Chapter 3.
CLASSIFICATION UNDER EXECUTIVE ORDERS

This chapter discusses classification under executive orders (EOs). Of the EOs that deal with security classification of information, only EO 12958, signed by President Clinton in 1995, is currently in effect. All earlier EOs on this subject have been repealed by subsequent EOs.

Executive Orders are issued by the president by authority of the executive powers granted him by the Constitution. Executive orders become effective upon presidential signature and subsequent publication in the *Federal Register*. They are regarded as a public act of which U.S. courts must take notice and give effect.[1] Executive orders have the force of public law.[2] However, an EO cannot contravene an act of Congress. The effect of an EO is generally confined to the activities of executive agencies in managing their responsibilities. Failure to obey provisions of an order results in administrative sanctions (e.g., reprimands and loss of job), not legal offenses.[3]

Although Congress has not explicitly authorized an EO dealing with classification of information, it has given this classification system implicit approval via two statutes. Under Sect. 552(b)(1) of the Freedom of Information Act (FOIA),[*] Congress has exempted from disclosure documents that have been properly classified under an executive order. Under the Internal Security Act of 1950,[†] Congress has prohibited government employees from giving information classified by the president (or under his direction) to foreign agents. Note that Exemption (b)(1) of the FOIA uses the terms "national defense or foreign *policy*," whereas EO 12958 uses the terms "national defense or foreign *relations*" [emphasis added]. Some members of Congress have objected to the use of the term "relations" rather than "policy" in the EOs establishing our classification system because "relations" is a much broader term than "policy."[4]

In 1947 the National Security Act[5] created the National Security Council (NSC), which was given responsibility to study national security matters. This Act also specified that the Director of Central Intelligence was responsible for protecting intelligence sources and methods from unauthorized disclosures.[6] In 1950 the Internal Security Act of 1950 authorized the criminal punishment of any federal official or employee who communicated classified information without authorization.[7]

---

[*] 5 U.S.C. Sect. 552(b). "This section does not apply to matters that are–(1)(A) specifically authorized under criteria established by Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive Order."

[†] 50 U.S.C. Sect. 783(b). "Communication of classified information by Government officer or employee. It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, . . . to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government . . . any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified."

CLASSIFICATION UNDER EXECUTIVE ORDERS PRIOR TO EO 12958

Executive Order 8381

The first EO dealing with classification was EO 8381, "Defining Certain Vital Military and Naval Installations and Equipment," issued on March 22, 1940, by President Franklin Roosevelt.[8] This EO was promulgated in accordance with a 1938 statute[9] concerned with protecting information relative to certain national defense interests ("vital military and naval installations or equipment"), which was similar to the 1869 Army order concerning forts (Chap. 2).[*] However, the order's scope went beyond the interests specifically listed in the statute ("photograph, sketch, picture, drawing, map, or graphical representation") to encompass "all official military or naval books, pamphlets, documents, reports, maps, charts, plans, designs, models, drawings, photographs, contracts, or specifications which are now marked under the authority or at the direction of the Secretary of War or the Secretary of the Navy as 'secret,' 'confidential,' or 'restricted' and all such articles or equipment which may hereafter be so marked with the approval or at the direction of the President."[10] Military and naval installations were defined to include "any commercial establishment engaged in the development or manufacture of military or naval arms, munitions, equipment, designs, ships, or vessels for the United States Army or Navy."[11] The three classification levels used by the military (Secret, Confidential, and Restricted) were adopted by this EO. However, they were not explicitly defined in this EO.

The main effect of this EO was to establish presidential approval of what the Army and Navy were already doing. This EO also apparently gave governmental civilian employees the authority to classify information, because it provides that the information could be classified "with the approval or at the direction of the President"[12] in addition to being classified by authority of the Secretary of War or the Secretary of the Navy. Until this time, Army and Navy personnel and civilian employees of those services had been the only recipients of governmental classification directives. This EO did not list any sanctions for its violation, apparently relying upon those specified by the 1938 statute (not more than a $1000 fine or 1 year imprisonment or both).[9]

Executive Order 9182

On June 13, 1942, President Roosevelt signed Executive Order 9182, *Consolidating Certain War Information Functions into an Office of War Information*.[13] This executive order was issued under the authority of the First War Powers Act, 1941.[14] Executive Order 9182 established an Office of War Information (OWI) within the Office of Emergency Management in the Executive Office of the President. Although the OWI's functions were mostly concerned with gathering and disseminating public information on the war effort, its responsibilities also encompassed security of information policies. The OWI's classification regulations, although not issued as an EO, were issued under the authority of an EO.

[*] The 1938 statute was an act "to prohibit the making of photographs, sketches, or maps of vital military and naval defensive installations and equipment, and for other purposes" [52 Stat. 3 (Jan. 12, 1938)].

On September 28, 1942, the Director of OWI issued OWI Regulation No. 4, concerning security classification of information. This regulation was applicable throughout the government ["To the Heads of Executive Departments, Independent Establishments, and Other Government Agencies, Including Corporations," but perhaps was not applicable to the War Department and Navy Department (see below with respect to Change No. 1)] and controlled the identification, handling, and dissemination of sensitive information. Office of War Information Regulation No. 4 contained all the elements of a security classification of information system. Although this OWI classification system was said to be the first in our history to encompass information other than military and defense information,[15] it should be noted that its definitions of "information" and "classified information" (see below) referred only to "information relating to national defense." This September 1942 OWI regulation is said to be the forerunner of subsequent EOs dealing with classification.[16]

The memorandum distributing OWI Regulation No. 4 included the following statement:[17]

> The necessity for a uniform practice within the Government with regard to the security of information has become a matter of some urgency. Practice has differed markedly among the departments, with the result that some documents which should have been treated as secret have been permitted too free a circulation, while others which were in no sense secret or confidential have been improperly classified in these categories.[*]

In the preamble to Regulation No. 4, the OWI director stated the following:

> In order to provide uniform safeguards over information which might prove of aid or comfort to the enemy and to prevent undue restriction of information which may appropriately be made available to the public, the following regulations are hereby issued by virtue of the authority vested in me by Executive Order 9182.

"Information" and "classified information" were defined, as were three categories of classified information (the following definitions include changes made by an amendment of November 13, 1942, which modified the original definitions of Secret and Confidential information):

> The term "information" as used herein shall include documents, maps, charts, blueprints, photographs, models or other materials which convey information relating to national defense, as well as copies thereof obtained by any means of reproduction or transcription.
>
> The term "classified information" shall designate information relating to national defense requiring special provision for safeguarding. Information which needs no safeguarding shall be referred to as unclassified information.
>
> Secret Information is information the disclosure of which might endanger national security, or cause serious injury to the Nation or any governmental activity thereof.
>
> Confidential Information is information the disclosure of which although not endangering the national security would impair the effectiveness of governmental activity in the prosecution of the war.

[*] Note that these concerns are very similar to concerns cited in 1907 by the Army's Chief of Artillery and in 1917 by AEF General Order No. 64 (see Chapter 2).

> Restricted Information is information the disclosure of which should be limited for reasons of administrative privacy, or is information not classified as confidential because the benefits to be gained by a lower classification, such as permitting wider dissemination where necessary to effect the expeditious accomplishment of a particular project, outweigh the value of the additional security obtainable from the higher classification.

