OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

Mr. Steven Aftergood
Federation of American Scientists
1725 DeSales Street NW
Suite 600
Washington, DC 20036

JAN 06 2011

Reference: DF-2011-00021

Dear Mr. Aftergood:

This is in response to your 15 November 2010 facsimile addressed to the Office of the Director of National Intelligence, wherein you requested, under the Freedom of Information Act (FOIA), **"...copies of ODNI records that document the ODNI's response to the Fundamental Classification Guidance Review to date."**

Your request was processed in accordance with the FOIA, 5 U.S.C § 552, as amended. ODNI searches resulted in the location of three documents responsive to your request. Upon review, it is determined that two documents may be released in segregable form with deletions made pursuant to FOIA Exemptions 2 and 6, 5 U.S.C. § 552 (b)(2) and (6). The remaining document must be denied in its entirety pursuant to FOIA exemptions 1, 2, 3, and 5, 5 U.S.C. § 552 (b)(1), (2), (3) and (5).

Exemption 1 protects information which is currently and properly classified in accordance with Executive Order 13526. Exemption 2 protects records that relate solely to the internal rules and practices of an agency. Exemption 3 protects information that is specifically covered by statute. In this case, the applicable statute is the National Security Act, which protects information pertaining to intelligence sources and methods. Exemption 5 protects privileged interagency or Intra-Agency information, which in this case is pre-decisional in nature. Exemption 6 protects information that would constitute a clearly unwarranted invasion of privacy.

Should you wish to appeal this determination, please do so in writing to:

Office of the Director of National Intelligence
Information Management Office
Washington, DC 20511

Appeals must be received within 45 days of the date of this letter. If you have any questions, please call the Requester Service Center at (703) 275-3642.

Sincerely,

John F. Hackett
Director, Information Management Office

Enclosure (Two Documents)

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Implementation Plan

Executive Order 13526

Classified National Security Information

Office of Primary Responsibility:
ODNI Mission Support Division
Information Management
[redacted] b2

31 December 2010

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE OF ENTRY	ENTRY MADE BY:
Initial Issuance	12/15/2010	12/15/2010	RWT/ODNI MSD/IM 12/15/2010

FOREWORD

The Office of the Director of National Intelligence (ODNI) classification management program reflects the many functions and challenges that make up the organizations of the ODNI. The program requires close cooperation among the mission, management, and support staffs, as well cooperation with external customers and support agencies. The success or failure of this agency's EO 13526 Implementation Plan will depend on the level of response from management and staff of these internal ODNI organizations.

This Implementation Plan is issued pursuant to Executive Order 13526 *"Classified National Security Information,"* Information Security Oversight Office (ISOO) Implementing Directive 1 (32 CFR Parts 2001 and 2003), ODNI Classification Guide, and ODNI Instructions 10.20, 23.01, 80.12 and 80.16. Collectively, these documents help guide ODNI management efforts in implementing policies and procedures for marking, safeguarding and declassifying ODNI information; assigning classification/declassification roles and responsibilities; training the workforce; and providing program oversight through an effective self-inspection program.

Comments relating to this Implementation Plan may be directed to Mission Support Division/Information Management. The staff of MSD/IM may be reached via email at: [redacted] or by calling [redacted] b2

b2

John F. Hackett
Director, Mission Support Division/
Information Management

INFORMATION MANAGEMENT

Contents

1. PURPOSE

This plan:

1.1 Implements the ODNI Classified National Security Information Program.

1.2 Implements the classification management elements outlined in EO 13526 and the references listed in Appendix 1.

1.3 Reiterates ODNI policy to promote commitment of leadership as well as close and continuing coordination in order to eliminate or minimize improperly marked and classified information which negatively impacts the information sharing imperative.

1.4 Outlines classification management responsibilities to various ODNI personnel and elements.

1.5 Provides direction and guidance to ODNI personnel on classification management components including security education and training, self-inspection programs, reporting requirements and ensuring authorized holders of classified information are held accountable.

2. APPLICABILITY AND SCOPE

2.1 This plan applies to all ODNI personnel who have access to and responsibilities for safeguarding, marking, processing, declassifying or destroying classified national security information, as defined in EO 13526 and EO 12951 (imagery declassification).

2.2 As used in this plan, the term "ODNI personnel" includes all ODNI components and all categories of ODNI personnel.

3. REFERENCES, DEFINITIONS, POINTS OF CONTACT AND SELF-INSPECTION GUIDE

3.1. References used in this plan are defined in Appendix 1.

3.2. Definitions used in EO 13526, the ODNI Classification Guide, this Plan and the classification management program in general, are defined in Appendix 2.

