, training for new personnel in the fundamentals of classification, as well as more specialized training for the various components. CMCG also provides original and derivative classifier refresher training and a classification assistance service that provides real-time assistance to Agency personnel. Beginning in FY14, CMCG deployed its first classification referent to serve as an in-house expert for specific business areas. These functions provide insight into the types of problems that are encountered on a daily basis and helps CMCG strengthen classification training, classification guide development, and regulatory policy adjustments which provide meaningful support to the workforce. CMCG brings issues to the attention of the SAO, who consults with the CIO, Agency Executive Director, and others as appropriate.

Approved for Release: 2022/01/27 C06896732

C06896732

Approved for Release: 2022/01/27 C06896732

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:

During FY14, 14 of the 18 OCA actions involved approval of new classification guides developed in collaboration with business areas in order to provide meaningful information protection guidance to officers working with those equities. CMCG continues to work closely with subject matter experts throughout the Agency to identify other business areas, programs, projects, and/or topics that would benefit from more customized guidance associated with classified material.

52. Derivative Classification:

CMCG strives to support CIA toward the highest standard for classifying material; therefore, a rate of over 20% under- and overclassification is not acceptable. Lessons learned from the self-inspection will help CMCG to tailor its classification training and guidance to focus on specific improvement standards, including a greater rate of accurate portion marking; better use of certain classification guide derivatives; and applying changes to the electronic classification marking tool to improve banner and portion marking. Based on the FY14 sample, an information campaign tailored to preventing the use of inappropriate "ORCON/NOFORN" caveats helped CMCG to reduce the use of this caveat from about 8% in FY13 to 4.1% in FY14. CMCG will continue to use similar strategies to inform the workforce on additional changes to classification markings and IC standards and requirements.

53. Declassification:

CIA continued declassification program improvements with the establishment of an automated digital dashboard to help the Agency better manage Freedom of Information Act (FOIA), Privacy Act (PA), and Mandatory Declassification Review (MDR) declassification efforts. In FY14, CIA achieved a FOIA/PA backlog reduction of 3% and an MDR backlog reduction of 38%. The Agency reduced the FOIA/PA appeals backlog by 13% and closed the ten oldest FOIA/PA appeals. In FY14, the Agency automatic declassification program again released over one million pages of information and, for the first time, 20,000 pages of President's Daily Briefs were reviewed for declassification.

54. Safeguarding:

The Agency's safeguarding measures are meeting mission needs. The Agency continually evaluates and tests its existing safeguarding measures. Safeguarding policies and procedures are being reviewed and updated to leverage technological advances for information technology (IT) systems; ensure best practices are used in information sharing; to inform the Agency population of proper classification conventions; and revise facility access protocols. In the IT systems area, the Agency is building tools to maximize accessibility of information for authorized personnel while automating process to detect and flag improper sharing of information.

55. Security Violations:

The review determined that Agency personnel appropriately report security violations. Currently, the Agency is updating its policies and procedures related to protection, accountability, control, and disposition of classified information to ensure personnel are provided with detailed guidance for all aspects of safeguarding classified national security information.

56. Security Education and Training:

The Agency security and education training program meets the needs of the Agency's mission through curriculum that offers instruction for all aspects of safeguarding information. For example, advanced training for administrators reinforces the users' responsibility to protect classified data, and specialized training ensures privileged users are informed fully regarding security policies and standards. Additionally, the Agency has published updated national security classification guides to promote the identification, markings, and integrity of classified security information.

57. Management and Oversight:

The self-inspection demonstrated the benefit of providing face-to-face guidance and training to Agency personnel in the WMA and the field. Travel efforts allowed CMCG to conduct hands-on interaction with field materials and officers and increased awareness of classification resources. The development of business-area specific classification guides and the deployment of a classification referent for a unique business area also demonstrated the value added to information protection when customized support is present. Interviews conducted during the self-inspection indicated that CMCG needs to improve efforts to publicize available web-based classification resources, its classification hotline, and its email support option. Accordingly, CMCG has taken steps to collaborate with IMS records management colleagues on unique customer-facing information resources, including internal blogs. CMCG will continue to assess the mission support and enhancement associated with customized classification guides, classification referents, and tailored training.