Note that the definition of Restricted, which permits "balancing" of classification costs and benefits, is closer to the then-current Navy definition than the Army's (see previous chapter). Note also that "classified information" (i.e., Secret, Confidential, or Restricted information) is "information relating to national defense requiring special provision for safeguarding" but that only Secret information's disclosure might endanger "national security." Thus, "national security" information seems to be an especially sensitive subset of "national defense" information in this OWI Regulation No. 4. The Army and Navy classification of information regulations of 1936 and 1938, respectively, and later, also defined "Confidential" information as not "national security" information (see previous chapter).

The head of each Federal agency or his designated representative was given the authority to classify information in all three categories. Overclassification was to be avoided:

> Documents or materials requiring classification shall be assigned the least restrictive classification consistent with the proper safeguarding of the information or material. Care should be taken to avoid overclassification, particularly in cases where undue restriction may prevent dissemination of information which should properly be disclosed to the public or Congress.

Classified documents, the pages of which were permanently and securely fastened together, were to be "plainly marked" with the appropriate classification designation on the cover, title page, and first page. Other documents whose pages were not permanently and securely fastened together were to be marked on the top and bottom of each page. Classified maps and photomaps were to be appropriately marked under the scale. Classified documents furnished to persons other than those in the Federal service were required to also have the following notation:

> This document contains information affecting the national defense of the United States within the meaning of the Espionage Act, 50 U.S.C. 31 and 32, as amended. Its transmission to or the revelation of its contents in any manner to an unauthorized person is prohibited by law.

Other information in this OWI Regulation No. 4 that is pertinent to the history of security classification of information is as follows:

> No person is entitled solely by virtue of his office or position to knowledge or possession of classified information. Except as provided by . . . [following subsections of the regulation] . . . such information is entrusted only to those individuals whose official duties require such information.
>
> The head of each agency may, by regulation, provide for the registration of secret or confidential information.

> The distribution of secret matter shall be held to the absolute minimum.
>
> Secret matters shall not be discussed over the telephone. Necessary references made to confidential matters over the telephone shall be held to the lowest practicable minimum.
>
> Cipher tables, alphabets and keys shall not be kept in the same container as the code books, documents, and devices to which they apply.
>
> In all agencies, appointed officers shall make an inspection immediately before the close of business to insure that all secret documents and cryptographic devices have been properly and safely put away.

The regulation also specifically cited the penalties of the Espionage Act. It is interesting to note that Confidential information could be discussed over an unsecure telephone line, although that practice was discouraged. Also of interest is the required end-of-the-day inspections with respect to Secret documents but the absence of comparable inspections for Confidential documents. This is perhaps consistent with the definition of Confidential information which stated that its disclosure would not endanger the national security.

By memorandum dated March 13, 1944, the Acting Director of OWI issued Change No. 1 to Office of War Information Regulation No. 4.[18] This Change No. 1 was to "be followed by all non-military Federal Departments and Agencies." Its major purpose was to implement the *Combined Security Classification Agreement*, which was an agreement between the United States and Great Britain on "definitions, classifications, and handling of matters to be safeguarded." A major result was the addition of "Top Secret" to the allowed classification categories.[*,†]

> Top Secret Information is information the security aspect of which is paramount and whose unauthorized disclosure would cause exceptionally grave danger to the nation.

Change No. 1 sometimes used the term "grading" to refer to "classification," evidently a result of the British influence on terminology. For example:

> Each document, or extract therefrom, except cryptographic material, shall be graded according to its own content and not necessarily according to its relationship to another document.
> It is the obligation of responsible authorities to keep classified matter under constant review

---

[*] An account of the administrative history of the Office of Scientific Research and Development (OSRD) indicated that the OSRD began using the "Top Secret" category in 1944. It was used primarily to protect operational information as the United States moved toward large-scale offensive war operations. This account also mentions the existence, for a short period of time, of a Navy classification of "Secret Security," which was more restrictive than Secret. The OSRD did not carry out any "Top Secret" projects because such classification resulted in a very inefficient use of their scarce manpower. Either the armed services carried out their own "Top Secret" projects or the classification was reduced to "Secret" before it was submitted to the OSRD (I. Stewart, *Organizing Scientific Research for War*, Little, Brown and Co., Boston, 1948, pp. 251-252).

[†] It should perhaps be noted that the Office of Scientific Research and Development issued an administrative circular on December 2, 1941, that provided Army and Navy guidance on U.S. practices for documents that had to be marked with both British and U.S. classification markings. U.S.-originated documents whose distribution would include the British were to be marked with one of three "double classifications," as appropriate to its U.S. classification: U.S. Secret - British Most Secret, U.S. Confidential - British Secret, U.S. Restricted - British Confidential [Administrative Circular 4.04 (*Classified information, documents or materials*), Office of Scientific Research and Development, Washington D.C., Dec. 2, 1941].

> and to downgrade it as soon as conditions permit.

This is perhaps the first specification of a requirement to review classified information for possible downgrading. It may also be the first use of the term "downgrading" in U.S. classification regulations. Previously, the term "reclassification" was used.

Concerning transmission of classified documents, Change No. 1 to OWI Regulation No. 4 stated the following:

> In transmitting a group of documents, or attachments or inclosures [sic] to a letter, each document, attachment, or letter will carry its own independent classification or no classification, consistent with the proper safeguarding of the information contained therein.
>
> A letter of transmittal or cover letter will be classified no lower than the highest classification of any of its inclosures. It should be noted that in some cases a letter may be deserving of a higher classification than any of its inclosures.

Other instructions of interest are the following:

> Top Secret documents will be of such a nature that only specifically designated individuals will handle them or originate them.
>
> The transmission and custody of Secret documents will normally be covered by a receipt system and registered documents periodically accounted for. It is mandatory that registered documents be covered by a receipt system.

Executive Order 9608 abolished all of the functions of OWI effective as of the close of business September 15, 1945. The office itself was abolished effective December 31, 1945.[19]

Executive Order 10104

The second EO dealing with classification of information, EO 10104, "Defining Certain Vital Military and Naval Installations and Equipment as Requiring Protection Against the General Dissemination of Information Relative Thereto," was issued by President Truman on February 1, 1950.[20] The authority for EO 10104 was based on the 1938 defense installation statute[6] and "in the interests of national defense." The three classification markings authorized by EO 8381 were continued, and a fourth marking, "Top Secret," was added. The Top Secret marking had been in use since 1944 under OWI regulations (see previous subsection) and perhaps earlier under Army or Navy regulations. None of those four classification markings were defined in this EO.

Executive Order 10104 used essentially the same definitions of vital military and naval installations or equipment as its predecessor EO 8381, except that it referred to prior authority for classification as being "the President, the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, or the Secretary of the Air Force."[21] The prior authorities for classification listed in EO 8381 were the Secretary of War or the Secretary of the Navy. Executive Order 10104 also included the new branch of the service, the Air Force, with respect to installations and

equipment. Executive Order 10104 was very similar to EO 8381, and its contents showed no influence from the wartime OWI classification regulations.

Executive Order 10290

On September 24, 1951, President Truman replaced EO 10104 with EO 10290,[22] effective 30 days after publication in the *Federal Register*. This EO was titled "Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information Which Requires Safeguarding in the Interest of the Security of the United States." In contrast with the two prior EOs, EO 10290 did not cite any specific statutory authority. The President relied on "the authority vested in me by the Constitution and statutes, and as President of the United States."