3.3. ODNI Classification Management points of contact are contained in Appendix 3.

3.4. The self-inspection guide used to assess the effectiveness of the ODNI Classification Management Program, per section 5.4(d)(4) of EO 13526 and section 2001.60 of ISOO Directive 1, is contained in Appendix 4.

4. POLICY

It is ODNI policy that:

4.1. All ODNI personnel, whether serving as an *Original Classification Authority* (OCA) or *derivative classification authority*, who create, process or handle National Security Information, shall undergo initial and periodic training to ensure information to which they have access is appropriately classified, marked, disseminated, safeguarded and, when necessary, declassified or properly destroyed, as appropriate.

4.2. ODNI OCA and derivative classifiers must be compliant with the provisions of EO 13526, the references listed in Appendix 1, this Plan, and any other provisions of law or policy governing classification management and the policies and procedures dealing with classified National Security Information.

4.3. ODNI management officials at all levels have the responsibility and authority to either directly enforce appropriate security and classification management procedures for personnel under their charge in order to ensure the protection of classified National Security Information. Questions should be referred to D/IM for guidance.

5. RESPONSIBILITIES

5.1. The Director of National Intelligence (DNI):

5.1.1. As outlined in the Order, the Director of National Intelligence or if delegated, the Principal Deputy Director of National Intelligence (PDDNI), may issue such policy directives and guidelines as deemed necessary to implement EO 13526, to the IC workforce and ODNI, with respect to the classification and declassification of all intelligence and intelligence-related information, and for access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered. Procedures or other guidance issued by other senior Staff element heads shall be in accordance with such policy directives or guidelines issued by the DNI and in accordance with directives issued by the Director of the Information Security Oversight Office (ISOO) under section 5.1(a) of EO 13526.

5.1.2. The DNI shall delegate original classification authority to ODNI personnel as deemed necessary and in accordance with the provisions of EO 13526, providing the Director, ISOO with an updated listing as changes occur.

5.1.3. Designate the Chief Management Officer as the ODNI Senior Agency Official with overall responsibility for the ODNI Classification Management Program.

5.2. The Chief Management Officer (CMO) shall:

5.2.1. As the senior agency official, exercise management oversight of the ODNI Classification Management Program and this Implementation Plan, as directed in section 5.4(d) of EO 13526.

5.2.2. Provide the resources necessary to accomplish the requirements set forth in implementing this Plan.

5.2.3. Ensure appropriate support of the Plan by all ODNI elements.

5.2.4. Assign to the Director of Information Management (D/IM), responsibility for administering the Classification Management Program, executing ODNI Self-Inspection Programs and the responsibility to serve as overall coordinator for implementing the provisions of this Plan.

5.25. Issue policy directives and guidance as deemed necessary to implement all aspects of EO 13526.

5.3. Deputy and Assistant Directors of National Intelligence (D/DNI/ A/DNI) shall:

5.3.1. Ensure all personnel under their charge follow the guidance provided in this Plan and its references.

5.3.2. Coordinate with D/IM, as required, to ensure periodic reports, required training, and reporting requirements are completed, as outlined in sections 1.3, 1.9, 5.2, 5.4 and 5.5 of EO 13526 and sections 2001.80, 2001.90 and 2001.91 of ISOO Directive 1.

5.4. The Director, Information Management Office (D/IM) shall:

5.4.1. Coordinate with the Director, ISOO, as necessary, in implementing an effective Classification Management Program throughout the ODNI.

5.4.2. Develop and maintain the ODNI Classification Guide and provide assistance in coordinating and developing other classification guides issued by ODNI Original Classification Authorities, as may be necessary, in accordance with section 2001.15 of ISOO Directive 1.

5.4.3. Update and maintain this Plan and the self-inspection guide and checklists identified in Appendix 4, ensuring changes are promptly made.

5.4.4. Establish working groups or forums, as necessary, to achieve compliance with the provisions of the EO 13526, and this Plan, in implementing classification management protocols, as required.

5.4.5. Develop, coordinate, provide and/or approve, as necessary, requisite training and education programs to ensure ODNI personnel understand classification management principles, policies, and sanctions, when access to classified National Security Information has been granted, in accordance with sections 2001.70 and 2001.71 of ISOO Directive 1.

5.4.6. Coordinate with ODNI elements to establish and maintain an internal, secure capability to receive complaints regarding over-classification and provide guidance on this issue to all ODNI personnel, as directed in section 5.4(d)(7) of EO 13526.

