NSA/CSS POLICY 1-52
CLASSIFIED NATIONAL SECURITY INFORMATION

DATE:	4 September 2019 (See Document History)
OFFICE OF PRIMARY INTEREST:	Information Security/Classification, 972-2534s
RELEASABILITY:	NSA/CSS Policy 1-52 is approved for public release. The official document is available on the Office of Policy (P12) website ("go policy").
AUTHORITY:	Michael S. Rogers, Admiral, U.S. Navy, Director, NSA/Chief, CSS
ISSUED:	31 August 2017

PURPOSE AND SCOPE

1. This document establishes policy and assigns responsibilities for *classifying*, *safeguarding*, and *declassifying* NSA/CSS *classified national security information*, pursuant to References a–i. This policy does not address *controlled unclassified information* or *information* classified under the Atomic Energy Act of 1954, as Amended (Public Law 83-703) (Reference j).

2. The companion manual to this policy, NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Guide" (Reference k), describes in detail the fundamental procedures critical for protecting and accessing NSA/CSS classified national security information.

3. This policy applies to all NSA/CSS elements and *affiliates*.

POLICY

4. NSA/CSS information that has been determined, pursuant to Executive Order 13526, "Classified National Security Information" (Reference a), or any predecessor order, to require protection against *unauthorized disclosure*, shall be classified, marked, safeguarded, and declassified in accordance with the provisions included in References a–i.

5. NSA/CSS information shall be originally classified only in accordance with Section 1.1. of Executive Order 13526 (Reference a). If there is significant doubt as to whether identifiable or describable damage to the national security could occur by originally classifying specific NSA/CSS information, then it shall not be classified. If there is significant doubt as to the level of damage to the national security that could be incurred (i.e., damage [CONFIDENTIAL], serious damage [SECRET], or exceptionally grave damage [TOP SECRET]), then the information shall be originally classified at the lower level. NSA/CSS

information shall be *downgraded* as applicable and declassified when it no longer qualifies for classification because of a determination that disclosure of the information would no longer damage national security.

6. In accordance with Executive Order 13526 (Reference a), the Director, NSA/Chief, CSS (DIRNSA/CHCSS) and other officials within NSA/CSS are specifically identified by position title as having the authority to determine the *original classification* for information; this position title is *Original Classification Authority (OCA)*. This authority shall be delegated only to officials who have a demonstrable and continuing need to exercise such authority and shall be limited to the minimum number required for the effective operation of NSA/CSS. In the absence of an OCA, a person who is appropriately trained and designated in writing to act on the OCA's behalf may exercise this authority. NSA/CSS OCAs also act as the *Declassification Authority* for information under their purview.

7. Failure to comply with this policy may be a violation of the terms imposed by a nondisclosure agreement pertaining to NSA/CSS activities and Federal law, and may lead to civil, administrative, and/or criminal sanctions. Such noncompliance shall be immediately reported to Security and Counterintelligence (S&CI, A5) for review and, as appropriate, investigation.

PROCEDURES

8. NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Guide" (Reference k and successor versions), describes in detail the procedures for classifying, safeguarding, and declassifying NSA/CSS classified national security information pursuant to Executive Order 13526 (Reference a); Intelligence Community Directive (ICD) 700, "Protection of National Intelligence" (Reference d); ICD 710, "Classification and Control Markings System" (Reference e); Department of Defense (DoD) Manual 5200.01, Vols. 1–3 (References f–h); Executive Order 12333, "United States Intelligence Activities," as amended (Reference l); and DoD Directive 5100.20, "The National Security Agency and Central Security Service" (Reference m). Additional intelligence community (IC) procedural guidance is available in ICD 710 (Reference e). Additional DoD procedural guidance is available in DoD Manual 5200.01, Vols. 1–3 (References f–h).

RESPONSIBILITIES

Director, NSA/Chief, CSS (DIRNSA/CHCSS)

9. Director, NSA/Chief, CSS (DIRNSA/CHCSS) shall:

a. Ensure that Agency Original Classification Authorities (OCAs) have a demonstrable and continuing need to exercise original classification authority;

b. Approve in writing requests to appropriate higher level authorities for *reclassifying* NSA/CSS information that has been declassified and released to the public under proper authority;

c. Authorize or delegate the authority to authorize the disclosure of *classified information* in *emergency situations* to individuals who are otherwise not eligible to receive the information;

d. Designate a *Senior Agency Official* to direct and administer NSA/CSS' *information security* program; and

e. Designate a senior official to be responsible for overseeing *Special-Access Programs* and *Controlled Access Programs* within NSA/CSS (see NSA/CSS Policy 1-41, "Programs for the Protection of Especially Sensitive Classified Information" (Reference n).