Executive Order 10290 provided a comprehensive system for identifying and protecting information, "the safeguarding of which is necessary in order to protect the security of the United States."[23] Classified information was to be designated as either Top Secret, Secret, Confidential, or Restricted and was also to be specifically identified as "Security Information."[24] Definitions were provided for terms such as classified security information, information, classify, security classification, unclassified information, document, material, agency, and cryptographic system.[25] Regulations were included to classify, upgrade, downgrade, declassify, disseminate, and handle (mark, transmit, store, and destroy) classified security information. Only the essentials of marking were required: the words "Security Information" and the appropriate classification had to appear on a document.[26]

Executive Order 10290 stated that "To avoid overclassification and depreciation of the importance of properly classified security information . . . security information shall be assigned its lowest security classification consistent with its proper protection."[27] The major criterion for the assignment of the "Top Secret" classification was that its unauthorized disclosure "would or could cause exceptionally grave danger to the national security."[27] Top Secret information "plainly requires the highest degree of protection." The "Secret" classification was to be given to information which required "extraordinary protection in the interest of national security."[27] "Confidential" information required "careful protection to prevent disclosures which might harm national security."[27] "Restricted" information concerned national security and required "protection against unauthorized use or disclosure, particularly information which should be limited to official use."[27] Note that all four classification levels in EO 10290 concerned national security, whereas OWI Regulation No. 4 definitions of Secret, Confidential, and Restricted, which were patterned after then-current Army and Navy classification regulations, stated that disclosure of Secret information would endanger national security but that the disclosure of Confidential or Restricted information would not endanger national security.

Executive Order 10290 made major changes in the government's classification system. Probably the most striking change was the extension, in peacetime, of the classification system to nonmilitary federal agencies, "To all departments and agencies of the Executive Branch."[28] An agency was defined as "any department or establishment within the Executive Branch, including any government corporation that is operated as an instrumentality of the Federal Government"[29] This EO represented a major departure from past practices. From the earliest days of our country until this

Order was promulgated, with the exception of World War II OWI Regulation No. 4, classification markings specified by military regulations or EOs primarily applied to the protection of defense information and rarely affected nonmilitary agencies.[30] This expansion of classification authority in peacetime to nonmilitary agencies and departments caused much concern (e.g., to Congress and the press) because of the potential restriction of the flow of information from these agencies to the public. This reaction is of interest, in retrospect, because the preface to the regulations stated that these regulations were being promulgated because "the furnishing of information to the public about government activities will be facilitated by clear identification and marking of those matters the safeguarding of which is required in the interests of national security."[31]

Another major change was to classify information on the basis of "national security," a term which is subject to broader interpretation than the term "national defense," which was the essential basis for the two previous EOs dealing with classification of information. [However, note that "national security" in OWI Regulation No. 4 had a narrower meaning than "national defense."]

Executive Order 10290 stated, "Documents shall be classified according to their own content and not necessarily according to their relationships to other documents. References to classified material which do not reveal classified security information shall not be classified."[32,*] This Order also provided for downgrading and declassification, both "automatic" and "nonautomatic."[33] It also provided for constant review of classified information for downgrading and declassification "as soon as conditions warrant."[34,†]

Sanctions for violations of EO 10290 were not specifically mentioned. However, the Order stated that, whenever practicable, "when classified security information affecting national defense is furnished authorized persons, in or out of Federal service, other than those in the Executive Branch, the following notation, in addition to the assigned classification marking, shall whenever practicable be placed on the material, on its container, or on the written notification of its assigned classification:"

> This material contains information affecting the national defense of the United States within the meaning of the espionage laws, Title 18, U.S.C., Secs. 793 and 794, the transmission or revelation of which in any manner to an unauthorized person is prohibited by law."[35]

Note that this admonitory marking was first used by the Army in its 1935 regulations concerning "Restricted" information ("technical" information at that time). This admonitory marking was also in OWI Regulation No. 4.

Each agency head was responsible for implementing these regulations in his agency. An agency head *could establish higher standards* than those in EO 10290 for identifying and protecting information.[36] The head of an agency could permit the discussion, over a nonsecure telephone line, of security information classified as Restricted if such security information originated within his

---

[*] This was a departure from Army and Navy classification regulations. See, for example, the Army regulation of 1936 which stated that "Documents classified as 'Secret' will not be referred to or listed in any catalog or publication which is not itself marked 'Secret,' . . ." [*Army Regulation* 330-5, 1936, §IV, Par. 18(c)]

[†] Similar to a requirement in Change No. 1 to OWI Regulation No. 4.

department.[37] The Attorney General was responsible for interpreting the regulations in connection with administrative problems.[38]

Executive Order 10290 specifically distinguished the term "Restricted" from "Restricted Data" and stated that the classification of Restricted Data was to be according to the provisions of the Atomic Energy Act.[39]

Executive Order 10501

In November 1953 President Eisenhower replaced EO 10290 with EO 10501, "Safeguarding Official Information in the Interests of the Defense of the United States,"[40] to be effective December 15, 1953. As authority for issuing this order, he cited "the authority vested in me by the Constitution and statutes, and as President of the United States," which was the same implied authority used by President Truman for EO 10290. Although essentially the same as EO 10290 in most respects, the new EO differed from the previous one in several ways. First, the new EO returned to "national defense" as the basis for classification, rather than "national security" which was cited in EO 10290. Thus, EO 10501 frequently mentioned information classified as "defense information," whereas EO 10290 had used the term "security information" in similar situations. Also, EO 10501 eliminated the "Restricted" classification level, keeping "Top Secret," "Secret," and "Confidential." All subsequent EOs have limited classification of information to those three levels. Also, EO 10501 was the first EO to specifically define each of the classification levels in distinct subsections of the order.

The "Top Secret" classification was to "be applied only to information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation."[41] Examples of this damage were cited: "leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense."[41]

The "Secret" classification applied to "defense information or material the unauthorized disclosure of which could result in serious damage to the Nation."[42] Examples of serious damage were "jeopardizing the international relations of the United States, endangering the effectiveness of a program or policy of vital importance to the national defense, or compromising important military or defense plans, scientific or technological developments important to national defense, or information revealing important intelligence operations."[42]

The "Confidential" classification applied to "defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the nation."[43]

Probably the most significant change occasioned by EO 10501 was the marked reduction in agency authority to classify information. Original classification authority was withdrawn from 28 entities, and in 17 others it was limited to the agency head.[44] Original classification authority was limited to those agencies having direct responsibility for national defense. For agencies having partial responsibility for national defense matters, original classification authority was limited to the agency head, without power of delegation. Agency personnel with original classification authority had to be specifically designated as having this authority.

A new area introduced in EO 10501 required agencies to designate "experienced persons to coordinate and supervise" agency activities under this order and required that these persons "maintain active training and orientation programs for employees concerned with classified defense information."[45] Individual employee responsibility in complying with this Order was emphasized.

The only classification-marking requirement was the classification designation; the prior EO had also required the words "Security Information." However, when a classification change was made, EO 10501 required, in addition to the new classification designation, an indication of the authority for the change, the date of the change, and the identity of the person making the change.[46]

The word "trustworthy" appeared in an EO for the first time with respect to access to information. Section 7 stated:

> Knowledge or possession of classified defense information shall be permitted only to persons whose official duties require such access in the interest of promoting national defense and only if they have been determined to be trustworthy.

