

ISOO HANDBOOK 2019-01: This guidance document does not have the force and effect of law and is not meant to bind the public, except as authorized by law or regulation or as incorporated into a contract. Accordingly, with regard to the public, this document only provides clarity regarding existing requirements under the law or agency policies. This guidance document is binding on agency actions as authorized under applicable statute, executive order, regulation, or similar authority.

Responsibilities of the Senior Agency Official (SAO)

This pamphlet contains excerpts from
E.O. 13526, *Classified National Security Information*,
and
32 CFR part 2001, *Classified National Security Information*,
that detail the specific duties and responsibilities of the
Senior Agency Official.

July 2018

Information Security Oversight Office

General Responsibilities of the Senior Agency Official

E.O. 13526, Sec. 5.4(d) General Responsibilities

Heads of agencies that originate or handle classified information shall designate a senior agency official to direct and administer the program, whose responsibilities shall include:

- (1) overseeing the agency's program established under this order, provided an agency head may designate a separate official to oversee special access programs authorized under this order.
- (2) promulgating implementing regulations, which shall be published in the *Federal Register* to the extent that they affect members of the public;
- (3) establishing and maintaining security education and training programs;
- (4) establishing and maintaining an ongoing self-inspection program, which shall include the regular reviews of representative samples of the agency's original and derivative classification actions, and shall authorize appropriate agency officials to correct misclassification actions not covered by sections 1.7(c) and 1.7(d) of this order; and reporting annually to the Director of the Information Security Oversight Office on the agency's self-inspection program;
- (5) establishing procedures consistent with directives issued pursuant to this order to prevent unnecessary access to classified information, including procedures that:
 - (A) require that a need for access to classified information be established before initiating administrative clearance procedures; and
 - (B) ensure that the number of persons granted access to classified information meets the mission needs of the agency while also satisfying operational and security requirements and needs;
- (6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;
- (7) ensuring that the performance contract or other system 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 the rating of:
 - (A) original classification authorities;
 - (B) security managers or security specialists; and
 - (C) all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings;
- (8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication;
- (9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function; and
- (10) establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper classification as needed.

Access by Historical Researchers and Certain Government Personnel

E.O. 13526, Sec. 4.4 Access by Historical Researchers and Certain Former Government Personnel

(a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

- (1) are engaged in historical research projects;
- (2) previously have occupied senior policy-making positions to which they were appointed or designated by the President or the Vice President; or
- (3) served as President or Vice President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of the national security:

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees or designees and Vice Presidential appointees or designees to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

Automatic Declassification

E.O. 13526, Sec. 3.3 Automatic Declassification

(j) At least 1 year before information is subject to automatic declassification, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office of any specific information that the agency proposes to exempt from automatic declassification under paragraphs (b) and (h) of this section.

32 CFR 2001.30 Automatic declassification

(n) *Delays in the onset of automatic declassification*

(1) *Media that make a review for possible declassification exemptions more difficult or costly.* An agency head or senior agency official shall consult with Director of the NDC before delaying automatic declassification for up to five years for classified information contained in media that make a review for possible declassification more difficult or costly.

Classification Challenges

E.O. 13526, Sec. 1.8 *Classification Challenges*

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official 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.

Classification Guides

E.O. 13526, Sec. 2.2 *Classification Guides*

(b)(1) Each guide shall be approved personally and in writing by an official who has program or supervisory responsibility over the information or is the senior agency official.

Classification Markings

32 CFR 2001.24 *Portion marking waivers*

(k) *Portion marking waivers.*

(1) An agency head or senior agency official may request a waiver from the portion marking requirement for a specific category of information.

Classification Prohibitions and Limitations

32 CFR 2001.13 *Classification prohibitions and limitations*

(a) *Declassification without proper authority.* Classified information that has been declassified without proper authority, as determined by an original classification authority with jurisdiction over the information, remains classified and administrative action shall be taken to restore markings and controls, as appropriate. All such determinations shall be reported to the senior agency official who shall promptly provide a written report to the Director of ISOO.

(b) *Reclassification after declassification and release to the public under proper authority.*

(5) Once the reclassification action has occurred, it must be reported to the National Security Advisor and to the Director of ISOO by the agency head or senior agency official within 30 days.

Declassification Authority

E.O. 13526, Sec. 3.1 *Authority for Declassification*

(b)(4) Information shall be declassified or downgraded by...officials delegated declassification authority in writing by the agency head or the senior agency official of the originating agency.

Declassification Guides

32 CFR 2001.32 *Declassification guides*

(b) *General content of declassification guides.* Declassification guides shall:

(1) Be submitted by the agency head or the designated senior agency official.

Fundamental Classification Guidance Review

32 CFR 2001.16 Fundamental classification guidance review

(c) *Participation in reviews.* The agency head or senior agency official shall direct the conduct of a fundamental classification guidance review and shall ensure the appropriate agency subject matter experts participate to obtain the broadest possible range of perspectives.