Chief, Policy, Information, Performance, and Exports (PIPE, P1), as the Senior Agency Official

10. The Chief, Policy, Information, Performance, and Exports (PIPE, P1) as the Senior Agency Official shall:

a. Perform the functions of component Senior Agency Official as outlined in Executive Order 13526; "Information Security Oversight Office (ISOO) Implementing Directive for Executive Order 13526, 32 Code of Federal Regulations Parts 2001 and 2003"; and DoD Manual 5200.01, Volumes 1 and 3 (References a, b, f, and h);

b. Serve as the NSA/CSS senior classification authority for classification and declassification guidance;

c. Grant, when appropriate, waivers to original and *derivative classification* training requirements;

d. Provide the final NSA/CSS determination regarding classification challenges. Inform the complainant of any right to appeal the decision to the Interagency Security Classification Appeals Panel and the procedures for such an appeal; and

e. Remove original or derivative classification authority from those who show reckless disregard or a pattern of errors in applying the standards contained in References a–i or who have not received the required training. Notify the ISOO of violations as required in Section 5.5 of Executive Order 13526 (Reference a). Approve temporary waivers to the training requirements, as necessary.

Chief, Policy, Information, Performance, and Exports (PIPE, P1)

11. The Chief, Policy, Information, Performance, and Exports (PIPE, P1) shall:

a. Establish uniform information security policies and procedures to ensure proper protection, handling, storage, and dissemination of all national security information under NSA/CSS purview or control;

b. Act as the NSA/CSS point of contact for all classification matters with the IC, DoD, and other departments or agencies, except for those addressed in Policy 1-41 (Reference n; see paragraph 19);

c. Interpret decisions concerning information security made by DIRNSA/CHCSS, the National Security Council, ISOO, the Secretary of Defense, the Office of the Director of National Intelligence (ODNI), and others as appropriate;

d. Establish and maintain classification and declassification policy in coordination with appropriate NSA/CSS stakeholder organizations to meet the information security needs of NSA/CSS;

e. Establish controls and procedures to ensure that classified information is accessible to the maximum extent possible by individuals who meet the criteria set forth in Section 4.1(a) of Executive Order 13526 (Reference a) in coordination with other appropriate NSA/CSS organizations with cognizance over or an equity in the information;

f. Oversee, in coordination with the Deputy Chief Information Officer (Y), policies to require that classified information on information technology systems is collected, created, marked, used, communicated, computed, disseminated, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized individuals;

g. Establish and maintain NSA/CSS' ongoing information security *self-inspection* program;

h. Maintain and publish the list of authorized NSA/CSS OCAs;

i. Provide initial training to new OCAs prior to their exercising OCA responsibilities. This training shall cover, at a minimum, classification/declassification standards, classification levels, classification/declassification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, *classification guides*, and information sharing;

j. Provide mandatory follow-up training in proper classification and declassification procedures at least once a calendar year to all OCAs;

k. Review for consistency all NSA/CSS classification and declassification proposals before they are forwarded to the appropriate OCA or Declassification Authority for decision. This review responsibility may be exercised by either the Chief, P1 or the Deputy Chief, P1;

l. Serve as OCA for elements that do not have resident OCAs;

m. Develop and maintain classification and *declassification guides* and ensure that original classification decisions are incorporated into classification guides on a timely basis in conjunction with appropriate NSA/CSS organizations. Publish guidance as necessary;

n. Establish procedures and conduct comprehensive evaluations to ensure that classification guides are regularly reviewed and updated at least once every 5 years;

o. Conduct the fundamental classification guidance review;

p. Establish and maintain the *Classification Advisory Officer (CAO) Program*;

q. Provide corporate-level CAO support as requested by organizations with no available registered CAOs;

r. Establish and maintain an information security education and training program for all Agency affiliates in collaboration with the National Cryptologic School (A2). Address compliance as required by the Undersecretary of Defense for Intelligence (Reference o);