Approved for Release: 2022/01/27 C06896732

C06896732

Approved for Release: 2022/01/27 C06896732

Enclosure 2

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 ○ No ○ NA
59. Has the agency validated that this training has been received?	59. ◉ Yes ○ No ○ NA
60. What percentage of the original classification authorities at your agency has received this training?	60. 83% ◉ Actual ○ Estimated
61. Have any waivers to this requirement been granted?	61. ○ Yes ◉ No ○ NA
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 ○ No ○ NA
63. Has the agency validated that this training has been received?	63. ◉ Yes ○ No ○ NA
64. What percentage of the derivative classifiers at your agency has received this training?	64. 97% ○ Actual ◉ Estimated
65. Have any waivers to this requirement been granted?	65. ◉ Yes ○ No ○ NA
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?	66. ◉ Yes ○ No
67. Has the agency validated that this training has been received?	67. ◉ Yes ○ No
68. What percentage of cleared personnel at your agency has received this training?	68. 100% ◉ Actual ○ Estimated
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 ○ No
70. Has the agency validated that this training has been received?	70. ◉ Yes ○ No
71. What percentage of the cleared employees at your agency has received this training?	71. 97% ○ Actual ◉ 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 ○ No ○ NA
73. What percentage of the documents sampled meet this requirement?	73. 98.9%
74. What was the number of documents reviewed for this requirement?	74. 1,648
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 ○ No ○ NA
76. What percentage of the documents sampled meet this requirement?	76. 50%
77. What was the number of documents reviewed for this requirement?	77. 1,648

Approved for Release: 2022/01/27 C06896732

C06896732

Approved for Release: 2022/01/27 C06896732

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 ○ No
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 ○ No
80. What percentage of such personnel at your agency has this element in their performance evaluations?	80. 100% ⦿ Actual ○ Estimated
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 ○ No ○ NA
82. Have all delegations been limited to the minimum required based on a demonstrable and continuing need to exercise this authority?	82. ⦿ Yes ○ No ○ NA
83. If changes have been made, have they been reported, by name or position, to ISOO?	83. ◉ Yes ○ No ○ NA
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 ○ No
85. Does your agency's training for OCAs and for personnel who apply derivative classification markings cover classification challenges?	85. ⦿ Yes ○ No
86. Does your agency's training for all other cleared personnel cover classification challenges?	86. ◉ Yes ○ No

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. 18 Original; 1,648 Derivative

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)	70
88 (b) Overgraded/Undergraded: Information classified at a higher/lower level than appropriate.	88 (b)	332
88 (c) Declassification: Improper or incomplete declassification instructions or no declassification instructions.	88 (c)	17
88 (d) Duration: A shorter duration of classification would be appropriat	88 (d)	87
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)	18
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)	256
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)	7
88 (j) Marking: A document lacks overall classification markings or has improper overall classification markings.	88 (j)	378
88 (k) Portion Marking: The document lacks some or all of the required portion markings	88 (k)	1,214
88 (l) Instructions from a classification guide are not properly applied.	88 (l)	453
88 (m) Other: Inappropriate use of prohibited ORCON/NOFORN caveat.	88 (m)	67

Approved for Release: 2022/01/27 C06896732

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 continue to use its mandatory derivative classifier refresher training, new employee training, and varied classification topic training courses to improve awareness of appropriate classification marking policies and practices. CMCG uses internal information forums, including IMS blogs, group newsletters, the CMCG website, and CIA news resources to publicize and promote requirements. During FY14, CMCG used these means to raise awareness regarding current and forthcoming changes to HCS and ORCON-USGOV. CMCG has started the process of translating lessons learned into process improvements through its classification assistance resources, feedback to field locations visited, and highlighting persistent problems through the internal media resources referenced above. CMCG will continue to work with electronic systems developers to address identified issues with automated classification and will maintain its active role in review of, and counsel toward, changes in IC markings standards and their application within the Classification Marking Tool. CMCG will continue its engagement with the major business areas of CIA to translate the findings of this inspection into action in FY15.

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.

Agency use of metrics to track its declassification efforts constitutes a best practice. Metrics allow managers to monitor, on a real-time basis, progress toward declassification review goals and to ensure review accuracy. In an environment of high researcher demand and resource constraints, such monitoring is critical to identify bottlenecks and inefficiencies, spot trends, and redeploy resources to improve review accuracy. This helps CIA to manage most efficiently its production workload to meet required deadlines.

The inclusion of field locations offered tremendous insights into the application of classification training, awareness, and resources to mission-critical activities. The ability to sample field documents and interview personnel provided CMCG with valuable information on the impact of location and close-to-mission focus on classification practices. Additionally, the opportunity to brief leadership in the field provided a valuable information sharing opportunity and allowed CMCG to promote available classification assistance resources. During FY14, the addition of a classification referent to a major-action business area provided the ability to better serve mission partners in a timely, efficient manner. CMCG will continue to explore additional deployment of these officers in the future.

CMCG deployed its FY15 mandatory derivative classification training refresher course on 1 October. This will allow CMCG to strengthen metrics reporting to ISOO on this E.O. 13526 obligation.

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.

Q65. One waiver was granted regarding the derivative classification training requirement. The individual who received the waiver completed the training before the end of FY14.

Q76. In its survey of 1,648 documents, CMCG found 70 documents that used Multiple Sources, a source document, or another government agency classification guide in either the classification block of the primary document or in attachments to the primary document. 56 of these documents involved Multiple Sources specifically. CMCG discovered that the major issue for derivative classifiers existed in the transfer of "Multiple Sources" as a classification citation from attachments to primary documents. Additional training and education on this point should help remedy the issue in FY15.