General Restrictions on Access

E.O. 13526, Sec. 4.1 General Restrictions on Access

(f) Consistent with law, executive orders, directives, and regulations, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information:

(1) prevent access by unauthorized persons;

(2) ensure the integrity of the information; and

(3) to the maximum extent practicable, use;

(A) common information technology standards, protocols, and interfaces that maximizes the availability of, and access to, the information in a form and manner that facilitates its authorized use; and

(B) standardized electronic formats to maximize the accessibility of information to persons who meet the criteria set forth in section 4.1(a) of this order.

(g) Consistent with law, executive orders, directives, and regulations, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

Loss, Possible Compromise or Unauthorized Disclosure

32 CFR 2001.48 Loss, possible compromise or unauthorized disclosure

(d) *Reports to ISOO.* In accordance with section 5.5(e)(2) or the Order, agency heads or senior agency officials shall notify the Director of ISOO when a violation occurs under paragraphs 5.5(b)(1), (2), or (3) of the Order that:

(1) is reported to oversight committees in the Legislative branch;

(2) may attract significant public attention;

(3) involves large amounts of classified information; or

(4) reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

Original Classification Authority

E.O. 13526, Sec. 1.3 Classification Authority

(c)(3) “Secret” or “Confidential” original classification authority may be delegated only by the President, the Vice President, an agency head or official designated pursuant to paragraph (s)(2) of this section, or the senior agency official designated under section 5.4(d) of this order, provided that official has been delegated “Top Secret” original classification authority by the agency head.

(d) Original classification authorities who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the agency head or the senior agency official designated under section 5.4(d) of this order until such training has taken place. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances.

32 CFR 2001.11 Original classification authority

(c) *Reporting delegations of original classification authority.* All delegations of original classification authority shall be reported to the Director of ISOO. This can be accomplished by an initial submission followed by updates on a frequency determined by the senior agency official, but at least annually.

Reporting Requirements

E.O. 13526, Sec. 5.4 General Responsibilities

(d)(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication

32 CFR 2001.90 Agency annual reporting requirements

(c) *Accounting for costs*

(1) Information on the costs associated with the implementation of the Order will be collected from the agencies. The agencies will provide data to ISOO on the costs estimates for classification-related activities. ISOO will report these cost estimates annually to the President. The senior agency official should work closely with the agency comptroller to ensure that the best estimates are collected.

32 CFR 2001.91 Other agency reporting requirements

(d) *Violations of the Order.* Agency heads or senior agency officials shall notify the Director of ISOO when a violation occurs under sections 5.5(b)(1), (2), or (3) of the Order and §2001.48(d).

Sanctions

E.O. 13526, Sec. 5.5 *Sanctions*

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of the order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3) of this section occur.

Security Education and Training

E.O. 13526, Sec. 5.4 *General Responsibilities*

(d)(3) establishing and maintaining security education and training programs.

32 CFR 2001.70 *Security Education and Training - General*

(b) *Responsibility.* The senior agency official is responsible for the agency's security education and training program. The senior agency official shall designate agency personnel, as necessary, to assist in carrying out this responsibility.

32 CFR 2001.71 *Security Education and Training - Coverage*

(c) *Training for original classification authorities.*

(3) Original classification authorities who do not receive such mandatory training at least once within a calendar shall have their classification authority suspended until such training has taken place.

(i) An agency head, deputy agency head, or senior agency official may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers shall be documented.

(d) *Training for persons who apply derivative classification markings.*

(3) Derivative classifiers who do not receive such mandatory training at least once every two years shall have their authority to apply derivative classification markings suspended until they have received such training.

(i) An agency head, deputy agency head, or senior agency official may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers shall be documented.

E.O. 13526, Sec. 5.4(d) General Responsibilities

(4) establishing and maintaining an ongoing self-inspection program, which shall include the regular reviews of representative samples of the agency's original and derivative classification actions, and shall authorize appropriate agency officials to correct misclassification actions not covered by sections 1.7(c) and 1.7(d) of this order; and reporting annually to the Director of the Information Security Oversight Office on the agency's self-inspection program

32 CFR 2001.60 Self-inspections

(b) *Responsibility.* The senior agency official is responsible for directing and administering the agency's self-inspection program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(c) *Approach.* The senior agency official shall determine the means and methods for the conduct of self-inspections.

(2) In accordance with section 5.4(d)(4) of the Order, the senior agency official shall authorize appropriate agency officials to correct misclassification actions.

(d) *Frequency.* Self-inspections shall be regular, ongoing, and conducted at least annually with the senior agency official setting the frequency on the basis of program needs and the degree of classification activity.

(e) *Coverage.* The senior agency official shall establish self-inspection coverage requirements based on program and policy needs.

(f) *Reporting.*

(1) *Internal.* The senior agency official shall set the format for documenting self-inspection findings.

(2) *External.* The senior agency official shall report annually to the Director of ISOO on the agency's self-inspection program.