5.4.7. Coordinate the production of cyclic reports required by EO 13526 and section 2001.90 of ISOO Directive 1, or as directed by D/ISOO, as they pertain to classification management functions, to include, but not limited to:

5.4.7.1. Annual classification count and SF 311 report;
5.4.7.2. Annual classification management activity costs;
5.4.7.3. Annual self-inspections;
5.4.7.4 . Delegation of Original Classification Authority

5.4.8 Provide the D/ISOO copies of ODNI policies and guidance, including this Plan, no later than 23 December 2010, and updates as required.

5.4.9. Comply with other classification management functions as outlined in the references listed in Appendix 1.

5.4.10. Coordinate with the Office of the National Counterintelligence Executive/ODNI Special Security Directorate (SSD) to ensure proper maintenance and annual security reviews of ODNI special access programs and their respective classification guides, including the repository for these guides in accordance with sections 4.3(b)(2) and (4) of EO 13526 and section 2001.60(e) of ISOO Directive 1.

5.4.11. Coordinate classification challenges submitted by employees as outlined in ODNI Instruction 80.12 – *Classification of ODNI Information* and the ODNI Classification Guide, section 2.15.

5.5 The Director of Security (D/SEC) shall:

5.5.1. Develop policy and procedures for reporting, investigating and resolving security incidents and violations and ensure procedures regarding access and safeguarding are monitored and implemented in accordance with section 4.1 of EO 13526, section 2001.40-54 of ISOO Directive 1, and other ODNI policies.

5.5.2. Coordinate with the D/IM staff on classification determinations involving data spills, security incidents or violations involving classified information and required reporting to the Director, ISOO.

5.5.3. Provide D/IM relevant statistics regarding cyclic classification management reports and security violations, when requested.

5.6 The Director of Human Resources (D/HR) shall:

5.6.1 Ensure systems used to rate civilian or military personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in rating employees whose duties significantly involve the creation, processing or handling of classified information, in accordance with EO 13526, section 5.4(d)(7).

5.7. Senior Officials Delegated as Original Classification Authorities shall:

5.7.1. Ensure compliance with the provisions contained in EO 13526 and the references contained in this Plan.

5.7.2. Ensure annual training is accomplished and documented, as required by section 1.3(d) of EO 13526 and section 2001.71 of ISOO Directive 1.

5.7.3. Observe and respect existing OCA decisions and only invoke original classification when an appropriate citation cannot be identified in the ODNI classification guide, or another source document or guide, and only after consultation with D/IM, if time permits.

5.7.4. Ensure copies of all original classification decisions are provided to D/IM within 10 days of each decision, as outlined in section 2.1.1 of the ODNI Classification Guide; this ensures proper accounting and reporting to ISOO for EO 13526 compliance.

5.7.5. Avoid over-classification of information. If significant doubt exists as to whether or not information should be classified, it shall not be classified. If there is significant doubt as to the level of classification, the lower level shall be applied.

5.7.6 Challenge the classification of information that is believed to be improperly classified or unclassified in accordance with section 1.8 of EO 13526 and section 2001.14 of ISOO Directive 1, and ODNI Instruction 80.12.

5.8. Derivative Classification Authorities shall:

5.8.1. Ensure compliance with the provisions contained in EO 13526 and references contained in this Plan.

5.8.2. Ensure original classification decisions are carried forward when applying derivative classification decisions and/or markings.

5.8.3. Ensure all classified information, regardless of form, possesses an appropriate classification banner, portion markings and a classification block.

5.8.4. Ensure initial, periodic and refresher training mandated and outlined in section 2.1(d) of EO 13526 and section 2001.70 of ISOO Directive 1 is completed and documented.

5.8.5. Challenge the classification of information that is believed to be improperly classified or unclassified in accordance with section 1.8 of EO 13526 and section 2001.14 of ISOO Directive 1, and ODNI Instruction 80.12.

6. REQUIREMENTS

6.1. Commitment of Leadership

6.1.1. The ODNI is an integral part to the defense of the United States, its territories and partners around the globe. As such, a large portion of the ODNI's daily routine requires access to exceptionally sensitive information while understanding the responsibilities inherent with such access. In all cases, we must ensure information is appropriately marked and safeguarded. Accordingly, this Plan is considered essential to the ODNI mission, and shall be afforded appropriate attention at all levels. Protecting the Nation's legitimate interests through an effective and efficient classification management program is everyone's business.