Q88H. CMCG found 256 instances in which documents 1) met the criteria for classification; 2) were marked as classified; and 3) were classified at the correct level; but with the wrong citation from the CIA National Security Classification Guide (NCSG). Adjusting for possible discrepancies in the level of classification, this number rises to 341.

Q88K. CMCG found the failure to fully and or appropriately portion mark to be a major issue in the FY14 self-inspection. CMCG applied a very conservative standard to this assessment, marking as wrong those documents that did not fully and correctly use portion marks for all required document portions. CMCG held classified documents and unclassified documents with dissemination controls to the same standard. Subsequently, CMCG found only 72 documents that fully met the standard for correct portion marks. Another 151 documents were found to be partially correct. Through document review and interviews with field personnel, CMCG found that the practice of portion marking often was not observed when officers were faced with time-sensitive, mission-critical matters.

Q88L. CMCG found 453 instances in which documents 1) met the criteria for classification; 2) were marked as classified; 3) were classified at the correct level; and 4) had at least one correct citation from the CIA NCSG, but were found to be missing other reasonable citations from the NCSG. Adjusting for possible discrepancies in the level of classification, this number rises to 478.

For ISOO Use Only

ISOO Analyst: _____
Date QC: _____
Analyst Initials: _____

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

C06896750

Approved for Release: 2022/01/27 C06896750

Central Intelligence Agency

Washington, D.C. 20505

5 November 2015

Mr. John P. Fitzpatrick, Director
Information Security Oversight Office
National Archives and Records Administration
Washington, D.C. 20408-0001

Dear Mr. Fitzpatrick:

(U) In response to the Information Security Oversight Office (ISOO), the Central Intelligence Agency (CIA) submits the enclosed FY 2015 Agency Annual Self-Inspection Program Data Report. This report covers the period from 1 October 2014 to 30 September 2015.

(U//FOUO) CIA built upon its successes from last year's report and continues to find great value in this exercise. In the 2,614 documents we reviewed, we found that portion marking continues to be a great shortcoming, but derivative classifiers tend to classify at the right level for the right reasons. We also found our OCA training numbers to be low, but this is due in part to shifts in personnel from OCA positions to newly created mission centers and directorates. CIA will review its OCA delegations in the coming months, likely increasing the number of OCAs to accommodate ten new mission centers and one new directorate. CIA will also use this review as opportunity to ensure that far more of our OCAs are properly trained by the end of FY 2016.

Approved for Release: 2022/01/27 C06896750

Approved for Release: 2022/01/27 C06896750

(U) Please contact Mr. Harry Cooper, Chief, Classification Management and Collaboration Group, at 703- [redacted] if you have any questions regarding the FY 2015 self-inspection report. (b)(3)

Sincerely, (b)(6)

[redacted]

Joseph W. Lambert
Director, Information Management Services

Approved for Release: 2022/01/27 C06896750

C06896750

Approved for Release: 2022/01/27 C06896750

Enclosure 2

AGENCY ANNUAL SELF-INSPECTION PROGRAM DATA: FY 2015

(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 3, 2015
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, Jr. Chief, Classification Management and 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, Jr. Chief, Classification Management and Collaboration Group (CMCG) 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. (•) Yes ( ) No
7. Does your agency perform original classification activity?	7. (•) Yes ( ) No
8. Does your agency perform derivative classification activity?	8. (•) Yes ( ) No
9. Does your agency have an approved declassification guide and declassify CNSI?	9. (•) Yes ( ) No

PART C: Self-Inspection Program Activity: Number of Self-Inspections Conducted

In FY 2014 and prior years, this information was reported on Standard Form 311, "Agency Security Classification Management Program Data."

10. Enter the **number of self-inspections** of the classified national security information program that were conducted by your agency during the reporting period. (Note that this does not include routine after-hours security checks.)	10. 17

PART D: 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

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

The SAO delegates responsibility to CMCG for the self-inspection program, approves the annual self-inspection plan, receives briefings on its results and recommendations, and approves follow-on actions.

12. 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?

During FY15, while conducting ongoing self-inspection of documents in the Washington Metro Area (WMA), CMCG engaged field location counterparts through travel. Following each travel opportunity, the SAO received a memo with the results. The self-inspection is designed to cover compliance with all 5.4(d) areas of responsibility and to identify best practices and areas of improvement.

13. 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 of CMCG, an SES-level officer, is designed to assist in directing and administering the self-inspection program. A number of classification specialists in CMCG conduct the self-inspections.

Approach

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

CMCG continues to utilize best practices developed during FY14, including a standard operating procedure, working with records management colleagues to capture electronic records, and collaborating with colleagues in the field to access their records. CMCG further refined its assessment worksheets to streamline collection and better address questions posed by the SAO, CMCG, and ISOO.