s. Respond appropriately to requests for information, requirements, tasking, etc. from external organizations (e.g., the Secretary of Defense, the ODNI, ISOO, and the Interagency Security Classification Appeals Panel);

t. Ensure prompt and appropriate responses to requests, appeals, challenges, complaints, and suggestions about NSA/CSS' information security program and policy;

u. Establish procedures to resolve allegations or complaints regarding incorrect classification at NSA/CSS. (Policy Manual 1-52 (Reference k) documents procedures for classification and marking challenges.); and

v. Notify S&CI (A5) of any known or suspected unauthorized disclosure and/or compromise of classified information. Coordinate with S&CI (A5) in reporting security incidents involving the disclosure or compromise of classified information to appropriate higher level authorities. Additionally, notify the Cryptologic Disclosures Action Group of any known or suspected unauthorized disclosure of NSA/CSS classified equities in accordance with NSA/CSS Policy 1-27, "Identifying, Investigating and Reporting Unauthorized Media Disclosures of NSA/CSS Classified Information" (Reference p).

NSA/CSS Original Classification Authorities (OCAs)

12. NSA/CSS Original Classification Authorities (OCAs) shall:

a. Certify in writing to the NSA/CSS Senior Agency Official before initially exercising OCA authority and annually thereafter that they have received training that covers the fundamentals of proper security classification and declassification, the limits of their authority, the sanctions that may be imposed, and OCA duties and

responsibilities, as described in paragraph 11.i. above. OCAs who do not receive such mandatory training at least once every calendar year shall have their original classification authority suspended;

b. Establish classification and declassification guidance for the information, systems, plans, programs, projects, or missions involving NSA/CSS information over which they have program or management responsibility;

c. Validate, update, or cancel the classification and declassification guides under their purview at least every 5 years or when directed as part of a fundamental classification guidance review to ensure that the guidance is current and accurate;

d. Acknowledge decisions of classification determinations within 30 days of request;

e. Raise or lower the classification level of or declassify NSA/CSS information under their purview as appropriate. For declassification decisions, determine whether public interest in disclosing information outweighs the damage to the national security that might reasonably be expected from the disclosure of such information;

f. Recommend to DIRNSA/CHCSS, as appropriate, the reclassification of information that has been declassified and released to the public under proper authority;

g. Coordinate with the Chief, P1 or Deputy Chief, P1 before making any original classification or declassification decisions. In a time-sensitive emergency situation, the OCA will advise P1 after the fact and complete any required records; and

h. Document all classification/declassification decisions in writing, e.g., in the form of classification guidance, memorandum, or other formal document.

NSA/CSS Classification Advisory Officers (CAOs)

13. NSA/CSS Classification Advisory Officers (CAOs) shall:

a. Meet all qualifications and training requirements;

b. Serve as their organizations' subject matter experts (SMEs) in the proper application of classification policy and marking mechanics, consulting other CAOs, SMEs, and Information Security/Classification (P131) personnel as necessary;

c. Assist in the development of classification and declassification guidance;

d. Upon request from any NSA/CSS affiliate, perform initial classification reviews of NSA/CSS information intended for public release per NSA/CSS Policy 1-30, "Review of NSA/CSS Information Intended for Public Release" (Reference q);

e. Be knowledgeable about and assist others with the prepublication review process as set forth in NSA/CSS Policy 1-30 (Reference q);

f. Coordinate any organizational classification–related issues with P131;

g. Assess organizational classification–related training needs and coordinate with P131 to provide these training needs;

h. As directed by P131, participate in the NSA/CSS Self-Inspection Program;

i. Provide classification determinations as part of the NSA/CSS Classification Challenge process;

j. Be knowledgeable about NSA/CSS, DoD, and IC policies governing information security and classification;

k. Maintain records of their classification review responses for the duration of their CAO assignment;

l. Complete refresher training at least once every 5 years; and

m. Perform other duties as described in the "Memorandum on the NSA/CSS Classification Advisory Officer Program" (Reference r).