6.1.2. Information Security

6.1.2.1. The potential for inadvertent or unauthorized disclosures of sensitive information continues to grow. Instant electronic communications through the internet and e-mail are powerful tools to convey information quickly and efficiently

to coworkers, superiors, subordinates, other agencies and our foreign partners. However, it also represents an instrument for adversaries to obtain information on ODNI facilities, personnel and operations that could be used against us. Key to an effective information security or information management program is commitment by all, and a robust security education, training and oversight program.

6.1.2.2. In accordance with ODNI policy, information intended for internal ODNI use must not be made available publicly without appropriate reviews of such information by the D/MSC/IM and Public Affairs Office/Internal Communication staffs.

6.2. Original Classification. The term original classification means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure. At the ODNI, several senior personnel have been delegated the authority to "originally" classify ODNI information. For the latest listing of original classification authority (OCA), see ODNI Instruction 80.16. OCAs are responsible for applying proper security classification markings as prescribed in section 1.3 of EO 13526 and section 2.3 of the ODNI Classification Guide.

6.3. Derivative Classification. Derivative classification means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification. Within the ODNI, derivative classifiers must have a security clearance, signed non-disclosure agreement and must have received initial and refresher training as prescribed by ODNI policy on the derivative classification process. Derivative classifiers are responsible for applying proper security classification markings as prescribed in section 2.1 of EO 13526 and section 2.3 of the ODNI Classification Guide.

6.4. Declassification. Declassification means the authorized change in the status of information from classified information to unclassified information. Guidance on declassifying ODNI information is contained in references (c), (d) and (e).

6.5. Safeguarding. Safeguarding means measures and controls that are prescribed to protect classified information. Within the ODNI, MSD/SECURITY is the primary office responsible for implementing processes and monitoring procedures used throughout the LX facilities in safeguarding national security information, in accordance with section 4.1, 4.2, 4.3 of EO 13526, section 2001.40-53 of ISOO Directive 1, and other ODNI procedures.

6.6. Security Violations. The term "security violation" means any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. Any suspected or known security violation occurring within the ODNI must be promptly reported to MSD/SECURITY.

6.7. Self-Inspections serve to evaluate the adherence to the principles, requirements and effectiveness of our comprehensive classification management program. See Appendix 4 for additional information, including checklists to be used in conducting annual self-inspections.

6.7.1. The D/MSC/IM shall develop and maintain a self-inspection program to ensure the ODNI classification management program is effective and in compliance with section 5.4 of EO 13526 and section 2001.60 of ISOO Directive 1.

6.7.2. Self-inspections shall be accomplished on an **annual** basis to ensure a comprehensive program and proper management controls are in place.

6.7.4. The self-inspection program shall normally be executed by ODNI Information Management Technical Officers (IMTO) and other selected classification management experts as appointed by the D/IM, and shall consist of:

6.7.4.1. Reviewing classification management functions;

6.7.4.2. Reviewing annual classification activities and reports;

6.7.4.3. Reviewing relevant security directives for currency and samples of internally generated classified information (in electronic and hard copy form) for marking compliance and feedback;

6.7.4.4. Interviewing producers and users of classified information and documenting such reviews using the self-inspection guide and forms contained in Appendix 4 of this Plan.

6.7.5. Completed self-inspection reports shall be delivered to the D/MSC/IM for consolidation and review.

6.7.6. The D/IM shall prepare a report to the Director, ISOO, as outlined in section 2001.60(f) of ISOO Directive 1, describing the results of the self-inspection.

6.8. Security Education and Training

6.8.1. EO 13526, ISOO Directive 1, ODNI Instruction 80.16, and the ODNI Classification Guide establishes OCA and derivative classification training

requirements for Senior ODNI officials and all other ODNI personnel having access to classified national security information. Managers at all levels are responsible for ensuring personnel under their control receive the minimum levels of training appropriate for their position. ODNI classification management training requirements are outlined below.

6.8.1.1. Initial Classification Training. Initial training and awareness in Classification Management principles are provided to all ODNI personnel and contractors at their entrance on duty (EOD) briefing.

6.8.1.2. Web-based training in classification management principles shall be used as needed to complement other venues for classification training.

6.8.1.3. Intermediate Level Training. Intermediate level training is provided by the D/IM staff twice per month in the form of classroom training. The briefing *"Classification Essentials"* provides personnel with an in-depth understanding of the policies relating to why we classify information along with procedural training in marking all forms of classified information.