Approved for Release: 2022/01/27 C06896750

C06896750

Approved for Release: 2022/01/27 C06896750

15. 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.

CMCG continued to review documents across all components of CIA through document sampling and classification assistance throughout FY15. CMCG also engaged in 16 field location visits during FY15, which are counted as separate self-inspections in Part C, above. CMCG continued to conduct the annual Classification Count and analysis.

16. 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
- ■ Derivative classification
- ■ Security violations
- ■ Declassification
- ■ Safeguarding
- ■ Security education and training
- ■ Management and oversight

17. Do your self-inspections include a review of relevant security directives and instructions?	17. ◉Yes ○No
18. Do your self-inspections include interviews with producers (where applicable) and users of classified information?	18. ◉Yes ○No

Approach: Representative Sample

(If your agency does not classify information, indicate NA.)

19. 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?	19. ◉Yes ○No ○NA
20. Do these reviews encompass all agency activities that generate classified information?	20. ◉Yes ○No ○NA

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

In the WMA, CMCG deliberately sampled documents that reflect the five major business areas of the agency. In field locations, CMCG worked closely with officers to ensure that the reviewed documents reflected an accurate depiction of their unique missions. The diversity of locations provided CMCG with a sample of all the activities encompassed by CIA's mission.

22. Do the reviews include a sampling of various types of classified information in document and electronic formats?	22. ◉Yes ○No ○NA

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

In the WMA, CMCG worked with IMS records management colleagues to collect a sample of documents that covered all agency components. This yielded material across the spectrum of the CIA mission. CMCG also reviewed analysis and reporting published on internal portals so as to evaluate trends of classified materials disseminated outside of the agency. CMCG continued to conduct visits to field locations, which provided a unique sample of documents related to the day-to-day mission critical activities of CIA.

24. 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 has continually assessed the documents reviewed to ensure the sample represents all major business areas and the missions/responsibilities of those areas. CMCG deemed that this sample was sufficient to enable a credible assessment, based on the requirements of 32 CFR 2001.60. CMCG also determined that documents from 16 field locations represent the spectrum of documents associated with CIA operations.

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

Designated CMCG full-time classification specialists conduct document reviews. For field reviews, CMCG designates teams of three individuals to conduct classification reviews, interview field personnel, and provide training on classification policies, practices, and employee obligations regarding their secrecy agreements.

26. Are the personnel who conduct the reviews knowledgeable of the classification and marking requirements of E.O. 13526 and its implementing directive?	26. ◉Yes ○No ○NA
27. Do they have access to pertinent security classification guides? (Indicate if NA.)	27. ◉Yes ○No ○NA
28. Have appropriate personnel been designated to correct misclassification actions? (Indicate if NA.) 28a. If so, identify below.	28. ○Yes ◉No ○NA

Frequency

29. How frequently are self-inspections conducted?

CMCG conducts the self-inspection year round. 16 field location visits took place over approximately seven months of FY15.

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

Field location visits require extensive coordination with the respective offices to facilitate access in a manner that would not disrupt mission critical activities. Document inspection in the WMA continued year-round in order to allow CMCG sufficient time to identify possible data gaps within the sample and to provide opportunity to return to IMS records management partners for additional documents.

