Department of Homeland Security
Management Directive System
MD Number: 11044
Issue Date: 08/12/2004

PROTECTION OF CLASSIFIED NATIONAL SECURITY INFORMATION CLASSIFICATION MANAGEMENT

I. Purpose

This directive implements the classification management portion of Executive Order 12958, as amended, Classified National Security Information. It prescribes the policies and procedures for the implementation, management, and oversight of the Classification Management Program within the Department of Homeland Security (DHS).

II. Scope

This directive is applicable to all persons who are permanently or temporarily assigned, attached, detailed to, or under contract with DHS. It is also applicable to other officials outside the Federal government who have been provided access to classified information.

III. Authority

A. Executive Order 12333, United States Intelligence Activities.

B. Executive Order 12829, National Industrial Security Program.

C. Executive Order 12958, as amended, Classified National Security Information.

D. Executive Order 13284, Amendment of Executive Orders, and Other Actions, in Connection with the Establishment of the Department of Homeland Security.

E. 6 CFR, Part 7, Department of Homeland Security, Classified National Security Information.

F. 32 CFR, Part 2001/2004, Implementing Directive for EO 12958, as amended.

G. Title 44, United States Code

H. DHS Delegation Number 8100.1, Delegation of Original Classification Authority.

I. Atomic Energy Act of 1954, as amended.

J. National Security Act of 1947

IV. Definitions

A. ***Authorized Person***: A person who has a need-to-know for access to classified information in the performance of official duties and who has been granted a personnel clearance or authorized access at the required level. The responsibility for determining whether a prospective recipient is an authorized person rests with the person who has possession, knowledge, or control of the classified information involved, and not with the prospective recipient.

B. ***Automatic Declassification***: The declassification of information based solely upon the occurrence of a specific date or event, as determined by the original classification authority; or the expiration of a maximum time frame for the duration of classification established under Executive Order 12958, as amended.

C. ***Classification***: The act or process by which information is determined to be classified information.

D. ***Classification Guidance***: Any instruction or source that prescribes the classification of specific information.

E. ***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.

F. ***Classified National Security Information ("Classified Information")***: Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

G. ***Confidential***: Level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

H. ***Declassification***: The authorized change in the status of information from classified information to unclassified information.

I. ***Declassification Authority***: The official who authorized the original classification, if that official is still serving in the same position; the originator's current successor in function; a supervisory official of either; or officials delegated declassification authority in writing by the agency head or the senior agency official.

J. ***Derivative Classification***: 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 guidance provided in a security classification guide. The duplication or reproduction of existing classified information is not derivative classification.

K. ***Freedom of Information Act (FOIA)***: Provides that any person has a right of access to federal agency records, except to the extent that such records are protected from public disclosure by statutory exemptions or exclusions.

L. ***Information***: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

M. ***Information Security***: As used in this directive, Information Security is the system of policies, procedures, and requirements established under the authority of Executive Order 12958, as amended, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

N. ***Mandatory Declassification Review***: The review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.5 of Executive Order 12958, as amended.

O. ***Need-to-Know***: A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information to perform, or assist in, a lawful and authorized governmental function.

P. ***Organizational Element***: As used in this directive, organizational element is as defined in DHS MD Number 0010.1, "Management Directive System and DHS Announcements."

Q. ***Original Classification***: The initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

R. ***Original Classification Authority***: An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

S. ***Secret***: Level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

T. ***Security Liaison***: An official who is assigned responsibility for implementing and managing an organizational element's security program as a secondary or additional duty.

U. ***Security Officer***: Authorized position within an organizational element whose primary duties are to serve as the lead official for developing, implementing, and managing security programs within the organizational element.

V. ***Source Document***: An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

W. ***Systematic Declassification Review***: The review for declassification of classified information contained in records that have been determined by the Archivist of the United States to have permanent historical value in accordance with Title 44, United States Code.

X. ***Top Secret***: Level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

V. Responsibilities

A. The ***Secretary of Homeland Security*** has designated the ***Chief Security Officer (CSO)*** as the ***Senior Agency Official (SAO)***. The Senior Agency Official shall:

1. Direct and administer the Department's program under which information is classified, safeguarded, and declassified.

2. Coordinate the Department's classification management program and serve as the DHS point of contact on matters associated with the Information Security Oversight Office (ISOO).

3. Promulgate and publish implementing directives as necessary for program implementation and ensure procedures are established and implemented to prevent unauthorized and unnecessary access to classified information.

4. Promulgate implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public.

5. Establish and maintain security education and training programs.

6. Establish and maintain a self-inspection and periodic review program to review and assess the management and safeguarding of classified information created and/or possessed by DHS agencies.