6.8.1.4. Original Classification Authority (OCA) Training. This training is mandated by EO 13526 annually for all personnel formally designated by the DNI as Original Classification Authorities. The training is scheduled by the D/IM staff upon designation. Following completion, a report is provided to the Director, ISOO. Failure to complete this training on an annual basis may be grounds for sanctions as outlined in the Order. Sanctions include loss of classification authority and or access to classified information, as deemed appropriate after consultation with the D/IM, OGC and DNI. For more information on classification authority, refer to section 1.3(d) of EO 13526 and section 2001.71(c)(3) of ISOO Directive 1.

6.8.1.5. Derivative Classification Authority Training. Section 2.1(d) of EO 13526 mandates derivative classification training every two years. Completion is required for all ODNI personnel who are not OCAs. Failure to complete the training, when required, may result in sanctions as deemed appropriate after consultation with the D/MSC/IM, OGC and DNI.

6.8.1.6. Refresher Training is available to any ODNI element upon request to the D/IM staff. For details, contact the IM staff via Lotus Note at DNI-Classification or call 703 275-2210/2214/2205 for details.

6.8.1.7. Tailored Classification Training. Tailored/structured training sessions are also available from the D/IM staff to suit individual group or office needs. Contact the IM staff for details.

6.9. Program Assessment

6.9.1. At least once every **two years**, ODNI/MSC/IM staff will conduct a Classification Management Program Assessment for the ODNI. This review will incorporate previously completed self-assessments, classification management policies, inspection reports, and any feedback (positive and negative) received during the year. The first program assessment will be completed by December 31, 2011 or as otherwise directed.

6.9.2. The D/IM will provide an assessment report on the ODNI Classification Management Program to the CMO, and upon approval, shall make the report available on the DNI Open.gov website with copies provided to the Director, ISOO as outlined in the Order and ISOO Implementing Directive.

6.10. Reporting

6.10.1. The D/IM is responsible for internal and external reporting associated with Classification Management activities outlined in section 5.4 of this Plan. All other ODNI elements will assist the IM staff as necessary to ensure reports are accurate, timely and in compliance with the applicable governing policy or directive.

6.11. Waivers and Exceptions

6.11.1. Requests for waivers and exceptions to the requirements set forth in this plan must be in writing and sent through the appropriate chain of command to D/IM. All such requests must include at a minimum the following information:

6.11.1.1. Identification of the requirement for which the waiver or exception is being requested (i.e., annual or bi-annual training);

6.11.1.2. Reason(s) for requesting the waiver or exception;

6.11.1.3. If the request is for a waiver, the expected duration of the delay, and date that the requirement will be met;

6.11.1.4. Point of contact.

6.11.2. All waiver requests will be staffed through the D/IM who shall provide such requests to the CMO with a recommendation. Upon receipt of the CMO's decision, the employee's office staff will be notified. The CMO decision will be final.

6.11.3. Requests for waivers shall be kept to the absolute minimum and predicated on mission needs. The CMO may revoke any waiver upon a finding of abuse.

6.12 Classification Challenges

6.12.1 Authorized holders of ODNI information who believe that its classification status is improper are *encouraged and expected* to challenge the classification status of the information. Classification challenges should be submitted to the ODNI/IM for initial review and determination. Internal classification challenges should be submitted via ODNI e-mail using the DNI-Classification Lotus Notes group. The ODNI/IM is responsible for the administrative processing of classification challenges including all correspondence with the challenger. While the determination on classification is in process, the information must be protected at the current security classification level marked. See section 2.15 of the ODNI Classification Guide for additional information and procedures.

APPENDIX 1 - References

(a) Executive Order 13526, 29 December 2009 [1]

(b) Information Security Oversight Office (ISOO) Directive 1, 32 CFR Parts 2001/2003 [2]

(c) ODNI Classification Guide 2008 [3]

(d) ODNI Instruction 10.20 (ODNI Director, Information Management) [4]

(e) ODNI Instruction 80.12 (Classification of ODNI Information) [5]

(f) ODNI Instruction 80.16 (Original Classification Authority Delegation) [6]

(g) CAPCO Authorized Classification & Control Markings Register and Implementation Manual (current versions)[7]

---

[1] Available at http://www.archives.gov/federal-register/executive-orders/2009-obama.html#13526

[2] Available at http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf

[3] Available thru ODNI/IM (classified document)

[4,5,6] Available thru ODNI/IM

[7] Available through ODNI/IM or the following link: [redacted]

b7

APPENDIX 2 - Definitions

The following is a comprehensive list of terms used throughout the classification management program pursuant to EO 13526 and ODNI policies:

(a) "Access" means the ability or opportunity to gain knowledge of classified information.