NSA/CSS Enterprise Leaders

14. The NSA/CSS *Enterprise Leaders* shall:

a. Establish procedures within their individual organizations to facilitate information sharing, in accordance with NSA/CSS Policy 11-1, "Information Sharing" (Reference s), while ensuring that access to classified information is limited to appropriately cleared personnel with a valid *need-to-know* (References a and f);

b. Establish CAO positions at appropriate organizational levels and in sufficient numbers to afford all members of their respective workforces ready access to necessary classification services;

c. Ensure that all employees under their authority receive mandatory information security training;

d. Ensure that all employees under their authority comply with the requirements of this policy and other relevant guidance; and

e. Develop and maintain classification and declassification guidance and ensure that original classification decisions are incorporated into classification guidance on a timely basis, in coordination with P1.

NSA/CSS Inspector General

15. The NSA/CSS Inspector General shall carry out audits and other evaluations as required by Public Law 111-258, "Reducing Over-Classification Act" (Reference c).

Chief, Security and Counterintelligence (S&CI, A5)

16. The Chief, Security and Counterintelligence (S&CI, A5) shall:

a. Review and, as appropriate, investigate instances of noncompliance with this policy that may constitute a security violation, in accordance with NSA/CSS Policy 5-2, "Security Investigations" (Reference t);

b. Coordinate with the Capabilities Director (Y) to resolve any incidents involving unauthorized access, compromise, or *data spills* of classified information residing in information systems, in accordance with NSA/CSS Policy 6-23, "Reporting and Handling of NSA/CSS Information System Security Incidents" (Reference u), to resolve the incident; and

c. Report, in coordination with P1, security incidents involving the disclosure or compromise of classified information to appropriate higher level authorities and coordinate damage assessments specific to the compromise of classified information as appropriate. Additionally, notify the Cryptologic Disclosures Action Group of any known or suspected unauthorized disclosure of NSA/CSS classified equities in accordance with NSA/CSS Policy 1-27 (Reference p).

Chief, Education and Training (A2)

17. The Chief, Education and Training (A2) shall collaborate with P1 to develop and deliver mandatory and discretionary information security courses.

Capabilities Director (Y)

18. The Capabilities Director (Y) shall:

a. Establish, with information owners, uniform procedures that provide adequate protection to ensure automated information systems that collect, create, mark, use, communicate, compute, disseminate, process, store, reproduce, transmit, or destroy classified information:

1) Prevent access by unauthorized persons;

2) Ensure the integrity of the information; and

3) Use common standards and formats to maximize the availability of information to authorized users;

b. Provide, when feasible, an automated classification tool for NSA/CSS Enterprise Solutions–approved email client and standard office automation applications to assist the users with protecting information. (It remains the responsibility of the user to ensure that the information is properly marked and safeguarded.); and

c. Notify S&CI (A5) of any incidents involving unauthorized access, compromise, or data spills of classified information resident in information systems, and coordinate with S&CI (A5), in accordance with NSA/CSS Policy 6-23 (Reference u), to resolve the incident.

Operations Mission Support Office

19. The Operations Mission Support Office shall oversee the programs identified in Policy 1-41 (Reference n).

NSA/CSS Civilian and Military Personnel

20. All NSA/CSS civilian and military personnel shall complete annual information security training. Civilian, military, contractor, and integree personnel working within NSA/CSS spaces and performing NSA/CSS mission, but not assigned to NSA/CSS, are encouraged but not required to receive this training.

Individuals Applying Derivative Classifications Markings

21. Individuals applying derivative classification markings shall:

a. Observe and respect the classification determinations made by OCAs;

b. Use only authorized sources to make derivative classification decisions, including classification guidance, memorandums, or other formal documents issued by an OCA;

c. Explicitly and uniformly apply classification and control markings when creating, disseminating, or using classified NSA/CSS information to maximize information sharing while protecting sources, methods, and activities from unauthorized or unintentional disclosure;

d. Determine appropriate classification markings for the NSA/CSS information that they produce, and apply appropriate control markings that correctly implement DoD and ODNI guidelines for dissemination;

e. Portion-mark all NSA/CSS documents that contain NSA/CSS information requiring control markings, regardless of classification, format, or medium in accordance with applicable DoD and ODNI standards;

f. Include a classification authority block on information that the individual derivatively classifies, regardless of format or media. This block must include a statement that appropriately identifies the individual as the derivative classifier of the information; and

g. Take all appropriate and reasonable steps, including consulting classification guidance, requesting assistance from P1, or soliciting guidance from the appropriate OCA(s) or CAO(s) when classification appears to be inconsistently or incorrectly applied. In cases of apparent conflict between classification guidance and a classified source document regarding a discrete item of information, the instructions in the classification guidance shall take precedence.