Approved for Release: 2022/01/27 C06896750

Enclosure 2

Coverage	
31. How do you determine what offices, activities, divisions, etc., are covered by your self-inspection program? What agency activities are assessed?	
CMCG engaged in document review and personnel interviews in field locations and performed extensive document review and data analysis in the WMA. CIA had five major business areas, and CMCG deliberately sampled documents that reflect these components and their respective areas of responsibility within the broader CIA.	
32. How is the self-inspection program structured to assess individual agency activities and the agency as a whole?	
CMCG carefully considers the type of function performed in each component and the types of documents that each of these components produces. Classification assistance questions and results from previous years' self-inspections help to shape this consideration. CMCG also considers the demanding circumstances surrounding work in the field and in high-tempo areas of CIA as it pertains to understanding how officers in the field classify information.	
Special Access Programs (SAP) (If your agency does not have the authority to create SAPs, indicate NA.)	
33. If your agency has any special access programs, are self-inspections of the SAP programs conducted annually?	33. ◉Yes ○No ○NA
34. 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?	34. ○Yes ○No ◉NA
35. 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?	35. ◉Yes ○No ○NA
Reporting	
36. What is the format for documenting self-inspections in your agency?	
CMCG documents its self-inspection through standardized document checklists, followed by data aggregation spreadsheets. CMCG also uses standardized forms for field personnel interviews. Following each field visit, CMCG prepares a classified trip report that analyzes findings and after-action opportunities related to classification training and practice improvements. As requested, CMCG briefs the SAO on these visits and overall progress. At the end of the self-inspection, CMCG prepares the annual report and briefing materials for the SAO and other senior officials, as necessary.	
37. Who receives the reports?	
The SAO; Chief of CMCG; the Chief Information Officer; other agency senior officials, as necessary; ISOO.	
38. Who compiles/analyzes the reports?	
The CMCG Analysis and Review Staff.	
39. How are the findings analyzed to determine if there are problems of a systemic nature?	
CMCG aggregates data from the document checklists and personnel interviews in spreadsheets, then develops formulas that identify opportunities for improvement in the reporting areas required by ISOO. CMCG also tracks and analyzes trends in classification derivative choices, application of dissemination controls, classification differences between WMA and field locations, and classification differences between the five major agency components. The final analysis helps CMCG identify potential areas for improvement in both customized and agency-wide original and derivative classifier training.	
40. How and when are the results of the self-inspections reported to the SAO?	
CMCG briefs the SAO after completion of data analysis and production of draft findings and recommendations. The annual self-inspection program data form is submitted to the SAO before it is released to ISOO. Once the SAO approves the findings and recommendations, CMCG submits the form to ISOO and begins implementation of recommendations as necessary.	
41. How is it determined if corrective actions are required?	
CMCG carefully analyzes its document review and interview data for opportunities for improvement in agency-wide classification practices. If/when patterns are evident, either in a particular business area or agency-wide, CMCG develops possible corrective action for consideration by the SAO.	
42. Who takes the corrective actions?	
This depends on the finding: CMCG, IMS records management partners, field offices when necessary.	
43. How are the findings from your agency's self-inspection program distilled for the annual report to the Director of ISOO?	
CMCG continues to conduct analysis of documents via spreadsheet. This information is distilled into findings for the Director of ISOO. Self-inspection findings are also supported by day-to-day classification support, training provided by CMCG to CIA, and data collected during the annual classification count.	
44. Has the SAO formally endorsed this self-inspection report? If yes, please provide documentation.	44. ◉Yes ○No

Enclosure 2

PART E: 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.

45. Original Classification:

The self-inspection determined that the number of original classifiers (OCAs) was kept at the lowest possible level, based on demonstrable and continuing need to exercise this authority, per E.O. 13526, Sec. 1.3. Original classifier training was frequently provided and, in keeping with this training, OCAs understood that their authority is only to be exercised in the rare case that an Agency classification guide does not provide sufficient guidance, and there appears to be a need for classification, based on E.O. 13526 criteria.

46. Derivative Classification:

From a sample of over 2,100 documents, the self-inspection found that 5.02% of documents were overclassified and 3.03% were underclassified. Specifically, 17.31% of documents classified as TOP SECRET (TS) were overclassified, including 16.83% that should have been SECRET (S). 2.84% of documents classified S were overclassified, with 2.07% that should have been CONFIDENTIAL (C). Less that 1% of C documents were overclassified, but 1.76% of C documents were underclassified. Most prominently, the self-inspection found that 87% of sampled documents lacked portion marking. CMCG also noted that 2% of sampled documents had an inappropriate ORCON/NOFORN caveat.

47. Declassification:

CIA continued declassification program improvements with additional metrics and statistical reports to better manage Freedom of Information Act (FOIA), Privacy Act (PA), and Mandatory Declassification Review (MDR) declassification efforts. In FY15, initial FOIA/PA backlog increased 43% and MDR backlog decreased 45%. The Agency reduced the FOIA/PA appeals backlog by 4% and the MDR backlog by 18%. The Agency closed nine of the 10 oldest FOIA initial cases and five of the 10 oldest FOIA appeals cases. The CIA automatic declassification program in FY15 received a 100% score in the ISOO assessment (external ISOO assessment vice "self-assessment"). The ISOO assessment evaluated missed exemptions, missed referrals, and improper exemptions. Our own internal quality assurance program for automated review, which looks at 100% of declassified documents, has identified a less than 2% error rate prior to official declassification (errors are subsequently corrected). Once released, errors identified by ourselves, other government agencies, or the public are rare.

48. Safeguarding:

The review found that the Agency has a robust program for safeguarding classified information. Within the components, instructions are in place and staff and contract employees are aware of the policies and procedures. The Agency has a diverse training and education program designed to address each aspect of safeguarding national classified information such as classification; personnel reporting requirements; and cyber security. Within each of the safeguarding disciplines, the Agency strives to develop proactive measures versus reactive measures to secure classified information. Following E.O. 13526 and the Intelligence Community Directives (ICDs), the Agency has revised numerous regulatory issuances to provide specific guidance to employees and contractors.

49. Security Violations:

The review determined that the Agency has a well-developed program to ensure security violations are investigated, adjudicated, and recorded in alignment with E.O. 13526, Presidential Decision Directive 12, ICDs 703 and 704, and with procedures established by the Department of Justice and the Federal Bureau of Investigation. Violations are recorded and tracked to prevent repeated violations. Employees receive one-on-one counseling when incidents do occur. The Agency has a sustained record of providing training and employee awareness to prevent security violations. The Agency's number of security violations has remained consistent between FY14 and FY15.