(b) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) "Authorized holder" of classified information means anyone who satisfies the conditions for access stated in section 4.1(a) of EO 13526.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Automatic declassification" means the declassification of information based solely upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under this order.

(f) "Classification" means the act or process by which information is determined to be classified information.

(g) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(h) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(i) "Classified national security information" or "classified information" means information that has been determined pursuant to EO 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(j) "Compilation" means an aggregation of preexisting unclassified items of information.

(k) ''Confidential source'' means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) ''Damage to the national security'' means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(m) ''Declassification'' means the authorized change in the status of information from classified information to unclassified information.

(n) ''Declassification guide'' means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(o) ''Derivative classification'' means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(p) ''Document'' means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(q) ''Downgrading'' means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(r) ''File series'' means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(s) ''Foreign government information'' means:
(1) Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) Information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or
(3) Information received and treated as ''foreign government information'' under the terms of a predecessor order.

(t) ''Information'' means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government.

(u) ''Infraction'' means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a ''violation,'' as defined below.

(v) ''Integral file block'' means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a Presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.

(w) ''Integrity'' means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(x) ''Intelligence'' includes foreign intelligence and counterintelligence as defined by Executive Order 12333 of December 4, 1981, as amended, or by a successor order.

(y) ''Intelligence activities'' means all activities that elements of the Intelligence Communities are authorized to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.

(z) ''Intelligence Community'' means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of Executive Order 12333, as amended.

(aa) ''Mandatory declassification review'' means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

(bb) ''Multiple sources'' means two or more source documents, classification guides, or a combination of both.

(cc) "National security" means the national defense or foreign relations of the United States.

(dd) "Need-to-know" means a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(ee) "Network" means a system of two or more computers that can exchange data or information.

(ff) "Original classification" means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

(gg) "Original classification authority (ODNI)" means an individual authorized in writing, by the DNI to classify information in the first instance. See ODNI Instruction 80.16 for the current listing of ODNI OCAs.

(hh) "Records" means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(ii) "Records having permanent historical value" means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(jj) "Records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(kk) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(ll) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(mm) ''Senior agency official'' means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(nn) ''Source document'' means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(oo) ''Special Access Program'' means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

(pp) ''Systematic declassification review'' means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

(qq) ''Telecommunications'' means the preparation, transmission, or communication of information by electronic means.

(rr) ''Unauthorized disclosure'' means a communication or physical transfer of classified information to an unauthorized recipient.

(ss) ''U.S. entity'' includes:
(1) State, local, or tribal governments;
(2) State, local, and tribal law enforcement and firefighting entities;
(3) Public health and medical entities;
(4) Regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or
(5) Private sector entities serving as part of the nation's Critical Infrastructure/Key Resources.

(tt) ''Violation'' means:
(1) Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;
(2) Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or
(3) Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(uu) ''Weapons of mass destruction'' means any weapon of mass destruction as defined in 50 U.S.C. 1801(p).

APPENDIX 3 - ODNI Classification Management Points of Contact

- DNI-Classification (e-mail group through Lotus Note on CWE)
- **Information Management (IM)**

  Director:

  Chief, Information Management Branch

  Chief, Information Release Branch:

  Sr. Classification Manager

  [redacted] b2

- **Information Management Technical Officers (IMTO):**

Phone	Customers Supported (subject to change)
[redacted] b2	DDII, NCPC, Af/Pak, ADNI/CLPO
	DDII, IARPA, ADNI/CIO, ADNI/CFO
	ADNI/A&T, ADNI/PE, ADNI/SRA, PAO
	ADNI/PS, ADNI/CHCO, OIG
	NCTC
	DNI/Front Office, CMO, Executive Secretariat, OGC, OLA, NCIX, PM-ISE

APPENDIX 4 - ODNI Self-Inspection Guide - *Classification Management*

This Self-Inspection Guide serves as a tool for Information Management Technical Officers (IMTOs) and Classification Management professionals in conducting self-inspections within the ODNI. The guide covers many elements of the classification management program as highlighted in section 5.4(d)(4) of Executive Order 13526, section 2001.60 of ISOO Implementing Directive 1, the ODNI Classification Guide, and this Plan.