Supervisors of all Civilian Personnel whose Duties Include Significant Involvement with Creating or Handling Classified Information

22. Supervisors of all civilian personnel whose duties include significant involvement with creating or handling classified information shall:

a. Include in the performance assessment of these individuals an evaluation of their marking and management of classified information; and

b. Ensure and verify completion of mandatory training. Preclude access to classified systems and networks by noncompliant affiliates (Reference o).

Authorized Holders of NSA/CSS Information

23. All authorized holders of NSA/CSS information shall:

a. Be held personally and individually responsible for properly safeguarding NSA/CSS classified national security information under their custody and control;

b. Complete annual information security refresher training to remain compliant with DoD and ODNI requirements. Failure to do so could result in loss of access to classified systems and networks (Reference o);

c. Ensure that access to such information is granted only to individuals with the appropriate clearances and accesses and a valid need-to-know;

d. Indicate, through marking or other means, the portions of national security information that require protection as classified and the portions that do not;

e. When practicable, use a classified addendum whenever classified information constitutes a small portion of a document that is otherwise not classified;

f. Challenge the classification status of information that they believe is improperly or incorrectly classified;

g. Ensure that classified information is not removed from official premises without proper authorization and approved safeguards;

h. Take custody of and safeguard classified material that is not properly controlled, and Immediately notify S&CI (A5);

i. Immediately notify S&CI (A5) upon the loss, unauthorized disclosure, or potential compromise of classified information. Additionally, notify the Cryptologic Disclosures Action Group of any known or suspected unauthorized disclosure of NSA classified equities in accordance with NSA/CSS Policy 1-27 (Reference p);

j. Comply with the prepublication review processes specified in NSA/CSS Policy 1-30 (Reference q);

k. Neither remove classified information from the Agency's control nor direct that information be declassified to remove it from Agency control when leaving Agency service; and

l. Attend a termination briefing when leaving Agency service that emphasizes their continued responsibility to protect national security information to which they have had access.

REFERENCES

a. Executive Order 13526, "Classified National Security Information," dated 29 December 2009

b. "Information Security Oversight Office (ISOO), Implementing Directive for Executive Order 13526, 32 Code of Federal Regulations Parts 2001 and 2003," dated 28 June 2010

c. Public Law 111-258, "Reducing Over-Classification Act," dated 7 October 2010

d. ICD 700, "Protection of National Intelligence," dated 7 June 2012

e. ICD 710, "Classification and Control Markings System," dated 21 June 2013

f. DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," dated 24 February 2012

g. DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information," dated 24 February 2012

h. DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," dated 24 February 2012

i. Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," dated 7 October 2011

j. Public Law 83-703, "Atomic Energy Act of 1954," as amended

k. NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Guide," dated 4 January 2019

l. Executive Order 12333, "United States Intelligence Activities," as amended

m. DoD Directive 5100.20, "The National Security Agency/Central Security Service (NSA/CSS)," dated 26 January 2010

n. NSA/CSS Policy 1-41, "Programs for the Protection of Especially Sensitive Classified Information," dated 13 September 2018

o. 32 CFR, Part 2002, Subpart G—Security, Education and Training §2001.T1

p. NSA/CSS Policy 1-27, "Identifying, Investigating and Reporting Unauthorized Media Disclosures of NSA/CSS Classified Information," dated 11 August 2014

q. NSA/CSS Policy 1-30, "Review of NSA/CSS Information Intended for Public Release," dated 12 May 2017

r. "NSA/CSS Memorandum on the NSA/CSS Classification Advisory Officer Program" dated 24 January 2019

s. NSA/CSS Policy 11-1, "Information Sharing," dated 28 March 2012

t. NSA/CSS Policy 5-2, "Security Investigations," dated 30 November 2017

u. NSA/CSS Policy 6-23, "Reporting and Handling of NSA/CSS Information System Security Incidents," dated 26 September 2016

GLOSSARY

affiliate—A person employed by, detailed to, or assigned to NSA/CSS, including members of the U.S. Armed Forces; experts, consultants, and contractors (including all subcontractors); or any other category of person who acts for or on behalf of NSA/CSS as determined by the Director, NSA/Chief, CSS. (Derived from: NSA/CSS Policy Glossary)

classifying—The act or process by which information is determined to be classified information (Reference a).