50. Security Education and Training:

The review concluded that the Agency's program for Security Education and Training supports multiple training levels--from orientation for new hires, to mandatory refresher courses, to in-depth, area-specific training for employees and contractors. Employee awareness is high as a result of regularly offered special courses and lectures. The Agency's program to record all training and enforce mandatory training requirements ensure the opportunity for all employees to demonstrate a sound understanding of safeguarding classified information.

51. Management and Oversight:

CMCG provides year-round classification assistance to CIA and its partners. This includes professional courses for classification specialists, training for new personnel in the fundamentals of classification, as well as training for various components and federal partners. CMCG also provides original and derivative classifier refresher training and a classification assistance service that provides real-time assistance to Agency personnel. Based on the initial success of the program in FY14, CMCG has increased the number of classification referents deployed to Agency business areas, which provides improved classification assistance to a second business area. These functions provide insight into the types of problems that are encountered on a daily basis and helps CMCG strengthen classification training, classification guide development, and regulatory policy adjustments which provide meaningful support to the workforce. CMCG brings issues to the attention of the SAO, who consults with the CIO, Agency Executive Director, and others as appropriate.

Enclosure 2

PART F: 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.

52. Original Classification:

During FY15, 9 of the 14 OCA actions involved approval of new classification guides developed in collaboration with business areas in order to provide meaningful protection guidance to officers working with these equities. CMCG continues to work closely with subject matter experts throughout the Agency to identify other business areas, projects, programs, and/or topics that would benefit from more customized guidance associated with classified material.

53. Derivative Classification:

CMCG continues to strive toward the highest standard for classifying material and continues to include lessons learned during the self-inspection in planning for future actions. Proper portion marking continues to be a major shortcoming agency-wide and will be a specific point of emphasis in all future training. Issues with classified information in cables and email signatures has been raised in many discussions and agency authorities have sent reminders to users in the field to be especially vigilant about this reoccurring error. By the end of FY15, CIA has created 24 Security Classification Guides (SCGs) and is in the process of developing another 23. Through FY16, CMCG will continue to provide live support to personnel and develop on-demand web-based training and assistance that can reach officers worldwide.

54. Declassification:

IMS is pursuing a major new information technology initiative, Next Generation Information Management (NGIM). This initiative includes new tools based on machine learning and artificial intelligence designed to significantly improve review accuracy, equity identification, and review efficiency. The Agency continues to refine processes and management to improve its declassification efforts. The Information Review and Release Group is also taking advantage of new resources and opportunities to increase training and outreach within the Agency and around the US Government. The Agency understands that declassification work will continue to increase at a staggering pace and CIA will continue to identify and leverage new partnerships and opportunities to meet the challenges ahead.

55. Safeguarding:

The Agency's safeguarding measures meet the needs of the mission; however, the Agency continues to seek advancement through innovation and use of technology while testing the current methods. The Agency is increasingly implementing metadata schema to enforce system safeguards. Improvements to these metadata systems will enable greater precision with document security practices. The Agency continues to revise and update policies and procedures to reflect modernization.

56. Security Violations:

The self-inspection affirmed that the Agency's education and training programs have developed a work force that appropriately report security violations. The Agency is a front running within the IC with respect to developing, implementing, and improving programs to enhance employee compliance with security regulations. For example, the Agency had a comprehensive program for reporting contact with foreign nationals prior to the Presidential Decision Directive 12. We continue to advance policy and procedures to inform the workforce and raise awareness.

57. Security Education and Training:

The Agency's security education and training program provides instruction for all levels and multiple aspects of safeguarding classified information, specifically adapted to our mission. The Agency's modernization has resulted in a comprehensive review of Agency training and employee development, including security education. The Agency maintains a fully developed curriculum to ensure safeguarding of classified information; essential security education is mandatory for all employees and contractors. For FY16, the Agency's web-based training for derivative classifiers will be compliant with the Americas with Disabilities Act, ensuring increased accessibility for derivative classifiers.

58. Management and Oversight:

The self-inspection continues to provide unique opportunities for CMCG to interact with personnel from all over the Agency and around the world. Travel allowed CMCG to better understand CIA's most active and sensitive programs, provide in-person guidance and training, and hear firsthand about the ways CMCG can improve support to its colleagues. CMCG will continue to improve its outreach to the Agency workforce and work with its colleagues to develop meaningful, timely solutions for every situation.