The comparable requirement in EO 10290 had stated that "The dissemination of classified security information shall be limited to persons whose official duties require knowledge of such information."[47] Similar statements with respect to requiring access to classified information "as necessary for the performance of his duties" or "official duties" continued in Nixon and Carter EOs. The Reagan EO changed the wording to "provided that such access is essential to the accomplishment of lawful and authorized Government purposes."[48] The Clinton EO essentially retained the Reagan EO's less-stringent requirement for access to information: " 'need-to-know' means . . . requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function."[49]

The National Security Council (NSC) was assigned responsibility to conduct a continuing review of the implementation of the order.[50] Each agency was to delegate a staff member to conduct such a review within the agency.[51] The president was to designate a member of his staff to act on suggestions or complaints from non-governmental sources regarding the Order.[52] The Attorney General was responsible for interpreting the regulations with respect to administrative problems.[53]

President Eisenhower's EO 1050l remained in effect for nearly 20 years. Although subsequent EOs amended EO 10501, most were directed at changes in agency classification authority. An exception was President Kennedy's 196l EO 10964,[54] which dealt primarily with declassification procedures. Kennedy's EO placed classified information into four groups, two of which included information exempt from automatic declassification, one of which included information to be automatically downgraded at 12-year intervals, and a fourth group which contained information automatically downgraded at 3-year intervals and automatically declassified after 12 years. That EO also added a new Sect. 19 that provided for administrative sanctions against government employees knowingly responsible for the unauthorized release or disclosure of classified defense information or material.

Executive Order 11652

Executive Order 11652,[55] "Classification and Declassification of National Security Information," was issued by President Nixon on March 8, 1972, to be effective June 1, 1972. It was the result of an interagency committee study initially headed by William H. Rhenquist, later Chief Justice of the United States Supreme Court. The authority for this order was cited as "the Constitution and statutes of the United States." Subsequent EOs dealing with classification have cited essentially the same authority (the Constitution and laws of the United States). While incorporating most aspects of EO 10501, the new order made several major changes in the government's classification system. Classification was to be assigned to official information or material that required protection against unauthorized disclosure in the interest of the national defense or foreign relations ("national security") of the United States. The Eisenhower EO had defined classified information only in terms of "national defense."

EO 11652 used "reasonableness" as a test to determine whether information was Top Secret, Secret, or Confidential. For example, to be classified Top Secret, the test of information was "whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security."[56] President Truman's EO 10290 defined Top Secret information in terms of whether its unauthorized disclosure "would or could cause exceptionally grave danger to the national security."[27] President Eisenhower's EO 10501 used "could result in exceptionally grave damage to the Nation."[41]

Secret information was defined in terms of "whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security."[57] The test for Confidential information was "whether its unauthorized disclosure could reasonably be expected to cause damage to the national security."[58] As with the previous order, examples were given for Top Secret and Secret information but not for Confidential information.

Authority to originally classify information was restricted to those offices in the executive branch that were concerned with matters of national security. Top Secret original classification authority was withdrawn from 31 entities.[59] Twelve "Departments" were given Top Secret original classification authority. Thirteen "Departments" were given Secret original classification authority.

Appearing for the first time in an EO were prohibitions concerning classification. "In no case shall information be classified in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or Department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security."[60]

Also appearing for the first time was a requirement to "portion mark"[*] documents, to the extent practicable "to facilitate excerpting and other use."[61] The identity of the highest authority authorizing the classification of material was to be indicated on the face of the material classified.[62] Also to be shown was information concerning the applicability of the General Declassification Schedule (see below), the office of origin, the classification category, and the date of classification.[63]

[*] To "portion mark" means to assign a classification level (e.g., Secret), or "Unclassified," to each portion of a document. A portion may be a paragraph, a line, a title, graphics, etc. A chapter would not be a "portion" unless it only contained one paragraph. Subparagraphs of a document may be marked when appropriate. Duration of classification may be specified. See EO 12958 for the most recent portion-marking requirements.

Absent was the following statement, which appeared in EOs 10290 and 10501: "Documents shall be classified according to their own content and not necessarily according to their relationship to other documents."[32,64]

Executive Order 11652 included a "General Declassification Schedule" that provided for automatic downgrading or declassifying of classified material at specified intervals (Top Secret-to-Secret and Secret-to-Confidential at a 2-year interval; Confidential-to-Unclassified at a 6-year interval).[65] However, material could be exempted from this schedule by officials with Top Secret original classification authority.[66] Exempted material was required to undergo a classification review, on a specific request, after 10 years had elapsed from date of origin of the information or material.[67] Automatic declassification was specified for information or materials 30 years old or more.[68] However, information or material could be exempted from this automatic declassification by a written determination by the head of the originating department.[69]

The NSC monitored the implementation of EO 11652. To assist the NSC, an Interagency Classification Review Committee was established. The committee consisted of members of the Departments of State, Defense, and Justice; the Atomic Energy Commission (AEC); the Central Intelligence Agency (CIA); and the NSC staff, with a chairman designated by the President.[70] Among other responsibilities, the committee was to act on "suggestions or complaints from persons within or without the government" with respect to this order.[71]

The classification training and orientation programs that were first specified in EO 10501 received further attention in EO 11652. Such programs were to include briefings for new employees, periodic reorientations during employment, and debriefings upon termination of employment.[72]

Executive Order 11652, like EO 10964 which amended EO 10501, included statements concerning sanctions for violations of the order. Section 13(A) authorized administrative reprimands for repeated unnecessary classification or overclassification of information or material. "Prompt and stringent administrative action" was to be taken against employees responsible for unauthorized release or disclosure of classified information or material.[73] For violation of criminal statutes, the case was to be referred to the Justice Department. Note that EO 10964 specified sanctions only for unauthorized disclosures.[74]

Executive Order 12065

President Carter issued Executive Order 12065, "National Security Information," which replaced EO 11652, effective December 1, 1978.[75] This Order mentioned, at its beginning, the need "to balance the public's interest in access to Government information with the need to protect certain national security information from disclosure." "National security" meant "the national defense and foreign relations of the United States."[76] The definitions for Top Secret, Secret, and Confidential, referred to as "classification designations," were essentially the same as those in EO 11652, except that, to be Confidential, the criterion was "identifiable damage" rather than "damage." If there was reasonable doubt about the proper classification, "the less restrictive designation should be used, or the information should not be classified."[77]

Top Secret original classification authority was given to 13 agencies. Secret original classification authority was given to four agencies. Two agencies were given Confidential original classification authority.

The definitions for the classification designations did not give examples of what constituted Top Secret and Secret information, as did EO 10501 and EO 11652. However, EO 12065 identified seven areas with which information had to be concerned before it could be considered for classification.[78] Those were military plans, weapons, or operations; foreign government information; intelligence activities, sources, or methods; foreign relations or foreign activities of the United States; scientific, technological, or economic matters relating to the national security; U.S. government programs for safeguarding nuclear materials or facilities; or "other" categories specially determined by the president, a presidential designee, or an agency head.[79] If information concerned one of those areas, and "its unauthorized disclosure reasonably could be expected to cause at least *identifiable* damage to the national security [emphasis added]," then it could be classified.[80] Although prior EOs had not designated specific areas that could be classified, they had mentioned most of those areas in examples of what constituted Top Secret or Secret information, and EO 11652 had indicated other areas in the types of information exempt from the General Declassification Schedule.[81] Also, prior EOs had not required *identifiable* damage.

In addition to specifying "categories of information" related to the national security that could be classified, EO 12065 identified two of those categories as being especially sensitive. Section 1-303 stated that "Unauthorized disclosure of foreign government information or the identity of a confidential foreign source is presumed to cause at least identifiable damage to the national security." Executive Order 12065 was the first EO to state such presumptions. However, in EO 11652, foreign government information and intelligence sources were included in the categories of information eligible for exemption from the General Declassification Schedule.[82]

Executive Order 12065 contained, for the first time in an EO,[*] an explicit statement on balancing the public's right to be informed of governmental activities against national security requirments. Section 3-303 stated:

> It is presumed that information which continues to meet the classification requirements in Section 1-3 requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified.