ELEMENTS FOR SELF-INSPECTION

A. Classification Management and Oversight
B. Security Education and Training
C. Original Classification
D. Derivative Classification
E. Marking
F. Safeguarding
G. Security Violations
H. Declassification
I. Customer Outreach and Oversight

Your job as an inspector/reviewer is to **verify** and **validate** the ODNI Classification Management Program is compliant with the Executive Order, ISOO Implementing Directive and ODNI policies regarding the elements listed above. To accomplish the self-inspection, simply review the self-inspection questions with personnel, along with samples of classified information produced within the ODNI office being reviewed, and provide comments in the applicable section.

The guide has a clean, concise, instructional format and is a unique stand-alone package providing the tools to perform a sound self-inspection. Each pertinent question should be answered and the results documented in the space provided. If clarification is needed to a Yes or No answer, use the space provided or use additional paper as required. At the end of each element, there are three summary questions that should also be answered. They are: **Observations, Deficiencies, and Action Taken.**

In the "**Observation**" section, the reviewer should include **positive** and **negative** observations. A **positive** observation might be "portion marking is consistently being applied based on a review of 25 sample documents produced within XYZ office." A **negative** observation might be "four personnel did not attend required training and there is no evidence of a training waiver being submitted or approved."

In the "**Deficiencies/Action Taken**" sections, the reviewer should state any deficiencies uncovered and what corrective action was being taken or will be taken.

Refer questions to the IM staff via [redacted] or by calling [redacted]. 62
[redacted] Submit completed checklists to the D/IM when completed.

Upon receipt/review of the self-inspection checklists, the D/IM shall prepare a report to the Director, ISOO as outlined in section 5.4.7 of this Plan and monitor corrective actions as necessary.

SELF-INSPECTION PROGRAM CHECKLIST– *Classification Management*

ODNI Element Being Reviewed: _____ **Date(s) of Self-Inspection:** _____

Element Point of Contact/Phone #: _____

IMTO Self-Inspector/Reviewer Name/Phone: _____

A. Classification Management & Oversight

1. Are policies in effect to guide ODNI personnel in properly marking classified information? (if yes, list them)

   YES / NO _____

2. Are procedures in place to address classification challenges?

   YES / NO _____

3. Are procedures in place to address marking abuses and/or over-classification?

   YES / NO _____

4. Are annual reviews in place for special access programs?

   YES / NO _____

5. Are there secure capabilities and guidance in place to receive and process information, allegations or complaints regarding over-classification or incorrect classification?

   YES / NO _____

6. Are systems used to rate civilian and military personnel performance in place for management of classified information as a critical element to be evaluated?

   YES / NO _____

   Observations: _____

   _____

   Deficiencies: _____

   Corrective Action Required (YES / NO) (if YES, provide completion date): _____

   _____

B. Security Education and Training

1. Is Classification training routinely provided to ODNI personnel?

   YES / NO _____

2. Is the training available to all employees and does it comply with EO 13526 and ISOO Directive 1?

   YES / NO _____

3. Does the ODNI classification training program include initial, cyclic and refresher training?

   YES / NO _____

4. Does the training outline specific sanctions that may be imposed for abuses in classifying information to include over-classification?

   YES / NO _____

5. Has the ODNI established internal procedures that ensure personnel are aware of their responsibilities for classifying national security information?

   YES / NO _____

6. Are Original Classification Authorities (OCA) provided annual training and is the training documented?

   YES / NO _____

7. Are ODNI personnel aware of sanctions that may be imposed against personnel who violate classification management policies?

   YES / NO _____

8. Are resources in place to assist personnel in classification matters?

   YES / NO _____

Observations: _____

_____

Deficiencies: _____

_____

Corrective Action Required (YES / NO) (if YES, provide completion date): _____

C. Original Classification:

1. Does the ODNI have an updated/approved list of personnel delegated as Original Classification Authorities (OCA)?

   YES / NO _____

2. Does the OCA delegation and training conform to the requirements set forth in EO 13526?

   YES / NO _____

3. Is the OCA training documented?

   YES / NO _____

4. Is the list of OCA delegations provided to ISOO in a timely manner?

   YES / NO _____

5. Have there been any documented abuses or challenges regarding OCA decisions? (If yes, explain the circumstances and outcome)

   YES / NO _____

   Observations: _____

   _____

   Deficiencies: _____

   _____

   _____

   Corrective Action Required (YES / NO) (if YES, provide completion date): _____

   _____

D. Derivative Classification:

1. Does the ODNI outline the requirements for derivative classification authority?

   YES / NO _____

2. Has the ODNI developed training for derivative classifiers?

   YES / NO _____

3. Is the training current and is it documented?

   YES / NO _____

4. Are derivative classification markings compliant with the EO and IC marking policy?

   YES / NO _____

5. Are resources in place to resolve questions concerning derivative classification marking issues?

   YES / NO _____

Observations: _____

_____

Deficiencies: _____

_____

_____

Corrective Action Required (YES / NO) (if YES, provide completion date): _____

_____

_____

E. Markings

1. Are procedures in place to properly mark classified information and are they being followed?

   YES / NO _____

2. Are procedures in place to assist personnel who have problems in applying authorized markings?

   YES / NO _____

3. Do classification banners and portion marking protocols conform to IC policy, as outlined in the CAPCO Markings Register and Implementation Manual?