C06896750

Approved for Release: 2022/01/27 C06896750

PART G: 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.)	
59. Does agency policy require training for original classifiers?	59. ◉Yes ○No ○NA
60. Has the agency validated that this training has been received?	60. ◉Yes ○No ○NA
61. What percentage of the original classification authorities at your agency has received this training?	61. 67% ◉ Actual ○ Estimated
62. Have any waivers to this requirement been granted?	62. ○Yes ◉No ○NA
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.)	
63. Does agency policy require training for derivative classifiers?	63. ◉Yes ○No ○NA
64. Has the agency validated that this training has been received?	64. ◉Yes ○No ○NA
65. What percentage of the derivative classifiers at your agency has received this training?	65. 93% ○ Actual ◉ Estimated
66. Have any waivers to this requirement been granted?	66. ○Yes ◉No ○NA
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)	
67. Does agency policy require initial training?	67. ◉Yes ○No
68. Has the agency validated that this training has been received?	68. ◉Yes ○No
69. What percentage of cleared personnel at your agency has received this training?	69. 100% ◉ Actual ○ Estimated
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)	
70. Does agency policy require annual refresher training?	70. ◉Yes ○No
71. Has the agency validated that this training has been received?	71. ◉Yes ○No
72. What percentage of the cleared employees at your agency has received this training?	72. 93% ○ Actual ◉ 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.)	
73. Does your agency's review of classification actions evaluate if this requirement is being met?	73. ◉Yes ○No ○NA
74. What percentage of the documents sampled meet this requirement?	74. 97.8%
75. What was the number of documents reviewed for this requirement?	75. 2,614
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)	
76. Does your agency's review of classification actions evaluate if this requirement is being met?	76. ◉Yes ○No ○NA
77. What percentage of the documents sampled meet this requirement?	77. 79.4%
78. What was the number of documents reviewed for this requirement?	78. 2,614

Approved for Release: 2022/01/27 C06896750

Enclosure 2

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)	
79. Does agency policy require this critical element in the performance evaluations of personnel in the categories required by E.O. 13526?	79. ◉ Yes ○ No
80. Has the agency validated that this critical element is included in the performance evaluations of personnel in the categories required by E.O. 13526?	80. ◉ Yes ○ No
81. What percentage of such personnel at your agency has this element in their performance evaluations?	81. 100% ◉ Actual ○ Estimated
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)	
82. 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.	82. ◉Yes ○No ○NA
83. Have all delegations been limited to the minimum required based on a demonstrable and continuing need to exercise this authority?	83. ◉Yes ○No ○NA
84. If changes have been made, have they been reported, by name or position, to ISOO?	84. ◉Yes ○No ○NA
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)	
85. 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?	85. ◉Yes ○No
86. Does your agency's training for OCAs and for personnel who apply derivative classification markings cover classification challenges?	86. ◉Yes ○No
87. Does your agency's training for all other cleared personnel cover classification challenges?	87. ◉Yes ○ No
Industrial Security	
The National Industrial Security Program (NISP) was established under E.O. 12829 to safeguard Federal Government classified information that is released to contractors, licensees, and grantees (hereinafter contractors) of the United States Government. The Secretary of Defense serves as Executive Agent for inspecting and monitoring the contractors, who require or will require access to, or who store or will store classified information, and for determining the eligibility for access to classified information of contractors and their respective employees. Besides the Department of Defense (DoD), there are four other agencies that are Cognizant Security Agencies (CSAs): the Office of the Director of National Intelligence (ODNI), the Department of Energy, the Nuclear Regulatory Commission, and the Department of Homeland Security, that are authorized to provide operational oversight of their contractors. The heads of other agencies, except the Central Intelligence Agency (CIA), are required to enter into agreements with the Secretary of Defense that establish the terms of the Secretary's responsibilities on behalf of these agency heads. The ODNI may enter into an agreement with the CIA authorizing the latter to inspect and monitor contractor programs requiring access to intelligence sources and methods, including Sensitive Compartmented Information.	
88. Does your agency have contracts that require access to classified national security information (CNSI), hereinafter referred to as classified contracts?	88. ◉Yes ○ No
89. Is your agency one of the CSAs designated by E.O. 12829?	89. ○Yes ◉ No
90. If your agency issues classified contracts and is not a CSA, has it entered into an agreement with the DoD to provide industrial security services, or in the case of the ODNI, with the CIA?	90. ○Yes ○ No ◉NA
91. If your agency issues classified contracts, has your agency head designated a senior agency official for the NISP?	91. ◉Yes ○ No ○NA
92. If your agency issues classified contracts, does it provide the contractor with current security classification guidance?	92. ◉Yes ○ No ○NA
93. Are the contractor's security requirements issued through either a specific contract clause or by a Contract Security Classification Specification (DD-254)?	93. ◉Yes ○ No ○NA

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

Enclosure 2

PART H: 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.