7. Develop special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas.

8. Ensure the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element to be evaluated in the rating of:

a. Original Classification Authorities

b. Security Managers, security specialists, or other officials performing security functions involving the safeguarding of classified information

c. Other personnel whose duties involve the creation or handling of classified information.

9. Account for costs associated with the implementation of programs for the protection of classified information. Report such costs to the Information Security Oversight Office (ISOO) upon request.

10. Assign promptly personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of Executive Order 12958, as amended, that pertains to classified information that originated in an organizational element of DHS that no longer exists and for which there is no clear successor in function.

11. Report violations, take corrective measures and assess appropriate sanctions as warranted, in accordance with Executive Order 12958, as amended.

12. Oversee DHS participation in special access programs authorized under Executive Order 12958, as amended.

13. Establish procedures to prevent unnecessary access to classified information, including procedures that:

a. Require that a need for access to classified information is established before initiating administrative clearance procedures.

b. Ensure that the number of persons granted access to classified information is limited to the minimum, consistent with operational and security requirements and needs.

14. Perform any other management duties as required by the position of Senior Agency Official that the Secretary may designate.

B. The ***Chief, Administrative Security Division*** shall:

Under the direction and authority of the SAO/CSO, administer, manage, and provide oversight for all programs relating to the safeguarding of classified information as cited in this directive.

C. The heads of ***Organizational Elements*** shall:

1. Ensure sufficient resources are in place to implement and manage the Information Security Program and the requirements of this directive.

2. Appoint a senior official within the organizational element to serve as the organizational element Security Officer/Security Liaison.

3. Issue additional written procedures necessary for the effective implementation of this directive. Procedures written to augment or supplement this directive may exceed the requirements cited in this directive but shall not lessen them. When an organizational element chooses to exceed the standards as cited herein, sufficient justification must exist to warrant any increased expenditures.

D. The organizational element ***Security Officer/Security Liaison*** shall:

1. Serve as the advisor to the head of the organizational element for all matters relating to implementation and compliance with the provisions of this directive.

2. On behalf of the head of the organizational element, implement, monitor, manage, and oversee the provisions of this directive within his/her respective organizational element.

3. Act as liaison between the organizational element, organizational element counterparts, DHS headquarters security staff, and other security officials both inside and outside of government.

4. Implement a viable and robust security education and training program.

E. ***Supervisors and Managers*** shall:

1. Ensure that they are aware of and comply with the applicable provisions of this directive, and promote and ensure compliance by staff members.

2. Begin security education and awareness upon initial assignment of an employee and reinforce periodically thereafter through routine office interaction, e-mail reminders, staff meetings and other office gatherings, or any other method or media contributing to an informed workforce.

F. All personnel shall:

1. Be responsible for protecting classified information from unauthorized disclosure.

2. Be aware of and comply with the applicable provisions of this directive and report to appropriate officials infractions or violations that affect the safeguarding of classified information.

VI. Policy & Procedures

A. ***General***.

1. Efficient and economic administration of the DHS classification management program requires the application of effective classification management principles. The integrity of the classification system is dependent upon the knowledge and judgment of officials involved in oversight, implementation, and practical application of the safeguarding and classification process. The consequences of an undefined and inconsistent classification management program are wasted resources, lack of public trust, and potential harm to the national security. Over-classification or unnecessary classification creates an undue economic burden, requires expenditure of funds and commitment of resources, and dilutes the legitimacy of properly classified information. DHS officials involved in the classification process shall comply with the standards cited in this directive and ensure integrity of the system is maintained by implementing a sound classification management program.

2. This directive prescribes the minimum standards for the protection of classified information. Organizational elements may exceed the standards cited in this directive but may not lessen them. When an organizational element chooses to exceed the standards as cited herein, sufficient justification must exist to warrant any increased expenditures.

3. Requests to waive requirements cited in this directive will be submitted through the Security Officer/Security Liaison of the requesting organizational element to the DHS Chief Security Officer. Waiver requests must include sufficient justification to support the request and identify compensatory measures that will be implemented to mitigate deficiencies.

4. Nothing in this directive is intended to conflict with or circumscribe the authority of the Office of the Inspector General.

B. ***Original Classification***.

Original classification is the initial determination that an item of information requires protection against unauthorized disclosure in the interest of national security. Original classification decisions can only be made by officials who have been specifically delegated this authority and have cognizance over the information, or, the DHS Senior Agency Official. Original classification decisions will be made in accordance with the guidance provided in this directive and the standards and criteria cited in Executive Order 12958, as amended.