   YES / NO _____

4. Does the ODNI Classification Guide convey updated markings to be used with classified information?

   YES / NO _____

5. Are classification and control markings applied to information as outlined in the CAPCO Register and Implementation Manual?

   YES / NO _____

6. Has the ODNI undergone any internal or external inspections or reviews in the area of classification management?

   YES / NO _____

7. If yes, were the results of the review made available to personnel either in document form or through training presentations?

   YES / NO _____

8. Are brochures or other training aids produced and disseminated to the work force to remind personnel of the importance of accurately marking classified information?

   YES / NO _____

   Observations: _____

   _____

   Deficiencies: _____

   _____

   Corrective Action Required (YES / NO) (if YES, provide completion date): _____

F. Safeguarding

1. Are there written policies and procedures in place to safeguard classified information? If yes, please list.

   YES / NO_____

   _____

2. Are modifications and/or improvements to the facility made with MSC/SEC concurrence?

   YES / NO_____

3. Are personnel provided information explaining the procedures in place for safeguarding and destroying classified information?

   YES / NO _____

4. Are abuses to safeguarding classified information promptly reported to MSC/SEC and/or management for action?

   YES / NO _____

   _____

   Observations: _____

   _____

   Deficiencies: _____

   _____

   Corrective Action Required (YES / NO) (if YES, provide completion date): _____

   _____

   _____

G. Security Violations:

1. Are there policies and procedures in place to guide ODNI personnel in reporting security violations?

   YES / NO _____

2. Are violations and/or incidents promptly investigated?

   YES / NO _____

3. Are personnel who commit security violations held accountable and appropriate refresher training provided and documented?

   YES / NO _____

4. Does the ODNI Security staff coordinate with ISSM and IM staffs in resolving security incidents/violations?

   YES / NO _____

5. Are security violations report to ISOO, as required by reference section 5.5 of the Order?

   YES / NO _____

Observations: _____

_____

_____

Deficiencies: _____

_____

Corrective Action Required (YES / NO) (if YES, provide completion date): _____

_____

_____

H. Declassification Procedures

1. Are there written procedures in place to declassify ODNI information?

   YES / NO _____

2. Is classified ODNI information assigned a declassification instruction as required by EO 13526?

   YES / NO _____

3. Is appropriately declassified ODNI information made available to the public in accordance with local policy?

   YES / NO _____

4. Does the ODNI Classification Guide clearly state the limitations imposed by EO 13526 regarding the automatic declassification of information after 25 or 50 years unless an exemption has been approved?

   YES / NO _____

5. Do OCA delegation instructions provide clearly defined roles for who can declassify ODNI information?

   YES / NO _____

6. Does the ODNI have an approved declassification guide?

   YES / NO _____

Observations: _____

_____

_____

Deficiencies: _____

_____

Corrective Action Required (YES / NO) (if YES, provide completion date): _____

_____

_____

SELF-INSPECTION PROGRAM CHECKLIST– *Classification Management*

ODNI Element Being Reviewed: _____ **Date(s) of Self-Inspection:** _____

Element Point of Contact/Phone #: _____

IMTO Self-Inspector/Reviewer Name/Phone: _____

I. Customer Outreach and Oversight

1. Is the customer aware of policies to guide personnel in properly marking classified information? (if yes, list them)

   YES / NO _____

2. Is the customer aware of any procedures in place to address classification marking issues?

   YES / NO _____

3. Is the customer aware of any procedures in place to address classification challenges or marking abuses?

   YES / NO _____

4. Is the customer satisfied with the classification training available to them?

   YES / NO _____

5. Do classified documents/information originating from the customer contain a classification banner, portion marking and classification block, as required by EO 13526 and the ODNI Classification Guide?

   YES / NO _____

6. Has the customer expressed any additional concerns about the ODNI classification management program?

   YES / NO _____

Observations: _____

_____

Deficiencies: _____

_____

Corrective Action Required (YES / NO) (if YES, provide completion date): _____

Date Completed: _____