Balancing was also mentioned in the preamble to the order (see above).

Maximum allowed duration of classification ranged from 6 to 30 years, depending upon specified criteria for the information. Documents classified for more than 6 years had to be marked with the name of the official who authorized the prolonged classification, and the reason for the

[*] The definition of "Restricted" in the Navy Department's 1938 regulations (see previous chapter) and the OWI Regulation No. 4 (this chapter) included a balancing "test." "*Restricted* matter is of such a nature that its disclosure should be limited for reasons of administrative privacy; or, is a matter not classified as *confidential* because the benefits to be gained by a lower classification outweigh the value of the additional security obtainable from the higher classification." [*United States Navy Regulations 1920*, 1938 reprinting, Art. 75 1/2, Par.(1)(b), p. 25(1).]

extended classification had to be noted on the document. Periodic review for classification was required for documents whose classification was extended beyond 20 years.

Prohibitions against classification (Sect. 1-601) were similar to those in the preceding order but added a prohibition against classification "to conceal violations of law."

Mention of basic research was included for the first time in an EO on classification of information. Section 1-602 stated that "basic scientific research information not clearly related to the national security may not be classified." Also new was a prohibition against reclassification of information: "Classification may not be restored to documents already declassified and released to the public under this Order or prior Orders."[83]

Derivative classification and classification guides were mentioned for the first time in an EO dealing with classification. Although "Derivative Classifiers" were not specifically defined, they were, by implication, "persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide."[84] Classification guides were discussed in Sects. 2-2 and 5-403. "Agencies with original classification authority shall promulgate guides for security classification that will facilitate the identification and uniform classification of information requiring protection under the provisions of this Order."[85] Each guide had to be approved by either an agency head or by a person with Top Secret original classification authority.[86]

Declassification was stressed in EO 12065: "Declassification of classified information shall be given emphasis comparable to that accorded classification."[87] Certain agency officials had the authority to determine that "the need to protect such information [which continued to meet classification requirements] may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified."[88]

The NSC was given responsibility of overall policy direction for the government's information security program.[89] This was the first explicit statement in an EO on responsibility for information security policy. The Administrator of General Services was responsible for implementing the order and for monitoring programs established pursuant to the order.[90] This responsibility was delegated to the Information Security Oversight Office (ISOO), a new Office which replaced the Interagency Classification Review Committee. The ISOO was an administrative part of the General Services Administration but received its policy direction from the NSC.

The Director of ISOO was to act on "complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program."[91] Appeals on certain declassification decisions could be taken to the ISOO Director and thence, in some instances, to the NSC.[92] This was the first specification in an EO of an appeals procedure for classification decisions.

Administrative sanctions were to be applied to "officers and employees of the U.S. Government" if they "knowingly and willfully" violated the provisions of the EO.[93]

An Interagency Information Security Committee was established by the order.[94] Membership included representatives from the Departments of State, Defense, Treasury, and Energy, the Attorney General, the Director of the CIA, the NSC, the Domestic Policy Staff, and the Archivist of the United States. Chairman of this committee was the Director of ISOO. "This Committee shall meet at the call of the Chairman or at the request of a member agency and shall advise the Chairman on implementation of this order."[95]

Executive Order 12356

Executive Order 12356, "National Security Information," was issued by President Reagan and became effective on August 1, 1982.[96] "National security" was defined in Sect. 6.l(e) as "the national defense or foreign relations of the United States" and was the same definition as in the prior EO. Information was defined in Sect. 6.l(b) to mean "any information or material, regardless of its physical form or characteristics, that is *owned by, produced by or for, or is under the control of the U.S. Government*" [emphasis added]. "National security information" was defined for the first time in an EO, in Sect. 6.1(c), to mean "information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated."

The definitions for Top Secret and Secret remained the same as in EO 12065, but the definition for Confidential was changed to require only "damage" to the national security, rather than "identifiable damage," as was required by the previous order. Prior to EO 12065, the criterion was "damage," so EO 12356 reverted to the criterion for Confidential information that was used prior to EO 12065. However, it should be noted that EO 12065 had stated that "information may not be classified unless . . . its unauthorized disclosure reasonably could be expected to cause at least identifiable damage to the national security." Therefore, EO 12356 eliminated the "identifiable damage" requirement for a determination that information was classified.

Section 1.1(c) of EO 12356 stated:

> If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

That was a change from the previous EO, which required that, if there was doubt, the less restrictive approach would be followed (the lower classification was to be used).

Section 1.3(a) of EO 12356 identified ten areas ("classification categories") with which information had to be concerned before it could be considered for classification. In addition to the seven areas specified by the previous EO, EO 12356 added "the vulnerabilities or capabilities of systems, installations, projects, or plans related to the national security," "cryptology," and "a confidential source." Additionally, EO 12356 added a parenthetical expression "including special

activities" to the area of intelligence activities so that this category of classifiable information now read "intelligence activities (including special activities), or intelligence sources or methods."

Executive Order 12356 stated that before information that concerned one or more of the ten categories could be classified, an original classifier had to determine "that its unauthorized disclosure, either by itself or in the context of other information, reasonably could cause damage to the national security."[97] This two-step process (determining category and damage) for classification of NSI was also required by the previous EO. However, EO 12356 added the phrase "either by itself or in the context of other information," which is said to be recognition of the "compilation" theory that has been used in the Department of Defense in special circumstances.[98] However, it seems more reasonable to interpret this in terms of classification of associations, rather than of compilations. Executive Orders 10290 and 10501 (Truman and Eisenhower) had stated that "Documents shall be classified according to their own content and not necessarily according to their relationships to other documents."[99] Such a statement was not in EOs 11652 or 12065.

Note that EO 12065 stated that "references to classified documents that do not disclose classified information may not be classified or used as a basis for classification."[100] Similar language was in earlier EOs.[32,60,63] That language was absent from EO 12356.

Section 1.3(c) stated a presumption that damage occurred on the disclosure of information in certain categories and thereby waived the damage-determination step of the classification process for those categories. That section stated that "unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security." This "presumption of damage" provision was expanded from EO 12065 to include intelligence sources or methods.

Section 1.3(d) stated that "information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or unauthorized disclosure in the United States or abroad of identical or similar information." This, together with a "no comment" policy on unofficial publications of information concerning classified projects, ensured that declassification actions were controlled by the government.

Executive Order 12356 abolished duration of classification of information limitations specified in prior EOs. Section 1.4(a) stated that "Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified." That was a significant change from EO 12065, which included 6-, 20-, and 30-year limitations for the duration of classification for certain types of information.

The markings required on classified documents or other forms of classified information were stated in Sect. 1.5(a). Those markings were (1) one of the three classification levels, (2) the identity of the original classification authority *if other than the person whose name appears as the approving or signing official*, (3) the *agency* and office of origin, and (4) the date or event for declassification *or the notation "Originating Agency's Determination Required*" (the requirements different from EO 12065 are italicized). Those markings were required unless a marking itself would reveal a confidential source or relationship not otherwise evident in the document or information.

The portion-marking requirement could be waived by agency heads for specific classes of documents or information.[101] The previous EO gave this waiver authority only to the ISOO Director.