1. Original Classification Authority (OCA)

a. An original classification authority (OCA) is an official authorized, in writing, either by the President, by agency heads, or other officials delegated by the President, to make an initial determination to classify information.

b. The Secretary of Homeland Security has been designated by the President as an OCA with authority to classify eligible information up to and including Top Secret. The Secretary can further delegate Top Secret original classification authority to additional DHS officials pursuant to EO 12958, as amended.

c. The DHS Chief Security Officer has been designated by the Secretary as the “Senior Agency Official” with original classification authority up to the Top Secret level. As the Senior Agency Official, the Chief Security Officer can delegate Secret and Confidential original classification authority to additional DHS officials.

d. Only the Secretary or the Chief Security Officer can further delegate original classification authority. Officials who have been delegated original classification authority by the Secretary or the Chief Security Officer can not further delegate the authority.

e. Refer to DHS Delegation Number 8100.1, Delegation of Original Classification Authority, or its predecessors, to determine those DHS positions permanently authorized to originally classify information.

f. Persons delegated original classification authority at a specified level are also authorized to classify information at a lower level.

2. Requesting Original Classification Authority

a. Where an operational need exists, the heads of organizational elements may request OCA delegation for additional officials. Requests for OCA delegations shall be submitted to the DHS Office of Security using DHS Form 11041-1, "Request for Original Classification Authority." The number of OCA delegated officials shall be kept to an absolute minimum. Requests for additional OCA's shall be based on justification of a demonstrated and continuing need for such authority.

b. Requests for OCA at the Top Secret level shall be processed by the DHS Office of Security, through the DHS Office of the General Counsel, to the Secretary.

c. Requests for OCA at the Secret and Confidential levels shall be processed and approved or denied by the DHS Chief Security Officer.

d. Upon approval, additional OCA delegations shall be memorialized, in writing, by the Secretary or the Chief Security Officer, as applicable.

3. Loss/Transfer of OCA Responsibilities

Original classification authority is delegated by position. Officials no longer performing the functions of an OCA, or no longer serving in positions delegated with OCA, are no longer authorized to exercise the authority. In the absence of a delegated OCA, the person officially designated to act in lieu of such official is transferred OCA authority, and can exercise OCA responsibilities.

4. Specialized Training

Officials serving in OCA delegated positions and other officials delegated OCA authority shall be trained on OCA responsibilities, methods, and procedures within sixty (60) days of occupying a delegated position. The DHS "Guide for Original Classification Authorities (OCA)" is available from the DHS Office of Security and will be provided to delegated OCA's.

C. ***Original Classification Decisions***.

1. Classification Standards

For information to be classified in the first instance, it must meet the following standards:

a. It is classified by an original classification authority.

b. It is owned by, produced for or by, or under the control of the U.S. government. For the purposes of this directive, "control" means the authority of the agency that originated the information, or its successor in function, to regulate access to the information.

c. It falls within one or more of the categories specified by E.O. 12958, as amended. (See paragraph VI.C.2 below.)

d. The original classification authority has determined the unauthorized disclosure of the information considered for classification could reasonably be expected to cause damage to the national security, which includes defense against transnational terrorism, and the classifier is able to identify or describe the damage.

2. Classification Categories

Information considered for classification shall fall into one or more of the following categories: (The numerical indicator preceding each category is the category identifier cited in Section 1.4 of E.O. 12958, as amended.)

a. 1.4(a) military plans, weapons systems, or operations;

b. 1.4(b) foreign government information;

c. 1.4(c) intelligence activities, (including special activities), intelligence sources or methods, or cryptology;

d. 1.4(d) foreign relations or foreign activities of the U.S., including confidential sources;

e. 1.4(e) scientific, technological, or economic matters relating to national security, which includes defense against transnational terrorism;

f. 1.4(f) U.S. Government programs for safeguarding nuclear materials or facilities;

g. 1.4(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

h. 1.4(h) weapons of mass destruction.

3. Classification Levels

At the time of original classification, the OCA will assign a classification level. There are only three authorized classification levels. Except as otherwise provided by statute, no other terms shall be used to identify U.S. classified information. Further, these terms shall not be used or applied to DHS originated unclassified information that does not meet the standards for classification in accordance with this directive and E.O. 12958, as amended.

a. TOP SECRET - level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.

b. SECRET - level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe.

c. CONFIDENTIAL - level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe.