Classification Advisory Officer (CAO) Program—An NSA/CSS-unique program, administered by Information Security/Classification (P131), for training and certifying individuals who are responsible for ensuring that classified and sensitive information in their organizations is properly marked and protected and that the employees in their organizations understand and properly apply classification rules and guidance.

classification guide—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 that establishes the level and duration of classification for each such element. (Derived from: Reference a)

classified information—See Classified National Security Information.

classified national security information—Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form (Reference a).

Controlled-Access Programs—Programs established to protect extremely sensitive and critical intelligence information, including *sensitive compartmented information* (Reference n).

controlled unclassified information—Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. (Source: DoD Manual 5200.01, Vol. 4)

data spill—The inadvertent or intentional escape of information of a higher classification to a system of a lower classification.

declassification—The authorized change in the status of information from classified to unclassified (Reference a).

Declassification Authority—The official who authorized the original classification if that official is still serving in the same position, the originator's current successor if that individual has original classification authority, a supervisory official of either the originator or the originator's successor if the supervisory official has original classification authority, or any officials delegated Declassification Authority in writing by DIRNSA/CHCSS or by the Senior Agency Official. An NSA/CSS OCA also acts as the Declassification Authority for information under the OCA's purview. (Derived from: Reference f)

declassification guide—Written instructions issued by a Declassification Authority that describe the elements of information regarding a specific subject that may be declassified and the elements that must remain classified. (Derived from: Reference a)

derivative classification—Incorporating, paraphrasing, restating, or generating in a new form classified information and marking the newly developed material to be 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. (Derived from: Reference a)

documentary—Books, papers, maps, photographs, machine-readable materials, or other materials, regardless of physical form or characteristics (Reference b)

downgrade—A determination by a Declassification Authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level (Reference a).

emergency situation—Circumstance in which there is an imminent threat to life or in defense of the homeland (Reference h).

Enterprise Leaders—Directors, the NSA/CSS Chief of Staff, Service Cryptologic Component Commanders, Cryptologic Center Commanders/Chiefs, and Field Leaders. (Source: NSA/CSS Policy Glossary)

information—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. (Derived from: Reference a)

information security—The system of policies, procedures, and requirements established in accordance with Executive Order 13526 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to Executive Order, statute, or regulation. (Derived from: Reference f)

need-to-know—A determination within the executive branch in accordance with directives issued pursuant to Executive Order 13526 that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function (Reference a).

original classification—An initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure (Reference a).

Original Classification Authority (OCA)—An individual authorized in writing, either by the President, the Vice President, or agency heads or other officials designated by the President, to classify information at the time of its the first instance (Reference a).

reclassifying—Classifying information that had been previously declassified and released under proper authority (Reference a).

safeguarding—Measures and controls that are prescribed to protect classified information (Reference a).

self-inspection—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 Executive Order 13526 and its implementation directives (Reference a).

Senior Agency Official—The official appointed to be responsible for directing and administering an agency's program under which information is classified, safeguarded, and declassified (Reference a). (NOTE: The Chief, Policy, Information, Performance, and Exports (PIPE, P1) is the NSA/CSS Senior Agency Official.)

sensitive compartmented information—Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established and overseen by the Director of National Intelligence. (Source: ICS Number 2008-700-1)

Special-Access Program—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. (Source: DoD Directive 5205.07)

unauthorized disclosure—Communication or physical transfer of classified information to an unauthorized recipient (Reference a).

DOCUMENT HISTORY

Date	Approved by	Description
31 August 2017	Michael S. Rogers, Admiral, U.S. Navy, Director, NSA/ Chief, CSS	Policy reissuance; supersedes NSA/CSS Policy 1-52, "Classified National Security Information," dated 16 November 2012.
5 April 2019	Steve Thompson, Chief, Policy, Information, Performance, and Exports (PIPE)	Substantive update to change SPP to PIPE, to remove the requirement to obtain a PIPE (P1) endorsement of an Original Classification Authority (OCA) proposal, and to clarify guidance concerning the role of a Classification Advisory Officer (CAO).
4 September 2019	Chief, Policy	Administrative update to incorporate accessibility enhancements.