Section 1.6(c) provided for the reclassification of declassified information under certain circumstances. This section stated that the president or a designated agency head or official "may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered." This statement contrasted with the previous EO, which stated that "classification may not be restored to documents already declassified and released to the public under this Order or prior Orders."[81]

Derivative classification was described in Part 2 of the order and was specifically defined in Sect. 2.1(a) as follows: "Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings." Other parts of Sect. 2.1, "Use of Derivative Classification," remained essentially the same as in Sect. 2.1 of the previous Order.

Section 2.2(b) of EO 12356 permitted classification guides to be approved by an official who "(1) has program or supervisory responsibility over the information or is the senior agency official designated . . . ; and (2) is authorized to classify information originally at the highest level of classification prescribed in the guide." The previous EO had required that classification guides be approved by an agency head listed in the order or by an official with Top Secret classification authority.

Absent from EO 12356 was a section that was in the previous EO that dealt with appropriate emphasis for declassification policy. Executive Order 12065 stated in Sect. 3-301:

> Declassification of classified information shall be given emphasis comparable to that accorded classification. Information classified pursuant to this and prior Orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or on the occurrence of a declassification event.

Executive Order 12356 had no provisions comparable to the first and third sentences of Sect. 3-301 of EO 12065.

Executive Order 12356 did not include an explicit statement on balancing the public's right to be informed of governmental activities against national security requirements. Such a statement was in EO 12065. However, the Preamble to EO 12356 stated that "it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure."[*] This acknowledgment of the positive and negative aspects of classification implied balancing those factors in classification decisions.

[*]President Truman's 1951 EO 10290 and all subsequent EOs included statements in their preambles concerning furnishing information to the public. Those statements became more explicit with each succeeding EO, with the statement in EO 12065 being the

Part 4 of EO 12356 described the safeguarding of classified information. A person is eligible for access to classified information, "provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes."[102] Prior EOs had been somewhat stricter in the requirement for access to classified information, using words such as "unless access is necessary for the performance of official duties."[103] Section 4.1(d) stated that, with some exceptions, "classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency."

As in the prior EO, the NSC was assigned responsibility for overall policy direction for the information security program, and the Administrator of General Services was assigned responsibility for implementing and monitoring the program established by the order.[104] The latter responsibilities were delegated to the ISOO Director by the order. The order did not establish any committees comparable to the Interagency Information Security Committee of the prior EO.

The sanctions to be imposed for violations of EO 12356 included "loss or denial of access to classified information,"[105] which was not present in the prior EO. Executive Order 12356 significantly expanded the group of persons subject to those sanctions from EO 12065's "officers and employees of the United States Government"[106] to "officers and employees of the United States Government, *and its contractors, licensees, and grantees*"[107] [emphasis added]. Thus, EO 12356 extended sanctions to contractors, licensees, and grantees in addition to governmental officers and employees. Also, the sanctions could be applied if someone "knowingly, willfully, or negligently" disclosed properly classified information to unauthorized persons.[108] The prior EO had not included "negligently" in its comparable section. The sanctions imposed by the EO itself did not extend beyond administrative sanctions; legal sanctions were imposed by "applicable law."

In general, EO 12356 is said to have reversed the trend, present in the two preceding EOs, towards classifying less information.[109] An explicit example of that change is that reclassification of information is permitted in certain instances. The provision in EO 12065 that specifically mentioned a "balancing" process in declassification decisions (public interest in disclosure balanced against national security requirements)[86] was omitted, although language implying such a process is contained in the Preamble to EO 12356. Because Section 1.3(a) of EO 12356 identifies ten areas of information that can be classified, compared with seven areas listed in the previous EO, these additional areas have been interpreted as a trend toward classifying more information. However, since cryptology, confidential sources, and vulnerabilities have always been considered as national security matters and thus protected against unauthorized disclosure, the additional areas could

---

most explicit.

"WHEREAS the furnishing of information to the public about government activities will be facilitated by clear identification and marking of those matters the safeguarding of which is required in the interest of national security" (EO 10290, Preamble).

"WHEREAS it is essential that the citizens of the United States be informed concerning the activities of their government" (EO 10501, Preamble).

"The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act and in the current public information policies of the executive branch" (EO 11652, Preamble).

See text for comparable information on EOs 12065, 12356, and 12958.

indicate an attempt to be more specific in delineating which information could be classified, therefore offering "better" (more detailed) classification guidance to original classifiers.

CLASSIFICATION UNDER EXECUTIVE ORDER 12958

Executive Order 12958, *Classified National Security Information*,[110] was issued by President Clinton on April 17, 1995, and became effective on October 16, 1995.

The process that led to EO 12958 formally began on April 26, 1993, with the issuance of Presidential Review Directive No. 19 (PRD-19). PRD-19 directed a review of "EO 12356 and other directives relating to the protection of national security information with a view toward drafting a new executive order that reflects the need to classify and safeguard national security information in the post Cold War period." The subsequent review by a 25-member interagency task force was chaired by the Director of ISOO and the final order was prepared in "an unprecedented environment of openness,"[111,*] which included (1) a 2-day public hearing with testimony of more than a dozen persons, (2) input from hundreds of persons from within and without the government, (3) a government-wide declassification conference, (4) input from Congress, and, of course, (5) significant input from the government agencies most concerned with classification and declassification of information.

The Preamble to EO 12958 is as follows:

> This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

Executive Order 12958 made many changes to the prior system for classifying and declassifying national security information. Those changes can be characterized as tending to provide more openness in the operation of our Government, an objective stated in the last sentence of the Preamble.

Executive Order 12958 extensively defines terms at the beginning of each Part of the

---

[*] "Unprecedented" may be somewhat exaggerated. President Carter's EO 12065 was the result of significant public and congressional input to a draft of the EO that was prepared by an interagency task group. However, President Reagan's EO 12356 was prepared essentially entirely by the executive branch of government, with essentially no input from the Congress or from the public. [U.S. Congress, House of Representatives, Committee on Government Operations, *Security Classification Policy and Executive Order 12356*, Twenty-Ninth Report by the Committee on Government Operations (Based on a Study by the Government Information and Individual Rights Subcommittee), House Report 97-731, 97th Congess, 2nd Sess., 1982, pp. 27-35.] Thus, with respect to the Reagan EO, the Clinton EO was indeed prepared in "an unprecedented environment of openness," but the Carter EO also was produced in a very open manner.

order, except the General Provisions part. Definitions in Part 1 include national security, information, classified national security information, foreign government information, classification, original classification, original classification authority, unauthorized disclosure, agency, senior agency official, confidential source, and damage to the national security. The order's definition of national security is unchanged from the prior EO. The definition of information is as follows:[112]

> "Information" means 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.

The prior EO's definition of information used the word "information" in that definition, whereas the new EO used the term "knowledge."[*] Also, the prior EO did not define "control."

The phrase "Classified national security information" or "classified information" is defined in EO 12958 to mean "information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure *and is marked to indicate its classified status when in documentary form* [emphasis added]."[113] The prior EO used the term "National security information" to describe information requiring protection. Perhaps the use of the term "classified national security information" is meant to explicitly distinguish between "classified" and "unclassified" national security information.[†] Also, the new EO is more explicit with respect to designating classified information, requiring that classified information be marked when in documentary form, whereas the prior EO only required that national security information be "designated."[114]

Of interest is the definition of "*damage* to the national security," which "means *harm* to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information" [emphasis added].[115] It would be of interest to know why the term "harm" was used to help define "damage" since both terms have essentially the same meaning.