4. Duration of Classification

At the time of original classification, the OCA will assign a date or event at which the information will be downgraded and/or declassified. At the time an item of information is classified, original classifiers shall:

a. Attempt to determine a specific date or event within ten years of the date of origination, upon which the information can be automatically declassified. If that is not possible, they shall attempt to:

b. Assign a date ten years from the date of origination at which the information can be automatically declassified. Should the sensitivity of the information warrant classification beyond a ten year period, they shall:

c. Assign a date no longer than 25 years from the date of origination at which the information will be automatically declassified, unless it is reclassified.

d. An OCA cannot classify information beyond 25 years unless such information has been specifically approved for exemption from declassification pursuant to E.O. 12958, as amended, and Section VI.J of this directive. The only exception to this rule is when disclosure of the information could be expected to reveal the identity of a confidential human source or human intelligence source. In this instance, the “Declassify On” line may be marked 25 X-Human. This marking is not authorized for use when the information pertains to non-human intelligence sources or intelligence methods.

5. Communicating Original Classification Decisions

Classification decisions will be communicated either through publication of a security classification guide (See Section VI.F) or through markings placed directly on the materials.

6. Classification Prohibitions

a. In no case shall information be classified to:

(1) Conceal violations of law, inefficiency, or administrative error;

(2) Prevent embarrassment to a person, organization, or agency;

(3) Restrain competition; or

(4) Prevent or delay the release of information not requiring protection in the interest of national security.

b. Basic scientific research information not clearly related to the national security shall not be classified.

7. Classification by Compilation

a. Compilations of items of information that are individually unclassified may be classified in certain circumstances if the compilation reveals an additional association or relationship that meets the standards and criteria for classification under E.O. 12958, as amended; the additional association or relationship is not otherwise evident or revealed in the individual items of information; and the information is classified by an OCA. In this instance, the additional association or relationship is what is considered for classification, not the individual items of unclassified information. Careful consideration must be taken when determining the need for classification by compilation. When the determination is made that classification by compilation is necessary, the OCA must provide explicit instructions as to what elements of the compilation, when combined, constitute classification and the additional association or relationship that warrants the classification.

b. Additionally, information classified at a lower level, when compiled with other information classified at a lower level, may be classified at a higher level, under the conditions cited above.

8. Classifying Equipment

Integrated parts or items of equipment, or other physical objects, shall be individually classified based on the standards and criteria for classification cited in this directive. The overall classification of an item of equipment or physical object will be based on the highest classification of the integrated parts.

9. Records of Classification Actions

a. Persons performing original classification actions shall maintain a record of each action taken. For originally classified information, the record shall include the total number of documents originally classified, by classification level, and by declassification date.

b. The record will be maintained by fiscal year and submitted to the DHS Office of Security as part of annual reporting requirements.

c. Records of classification actions will be counted and reported by document – not by page. For example, a newly created originally classified document consisting of multiple pages and containing both SECRET and CONFIDENTIAL information is counted and reported as one originally classified document at the SECRET level.

D. ***Derivative Classification***.

Derivative classification means the incorporating, paraphrasing, restating, or generating in new form information that is already classified (source), and marking the newly developed material consistent with the classification markings on an existing source or as published in a security classification guide.

1. Derivative Classification Authority

Delegated authority is not required to perform a derivative classification action. Any employee with the appropriate level of security clearance and the need to perform a derivative classification action as part of their official government duties is authorized to do so.

2. Derivative Classification Applications

a. If an individual applying derivative classification markings believes the paraphrasing, restating, or summarizing of classified information has changed the level of, or removed the basis for classification, they will consult the appropriate OCA for a classification decision.

b. When applying derivative classification markings:

(1) Original classification markings cited on the source or in a security classification guide, will be respected and carried forward to the newly created document.

(2) All applicable classification markings, declassification instructions, and handling instructions will be placed on the newly created material.

(3) Questions on the classification markings as they appear on the source or in a security classification guide will be referred to the originator. For challenges to classification refer to Section VI.E.3, below.

3. Records of Derivative Classification Actions

a. Persons performing derivative classification actions shall maintain a record of each action taken. For derivatively classified documents, the record shall include the total number of documents derivatively classified, by classification level.

b. The record will be maintained by fiscal year and submitted to the DHS Office of Security as part of annual reporting requirements.

c. Records of classification actions are counted and reported by document – not by page. For example, a newly created derivatively classified document consisting of multiple pages and containing both SECRET and CONFIDENTIAL information is counted and reported as one derivatively classified document at the SECRET level.

4. Specialized Training

Persons performing, or who plan to perform, derivative classification actions should attend specialized training on marking classified materials. Contact the DHS Office of Security or the organizational element Security Officer for training sources.