94. 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.)	94.	2,614
95. 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.		
95 (a) Over-classification: Information does not meet the standards for classification.	95 (a)	126
95 (b) Overgraded/Undergraded: Information classified at a higher/lower level than appropriate.	95 (b)	73
95 (c) Declassification: Improper or incomplete declassification instructions or no declassification instructions.	95 (c)	90
95 (d) Duration: A shorter duration of classification would be appropriate.	95 (d)	119
95 (e) Unauthorized classifier: A classification action was taken by someone not authorized to do so	95 (e)	0
95 (f) "Classified By" line: A document does not identify the OCA or derivative classifier by name and position or by personal identifier.	95 (f)	28
95 (g) "Reason" line: An originally classified document does not cite a reason from section 1.4 of E.O. 13526.	95 (g)	0
95 (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.	95 (h)	56
95 (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.	95 (i)	20
95 (j) Marking: A document lacks overall classification markings or has improper overall classification markings.	95 (j)	959
95 (k) Portion Marking: The document lacks some or all of the required portion markings	95 (k)	2,227
95 (l) Instructions from a classification guide are not properly applied.	95 (l)	943
95 (m) Other: Unauthorized ORCON/NOFORN caveat.	95 (m)	53

PART I: Corrective Actions

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

CIA will continue to provide year-round classification training to all original and derivative classifiers. Efforts are underway to provide more web-based training and quick help videos which will be particularly helpful for officers in the field. Training for new employees will also continue and course administrators have updated the content and methods to provide a better learning experience.

CIA intends to continue development of classification guides that address current practices in all business areas. CMCG believes that guides addressing CIA's key functions will lead to better derivative citations, provide better on-demand guidance, and reinforce declassification decisions. Thorough guides will also provide a strong foundation for any future automated classification assistance tools.

Emphasis on portion marking will be a continued theme for outreach and training across the Agency. CMCG will reinforce the fact that almost all classified documents, regardless of how broad the dissemination, must be portion marked to ensure both proper protection and dissemination of information. CMCG has reiterated this in all training and outreach activities, and will continue to do so as long as necessary.

CMCG has continued to increase the number of classification experts deployed to business areas, building on the recorded success of its pilot program in FY14. CMCG has found that Agency personnel appreciate the in-person assistance these forward-deployed classification officers (FDCOs) provide and that FDCOs make significant contributions to resolving the increasing number of classification questions CMCG regularly fields.

Enclosure 2

PART J: 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.

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

CMCG built much of its FY15 self-inspection practices on successes developed during FY14, especially with travel, outreach, and data analysis. CMCG took time early in the process to revise the data collection worksheets in an effort to speed up the review process and to quickly produce data relevant to questions from ISOO and within CMCG. This effort increased production during the process of inspection, which resulted in a larger volume of documents reviewed.

Travel to the field and in-person interviews with officers has produced unique insights into how some of our operational personnel interact with classification rules, tools, and training. CMCG is careful to inform all field locations that visits are for research on how to improve CIA's classification services, and will not lead to any punitive reaction. CMCG finds that a candid demeanor leads to candid responses. CMCG is actively mining these responses and the statistical data to refine training, software, and outreach.

PART K: Explanatory Comments

98. 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.

Q28. CMCG often find that the reviewed documents cannot be easily edited to fix classification errors. However, CMCG highlights systematic errors for officers or their local classification specialists in an effort to prevent future errors.

Q34. Annual recertification of CIA's SAPs is conducted by ODNI. CIA responds to ODNI's annual data call to recertify its SAPS, which is a process separate from the annual self-inspection.

Q61. CIA just completed a modernization effort, which affected the number of staff in OCA positions during the end of the reporting period. Many staff moved from positions with OCA to newly created positions that do not yet have OCA. In FY16, CIA will reassess OCA roles in the new Agency structure and use the opportunity to ensure proper training is provided.

Q65. The reported 93% captures the Agency population within one year. This percentage may actually be higher than reported when assessing a two-year period.

Q70. CIA requires that all officers complete their derivative classifier training on an annual basis, which also serves as the annual refresher training.

Q95(h). This number represents the number of classified documents that failed to cite at least one correct CIA Security Classification Guide (SCG). Of these, 33 cited a legacy SCG, 8 incorrectly cited SCGs from other agencies, and 15 had no SCG in the classification block. CMCG further found that 751 documents failed to cite at least one correct SCG and 855 document should have cited another SCG to address all of the classified equities in the document.

Q95(k). As with previous years, CMCG found the lack of portion marking to be the greatest flaw in CIA's classification practices. CMCG found that, generally, documents intended for external readership (e.g. finished intelligence, disseminated human intelligence reporting, interagency memos, etc.) are portion marked and correctly, but documents intended for limited readership (e.g. emails, cables, spreadsheets, etc.) are not portion marked at all. The lack of portion marking is a problem with cable traffic moreso than other products. Changes to our cable preparation system will be considered as a means to solve this systematic issue.

Q95(l). This number represents the number of documents that 1) met the criteria for classification; 2) were marked as classified; 3) were classified at the correct level; and 4) had cited at least one correct CIA SCG, but were found to be missing other reasonable CIA SCGs.

For ISOO USE Only

ISOO Analyst: _____
Date QC: _____
Analyst Initials: _____