The EO 12958 definition of agency was changed by Executive Order 12972,[116] effective September 18, 1995, to the following:

> Agency means an "Executive agency" as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into

[*] The Truman EO (10290) was the first, and only other, EO to use "knowledge" to define "information."

[†] The author is not aware of an official definition for "unclassified national security information." However, the Introduction section of Chapter 6, following, gives some recent examples of presidential broadening the scope of "national security," which might indicate the possible existence of "unclassified national security information."

In Sect. 3147 of the National Defense Authorization Act for Fiscal Year 2000 (S. 1059), Congress amended the Atomic Energy Act of 1954 by adding Section 234B, *Civil Monetary Penalties for Violations of Department of Energy Regulations Regarding Security of Classified or Sensitive Information or Data*. However, during rule-making proceedings to implement that new Sect. 234B, the Department of Energy (DOE) noted that DOE's proposed rule (10 CFR Part 824) did not include "sensitive information" because, *inter alia*, "Neither the statute nor its legislative history defines the term" and "there is no commonly accepted definition of "sensitive information" within DOE or the Executive Branch. [*Fed. Reg.* **67**(62), 15339-15344, 15340 (April 1, 2002)]

the possession of classified information.

A major change established by EO 12958 is the requirement that an original classification authority must *identify* or *describe* the damage to the national security before information can be classified.[117] The requirement that damage be "identifiable" before information could be classified first appeared in the Carter EO (12065) but was not in the Reagan EO (12356). Related changes are the requirement that "if there is significant doubt about the need to classify information, it shall not be classified"[118] and "if there is significant doubt about the appropriate level of classification, it shall be classified at the lower level."[119] The prior EO (12356) stated that "if there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority. . . . If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority . . . ."[120,*] Executive Order 12065 stated that "if there is reasonable doubt which designation [Top Secret, Secret, or Confidential] is appropriate, or whether the information should be classified at all, the less restrictive designation should be used, or the information should not be classified."[121] Thus, with respect to this guidance, EO 12958 is more "open" than the Reagan EO but not as open as the Carter EO.

Executive Order 12958 requires that original classification authorities be trained in original classification matters, but has no similar requirement for derivative classifiers.[122] Also, original classification authorities must indicate, on the face of the classified document, or on other classified media in an appropriate manner,[123] "a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order."[124] In addition to the identity of the original classification authority, his or her position title must be indicated on the face of a document.[125] Classification authorities must "whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document."[126]

Classification categories are reduced to seven in EO 12958, as compared to 10 in EO 12356. However, the reduction is mostly illusory because (1) "cryptology" and "confidential sources" were separate categories in EO 12356 but are combined with other categories in EO 12958 and (2) the "other" category in EO 12356 was eliminated, perhaps because it was so infrequently used.[127] A significant change was made with respect to the presumption of classification of certain of these categories. Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods was presumed to cause damage to the national security in EO 12356.[128] This presumption is absent in EO 12958.

Perhaps the biggest change made by EO 12958 is the reintroduction of time limits on classification of information. At the time of classification, the original classification authority should try to establish a date or event for declassification (no change from previous EO), but not longer than 10 years.[129] However, if such a declassification duration cannot be established, then the document is to be marked for declassification after 10 years.[130] (The prior EO's comparable requirement was that

[*] Unfortunately, the EO did not provide guidance to an original classification authority should do if he or she had "reasonable doubt."

the classifier could specify "Originating Agency's Determination Required" for the classification duration.) At the time of classification, the original classifier can exempt the information from the 10-year declassification requirement under certain circumstances.[131] The declassification instructions must be indicated on the face of a document.[132] A consequence of this change is that, under prior EOs, agencies had to commit resources to declassify information; under the new EO, agencies have to commit resources to exempt information from automatic declassification.

Portion-marking requirements are continued in this EO, with the addition that each portion exempt from automatic declassification had to be identified.[133] Reclassification of information is forbidden "after it has been declassified and released to the public under proper authority."[134]

Classification of compilations of information are specifically addressed in this EO in Sect. 1.8(e):

> Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information. As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Authorized holders of classified information are encouraged (and expected) to challenge the classification status of information that they believe is improperly classified or unclassified.[135]

Part 2 of the EO, concerning derivative classification, includes definitions of derivative classification, classification guidance, classification guide, source document, and multiple sources. When derivative classification is based on multiple sources, derivative classifiers must list, on the official file or record copy of the document, all of those sources.[136] Another new requirement in this section is to assure that classification guides are reviewed and updated periodically.

Part 3 of the EO concerns declassification and downgrading. Definitions are provided for declassification, automatic declassification, declassification authority, mandatory declassification review, systematic declassification review, declassification guide, downgrading, and file series. Policy that first appeared in EO 12065, but was absent from EO 12356, reappeared in EO 12958:[137]

> It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified.

The explicit statement of such a "balancing" requirement is considered to be a major indication of the "openness" policy of this EO.

Decisions by the Director of ISOO that direct an agency to declassify information can be appealed to the president.[138] Previously, the appeal was to the NSC.

Section 3.4 of the order, "Automatic Declassification," established major new requirements.

Within 5 years[*] of the date of the order, all records that are more than 25 years old and that have permanent historical value (as defined in 44 U.S.C.) are to be automatically declassified. This declassification is effective whether or not the records have been reviewed for classification. Subsequently, all such records are automatically declassified no longer than 25 years from the date of the original classification. Exemptions from this requirement were provided. (See below for a discussion of the impacts of this requirement.)

In November 1999, Sect. 2 of Executive Order 13142[139] amended EO 12958 to add new language at the end of Sect. 3.4(a) to extend the automatic declassification date for certain records to 8 years from the date of EO 12958. Such records were those that contained information classified by more than one agency and records that contained significant numbers of documents concerning intelligence sources and methods.

Agencies are required to conduct systematic declassification reviews of historically valuable records exempted from automatic declassification.[140]

The Archivist of the United States is required to establish a government-wide database of declassified information.[141] All declassified information in this database, with certain exceptions, is to be made available to the public.[142]

This order changed the administrative responsibility implementing the order. Formerly, the Administrator for General Services was responsible for implementing the order. Executive Order 12958 assigned responsibility for issuing directives to implement the order to the Director of the Office of Management and Budget (OMB) in consultation with the Assistant to the President for National Security Affairs (the head of the NSC) and the co-chairs of the Security Policy Board.[143,†] The implementation and monitoring functions were delegated by the order to the Director of ISOO. ISOO's administrative location was now within the OMB. Executive Order 13142[144] issued in November 1999, amended EO 12958 to assign the authority for issuing directives to implement EO 12958 to the Director of ISOO under the direction of the Archivist of the United States rather than to the OMB Director. Also, the location of ISOO was changed from the OMB to the Archivist of the United States. The Archivist appoints the director of ISOO, subject to the approval of the president.

Executive Order 12958 did not explicitly assign responsibility for either classification policy or information-security policy, which had formerly been assigned to the NSC. It is likely that this responsibility had been assigned to the Security Policy Board by Presidential Decision Directive 29 of November 1994, but EO 12958 did not so indicate. It is not likely that classification policy matters were assigned to the Information Security Policy Advisory Council (see below), which was to be appointed by the president and was to consist of nongovernmental employees. A Classification

[*] This was changed to 6 1/2 years by Sect. 1 of Executive Order 13142, *Fed. Reg.* **64**, 63169, Nov. 23, 1999.