E. ***Classification Considerations***.

1. Reclassifying Previously Declassified Information

a. Information may be reclassified after it has been declassified and released to the public under proper authority. The following conditions will be met:

(1) The Secretary or Deputy Secretary, DHS, personally endorses, in writing, that the reclassification action is in the best interest of national security and meets the standards and criteria for classification.

(2) The released information may be reasonably recovered and brought back under DHS control.

(3) The reclassification action is reported within thirty (30) days to the Director, Information Security Oversight Office.

b. Information not previously disclosed to the public under proper authority may be classified or reclassified after DHS has received a request for it under the Freedom of Information Act (5 U.S.C.552) or Privacy Act of 1974 (5 U.S.C. 552a); or the mandatory review provisions of section 3.5 of E.O. 12958, as amended. Information may be reclassified only if classification meets the requirements of E.O. 12958, as amended, classification is accomplished on a document-by-document basis, and reclassification is approved by the DHS Chief Security Officer.

2. Exceptional Circumstances

a. If an individual originates or develops information believed to require classification and no authorized OCA is available, they shall safeguard and mark the information in the manner prescribed for the classification level. Additionally, the notation: "TENTATIVELY CLASSIFIED PENDING AN ORIGINAL CLASSIFICATION DECISION." shall be prominently and conspicuously marked on the bottom of each page.

b. A request for a classification decision will be submitted, by a means approved for the level of classification, to the OCA having subject matter interest and classification responsibility. The OCA shall notify the sender of a classification determination within thirty (30) days of receiving the request.

c. When guidance is needed to determine the appropriate OCA with subject matter interest, contact the organizational element Security Officer or DHS Office of Security.

3. Classification Challenges

Authorized holders of classified information, who, in good faith, believe its classification status is improper, are encouraged and expected to challenge the classification status. Classification challenges shall be presented to the classifier of the information. Where necessary, assistance and/or anonymity in processing a classification challenge can be obtained by processing the challenge through the DHS Office of Security.

a. Processing Formal Classification Challenges

(1) Formal challenges to classification shall be in writing and presented to an OCA having jurisdiction over the challenged information. Every effort should be made to keep the written correspondence unclassified. However, if the challenge includes classified information it shall be marked and safeguarded accordingly. The written correspondence shall sufficiently describe the information being challenged and can consist of only a question as to why the information is classified or why it is classified at a particular level.

(2) Individuals submitting a classification challenge shall not be subject to retribution of any kind for bringing such actions. Anonymity can be requested by processing the challenge through the DHS Office of Security. The DHS Office of Security shall honor a challenger's request for anonymity and serve as the agent for the challenger in processing the challenge.

(3) The OCA receiving the challenge shall provide a written response with a classification/declassification decision to the challenger within sixty (60) days of receipt.

(4) The individual submitting the challenge has a right to appeal the decision to the Interagency Security Classification Appeals Panel established by Section 5.3 of E.O. 12958, as amended. The DHS Office of Security will assist with appeals as needed.

(5) Challenged information remains classified and shall be protected at its highest level of classification until a final classification determination is made by an appropriate OCA.

b. Informal Classification Challenges

The classification challenge provision does not prohibit an authorized holder from informally questioning the classification of information through direct and informal contact with the classifier. When appropriate or when uncertainties exist over the classification status, holders of classified information are encouraged to make direct contact with the classifier to obtain clarification. When a change in classification results from an informal challenge, the challenger will ensure the official from whom the change was received is authorized to make such a change, and a record of the change, to include the official's name, position, agency, and date is maintained with a file copy of the document.

4. Third Agency Rule

Classified information originated by another government agency and furnished to a DHS organizational element shall not be further distributed outside DHS without the prior consent of the originating agency. Unless limitations have been imposed by the originator, this restriction does not apply to further distribution within and between organizational elements of DHS or distribution to cleared contractors who require the information in the performance of a DHS contract.

F. ***Security Classification and Declassification Guides***.

1. A classification guide is a documentary form of classification guidance issued by an original classification authority. The guide identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each element.

2. OCA's will issue security classification guides to cover program specific information subject to classification guidance. Each guide shall be approved personally, and in writing, by an official who has program or supervisory responsibility over the information and who has been delegated original classification authority at the highest level of classification cited in the guide, or by the DHS Senior Agency Official.

3. Classification guides are intended to facilitate the proper and uniform derivative classification of information. To ensure consistency in classification guidance, consult with appropriate subject matter experts and potential users of the guide. This includes inter-agency coordination with other government agencies having an interest in similar programs and information.

4. A classification guide will be prepared for each system, plan, program, or project involving the classification of information and be prepared consistent with the DHS format for classification guides. The DHS "Handbook for Writing Security Classification Guides" is available from the DHS Office of Security to assist writers in preparing the guides.

5. Preparation and publication of classification guides will be coordinated through the DHS Office of Security for concurrence, prior to presentation of the guide to an OCA for approval and signature. A final copy of the classification guide will be submitted to the DHS Office of Security. The DHS Office of Security will maintain an index and will be the central repository of DHS issued classification and declassification guides.

6. Declassification guides shall be issued to facilitate the declassification of information contained in records determined to be of permanent historical value under Title 44, United States Code. A classification guide can also serve as a declassification guide.

7. Declassification guides issued pursuant to the automatic declassification provisions cited in Section 3.3 of Executive Order 12958, as amended, will precisely state the categories or elements of information to be declassified or downgraded and those specific categories or elements that will be exempt from declassification.

8. Categories or elements of information to be exempt from automatic declassification will cite the exemption category per Section 3.3 of Executive Order 12958, as amended.

9. Prior to publication of a declassification guide, it will be coordinated through the DHS Office of Security and the Information Security Oversight Office (ISOO).

10. Classification and declassification guides will be updated as circumstances require. A complete review will be conducted no later than five (5) years after publication.

G. ***Declassification***.

1. It is DHS policy that information shall remain classified as long as:

   a. It is in the best interest of the national security to keep it protected, and;

   b. Continued classification is in accordance with the requirements of the E.O. 12958, as amended.

2. If DHS officials have reason to believe that the public interest in disclosure of information outweighs the need for continued classification, they shall refer the matter to the appropriate original classification authority, or the DHS Senior Agency Official, for an assessment and determination on whether declassification is appropriate.

3. None of the provisions cited in this directive apply to information classified in accordance with the Atomic Energy Act of 1954, as amended (Restricted Data and Formerly Restricted Data).

H. ***Declassification Authority***.

1. Information may be declassified or downgraded by:

a. The Secretary of Homeland Security,

b. The DHS Senior Agency Official,

c. Officials who have been delegated Original Classification Authority, their current successor in function, or a supervisory official of either, and

d. Officials who have been delegated declassification authority, in writing, by the Secretary or the DHS Senior Agency Official.

2. The authority to declassify or downgrade information extends only to information for which the official has classification, program, or functional responsibility, or, to other information as provided for by delegation under Section VI.H.1.d, above.

3. Persons with declassification authority shall develop and issue declassification guides to facilitate effective review and declassification of information not previously covered by a classification or declassification guide, and for information exempt from automatic declassification, in accordance with Section VI.E, of this directive.

4. Declassification authority is not required for simply canceling or changing classification markings in accordance with declassification or downgrading instructions cited on a document, directions found in a security classification guide or declassification guide, or instructions received from an original classification or declassification authority.

I. ***Declassification Decisions by Original Classifiers***.

1. Assigning Declassification Instructions

At the time an item of information is classified, original classifiers shall:

a. Attempt to determine a specific date or event within ten years from the date of origination upon which the information can be automatically declassified. If that is not possible, they shall attempt to:

b. Assign a date ten years from the date of origination at which the information can be automatically declassified. Should the sensitivity of the information warrant classification beyond a ten year period, they shall:

c. Assign a date no longer than 25 years from the date of origination at which the information will be automatically declassified.

2. Extension of Classification

a. If an original classification authority with jurisdiction over the information does not extend the classification of information that has been assigned a specific date or event for declassification, the information is automatically declassified upon the occurrence of the date or event.

b. Decisions to extend classification must take into account the potential difficulty of notifying holders of the extension, including the possible inability to ensure continued, uniform protection of the information. Officials who make a determination to extend a declassification date are responsible for notifying holders of the information of the decision, and, providing a new date for declassification.

c. If an original classification authority has assigned a date or event for declassification that is less than 25 years from the date of classification, an original classification authority with jurisdiction over the information may extend the classification duration of such information for a period not to exceed 25 years from the date of origination.

d. For information in records determined to have permanent historical value, successive extensions of classification may not exceed 25 years from the date of the information's origin.

J. ***Automatic Declassification at 25 Years***.

1. Automatic Declassification of Permanent Historical Records

a. Executive Order 12958, as amended, mandates that information contained within permanently valuable historical records (as defined by Title 44, U.S. Code) shall be automatically declassified 25 years from the date of original classification. This mandate shall take full effect on December 31, 2006, at which time such records that have not been otherwise exempt in accordance with this directive, will be automatically declassified whether or not the records have been reviewed. Subsequently, all classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of its original classification, except as otherwise indicated in this policy.

b. Organizational elements will use the time allotted between publication of this directive and December 31, 2006, to review existing information subject to the provisions of this mandate and declassify or request an exemption from automatic declassification in accordance with the provisions of this directive. Organizational elements will develop a declassification plan and declassification guide(s), as appropriate. Such reviews must take into account the potential existence of equities from other government agencies and ensure that such equities are appropriately identified and referred to the applicable agency.

2. Exemption of Specific Information not Contained in a File Series

a. The Secretary of Homeland Security may propose to exempt specific information, not otherwise contained in an exempted file series, from automatic declassification. Specific information may be exempted only if its release could be expected to:

(1) Reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

(2) Reveal information that would assist in the development or use of weapons of mass destruction;

(3) Reveal information that would impair U.S. cryptologic systems or activities;

(4) Reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) Reveal actual U.S. military war plans that remain in effect;

(6) Reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) Reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

(9) Violate a statute, treaty, or international agreement.

b. Such exemption requests shall be endorsed by the senior official of the organizational element to which the information applies and submitted through the DHS Chief Security Officer, to the Secretary. Submissions shall be made no earlier than five (5) years, and no later than 180 days, before the information is scheduled for automatic declassification. In addition to the specific exemption cited above, submissions shall include:

(1) Description of the specific information to be exempted;

(2) Explanation why the information must remain classified beyond a 25 year period; and

(3) Except for the identity of a confidential human source or human intelligence source, a specific date or event upon which the information will be declassified.

c. Exemptions endorsed by the Secretary under this provision will be promptly submitted to the Information Security Oversight Office, by the DHS Chief Security Officer, for approval.

3. Exemption of Information Contained in a Specific File Series

a. Specific file series may be exempt from the 25 year automatic declassification provisions of the Order. Such exemption requests shall be endorsed by the senior official of the organizational element to which the information applies and submitted through the DHS Chief Security Officer, to the Secretary. The Secretary shall notify the President, through the Assistant to the President for National Security Affairs and the Information Security Oversight Office, of any specific file series proposed for exemption from 25 year automatic declassification. Submissions shall be made no earlier than five (5) years, and no later than 180 days, before the information is scheduled for automatic declassification. In addition to the specific exemption cited in VI.J.2.a, submissions shall include:

(1) Description of the file series;

(2) Explanation of why information within the file series must remain classified beyond a 25 year period; and

(3) Except for the identity of a confidential human source or human intelligence source, a specific date or event upon which the information will be declassified.

b. Information in these file series shall not be subject to automatic declassification unless the Secretary specifically decides to remove the series from the exempted category.

c. Information exempted from automatic declassification at 25 years remains subject to the mandatory and systematic declassification review provisions of this Policy.

4. Onset of Automatic Declassification

a. The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, that are otherwise subject to automatic declassification under this section, shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(2) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, the Secretary or the DHS Chief Security Officer may delay automatic declassification for up to five (5) additional years for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly.

(3) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, the Secretary or the DHS Chief Security Officer may delay automatic declassification for up to three (3) years for classified records that have been referred or transferred to DHS by another agency less than three (3) years before automatic declassification would otherwise be required.

(4) By notification to the Director of the Information Security Oversight Office, the Secretary or DHS Chief Security Officer may delay automatic declassification for up to three (3) years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

b. Information contained in records not determined to be permanently valuable, and not scheduled for disposal or retention by the National Archives, is not subject to automatic declassification. Agency retention and destruction requirements apply.

K. ***Mandatory Review for Declassification***.

1. Any individual may request a review for declassification of information classified under E.O. 12958, as amended, or its predecessor orders. Such requests shall be sent to the Department of Homeland Security, Director, Departmental Disclosure, Privacy Office, Washington D.C. 20528 (here and after, the Disclosure Officer).

2. Information originated by the incumbent President; the incumbent President's White House Staff; committees, commissions, or boards appointed by the incumbent President, or other entities within the Executive Office of the President that solely advise and assist the incumbent President are exempt from the provisions of this section.

3. Responsibilities

a. The Disclosure Officer shall serve as the central processing point for all mandatory review requests concerning DHS information. The Disclosure Officer will promptly, but no later than thirty days from receipt, forward mandatory review requests to the applicable DHS organizational element(s) having primary jurisdiction over the requested information. The Disclosure Officer will provide the requester with an acknowledgment of receipt of the request.

b. Organizational elements shall promptly process the request. Information reviewed shall be declassified if it no longer meets the standards for classification established by Executive Order 12958, as amended, and this directive. Information that is declassified shall be released to the requester unless withholding is appropriate under applicable law (for example, the Freedom of Information Act or the Privacy Act of 1974).

4. Processing Mandatory Review Requests

a. The request must sufficiently describe the document or material with enough specificity to allow it to be located by the organizational element with a reasonable amount of effort. When the description of the information in the request is deficient, the organizational element shall solicit as much additional identifying information as possible from the requester. If the information or material requested cannot be obtained with a reasonable amount of effort, the organizational element shall provide the requester, through the DHS Disclosure Office, with written notification of the reasons why no action will be taken and of the requester's right to appeal.

b. Requests for review of information that has been subjected to a declassification review request within the preceding two years shall not be processed. The Disclosure Officer will notify the requester of such denial.

c. Requests for information exempted from search or review under Sections 105C, 105D, or 701 or the National Security Act of 1947 (50 U.S.C. 403-5c, 403-5e, and 431), shall not be processed. The Disclosure Officer will notify the requester of such denial.

d. If documents or material being reviewed for declassification under this Section contain information that has been originally classified by another government agency, the reviewing activity shall notify the Disclosure Officer. Unless the association of that organization with the requested information is itself classified, the Disclosure Officer will then notify the requester of the referral.

e. A DHS organizational element may refuse to confirm or deny the existence, or non-existence, of requested information when the fact of its existence, or non-existence, is properly classified.

f. DHS organizational elements shall make a final determination on the request as soon as practicable but within one year from receipt. When information cannot be declassified in its entirety, organizational elements shall make reasonable efforts to redact those portions that still meet the standards for classification and release those declassified portions of the requested information that constitute a coherent segment.

g. Organizational elements shall notify the Disclosure Officer of the determination made in the processing of a mandatory review request. Such notification shall include the number of pages declassified in full; the number of pages declassified in part; and the number of pages where declassification was denied.

h. The Disclosure Officer shall maintain a record of all mandatory review actions for reporting in accordance with applicable federal requirements.

5. Processing Appeals

a. The mandatory declassification review system shall provide for administrative appeal in cases where the review results in the information remaining classified. The requester shall be notified of the results of the review and of the right to appeal the denial of declassification. To address such appeals, the DHS Disclosure Office shall convene a DHS Classification Appeals Panel (DHS/CAP). The DHS/CAP shall, at a minimum, consist of representatives from the Disclosure Office, the DHS Office of Security, the DHS Office of General Counsel, and a representative from the organizational element having jurisdiction over the information.

b. If the requester files an appeal through the DHS/CAP, and the appeal is denied, the requester shall be notified of the right to appeal the denial to the Interagency Security Classification Appeals Panel (ISCAP).

6. Foreign Government Information

The declassifying agency is the agency that initially received or classified the information. When foreign government information is being considered for declassification or appears to be subject to automatic declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. The declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

L. ***Freedom of Information Act and Privacy Act Requests***.

1. If a requester submits a request under both the mandatory declassification review provisions cited in this directive and the Freedom of Information Act, the requester shall be advised to elect one process or the other. If the requester fails to elect one or the other, the request will be treated as a FOIA request.

2. Upon receipt of a request for classified information under the Freedom of Information Act or the Privacy Act of 1974, the receiving office will process the request in accordance with the provisions of those acts.

M. ***Systematic Review for Declassification***.

1. Contain information, which has been identified to have significant value for historical or scientific research or for promoting the public welfare, and

2. Have a reasonable likelihood of being declassified upon review.

N. ***Downgrading***.

1. Downgrading of information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level, and can be properly protected at a lower level. The principal purpose of downgrading is to conserve security resources by avoiding protection of information at too high a level. Information may be downgraded by any official authorized to originally classify the information.

2. Existing documents that identify a specific date or event at which the information may be downgraded, shall be automatically downgraded upon occurrence of that date or event, unless they have been reviewed and reclassified.

3. Downgrading Decisions During Original Classification

Downgrading should be considered when original classifiers are deciding on the duration of the classification to be assigned. If downgrading dates or events can be identified, they must be specified along with the declassification instruction. Note that downgrading instructions DO NOT replace declassification instructions.

4. Downgrading at a Later Date

Information may be downgraded by any official who is authorized to originally classify the information. The authorized official making the downgrading decision shall notify holders of the change in classification.

O. Upgrading

Classified information may be upgraded to a higher level of classification only by officials who have been delegated the appropriate level of Original Classification Authority. Information may be upgraded only if holders of the information can be notified of the change so that the information will be uniformly protected at the higher level. The Original Classification Authority making the upgrading decision is responsible for notifying holders of the change in classification.