[†] The Security Policy Board (SPB) was established by Presidential Decision Directive 29 of September 16, 1994. The SPB is under the Assistant to the President for National Security Affairs and was created by designating the Joint Security Executive Committee, established by the Deputy Secretary of Defense and the Director of Central Intelligence, as the SPB. The SPB was an interagency body that was to develop integrated and coherent security policies, including classification policies. In 1995, it was said that the SPB was dominated by the Central Intelligence Agency and was attempting to take over management of the government's classification function, which was then an ISOO function. (Steven Aftergood, "Security Policy Board Delays New Executive Order," *Secrecy and Government Bulletin*, **46**, March-April 1995, Federation of American Scientists, Washington, D.C.)

Management Committee was created in 1995 by the Security Policy Forum under the sponsorship of the Security Policy Board. The mission of the Classification Management Committee, as propounded in its draft charter, was:

> To coordinate, formulate and evaluate the U.S. Government's classification management policy, the purpose of which is to prescribe a uniform system for classifying and declassifying national security information. Such policy shall be flexible, threat driven, cost effective and emphasize a commitment to an open government.

Membership in this committee was to consist of one voting representative from each organization (about 30) belonging to the Security Policy Forum. The Director of ISOO was to be chairman of the committee, responsible for assigning tasks, establishing working groups, and recommending policy to the Security Policy Board through the Security Policy Forum. Voting was to be at the discretion of the chairman. Little information is publicly available concerning the activities of the Classification Management Committee.[*]

Several changes and new requirements were included in Part 5 of the EO, "Implementation and Review." Definitions were included for "self-inspection," "violation," and "infraction." An Interagency Security Classification Appeals Panel (ISCAP) was established. The secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs are each to appoint a member, with the president to select one of the appointees to serve as Chair. The Director of ISOO is the ISCAP executive secretary. The functions of ISCAP are to decide on appeals by persons who have filed classification challenges, to act on agency requests for exemptions from automatic declassification, and to decide on appeals from requests for mandatory declassification reviews. In October 2000, the ISCAP reported that since its formation it had acted on 218 appeals seeking declassification of documents.[145] In 80% of those appeals (176 documents), the documents were declassified in whole or in part.

In 1999, the Department of Justice dismissed a claim by the Director of Central Intelligence that he possessed independent authority (i.e., under the National Security Act of 1947) to classify information concerning intelligence sources and methods and that his classification decisions in those areas were not subject to substantive review by ISCAP.[146] However, the document in question was subsequently withheld (not declassified) by ISCAP.[147]

An Information Security Policy Advisory Council ("Council") was also established. "The Council shall be composed of seven members appointed by the President for staggered terms not to exceed 4 years, from among persons who have demonstrated interest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government."[148] The functions of the Council are to advise the President or other appropriate executive branch officials on policies established under EO 12958, to provide recommendations to agency heads on

[*] President George W. Bush issued National Security Presidential Directive 1 on February 13, 2001. Among other changes, this directive abolished the Security Policy Board (and several other entities) effective March 1, 200l. Security Policy Board duties established in Presidential Decision Directive 29 were transferred to various National Security Council Policy Coordination Committees (NSC/PCC) which "shall be the main day-to-day fora for interagency coordination of national security policy." Seventeen NSC/PCCs were established; classification policy (and the Classification Management Committee) was assigned to the Records Access and Information Security PCC, chaired by the Assistant to the President for National Security Affairs.

subject areas for systematic declassification review, and to serve as a forum for discussing policy issues in dispute.[149] So far as is known, this Council has not yet been established.

Under Sect. 5.6, heads of agencies are to make several commitments regarding implementing the order, including establishing an ongoing self-inspection program and assuring that performance-management matters include management of classified information as a critical element of performance review. Also, costs of classification are to be accounted for and reported.

Executive Order 12958 added "certificate holders"[*] to the list of entities subject to sanctions under this order[150] and expanded the actions subject to sanctions to include "knowingly, willfully, or negligently" contravening "any other provision of this order or its implementing directives."[151] Also added under "Sanctions" was the following:[152]

> 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 this order.

Executive Order 12958 states that nothing in the order supersedes requirements of the Atomic Energy Act of 1954 or the National Security Act of 1947.[153] The National Security Act of 1947 had not been cited in prior EOs with respect to this matter.

Finally to be noted is the following statement at Sect. 6.1(c) of the EO:

> This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees.

This perhaps means that someone with a classification-question lawsuit against one or more of the mentioned parties cannot use the provisions of EO 12958 as a basis for requesting a court to substantively review an agency's classification decision.

One of the major effects of EO 12958 has been the release by government agencies of large volumes of previously classified information. The ISOO *1999 Report to the President* reported that under the Automatic and Systematic Review Declassification programs, about 127 million pages of historically valuable records were declassified during 1999. During the first four years of EO 12958, about 720 million pages have been declassified. This represents about 80% of *all* documents that have been declassified since Fiscal Year 1980.[154] (See Chapter 5 for some information about inadvertent releases of classified atomic energy information in some of that released information.)

The implementing directive for EO 12958 was prepared by ISOO and issued on October 13, 1995.[155] It is codified at 32 CFR Part 2001.

---

[*] The term "certificate holder" is used exclusively by the Nuclear Regulatory Commission (NRC). The NRC usually grants licenses to entities that it regulates, with the exception of USEC, Inc., which operates the gaseous-diffusion uranium-enrichment plant at Paducah, Kentucky. (Until June 2001, USEC also operated a gaseous-diffusion uranium-enrichment plant at Portsmouth, Ohio.) USEC's operation of the gaseous-diffusion plant at Paducah is regulated by the NRC under a "certificate of compliance" and USEC is a "certificate holder." [Private communication from Philip Calabrese, Information Security Oversight Office, August 2, 2001.]

Tables 3.1.A through 3.1.D compare some aspects of the eight EOs that have been issued to regulate classification of information in the United States.

Table 3.1.A. Comparison of some aspects of Executive Orders for classification of information

EO; issue date; President	Authority for promulgation	Primary basis for classification	Classification levels[a]	Tests for classification
EO 8381; 3/22/40; F. D. Roosevelt	Sect. 1 of 52 Stat. 3 1/12/38	National defense	S R C	None specified
EO 10104; 2/1/50; H.S. Truman	18 U.S.C. §§795, 797 "and in the interests of national defense"	National defense	TS S C R	None specified
EO 10290; 9/24/51 (effective 10/27/51); H. S. Truman	"The Constitution and statutes, and as President of the United States"	National security	TS S C R	Unauthorized disclosure would or could cause exceptionally grave damage to the national security. Requires extraordinary protection in the interest of national security. Requires careful protection to prevent disclosures which might harm national security. Has such bearing upon national security as to require protection against unauthorized use or disclosure.
EO 10501; 11/5/53 (effective 12/15/53); D. D. Eisenhower	Same as EO 10290	National defense	TS S C	Applied only to that information or material the defense aspect of which is paramount and the unauthorized disclosure of which could result in exceptionally grave damage to the nation. Defense information or material the unauthorized disclosure of which could result in serious damage to the nation. Defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the nation.
EO 11652; 3/7/82 (effective 6/1/72); R. M. Nixon	"The Constitution and statutes of the United States"	National security (national defense or foreign relations)	TS S C	Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Unauthorized disclosure could reasonably be expected to cause damage to the national security.
EO 12065; 6/28/78 (effective 12/1/78); J. Carter	"As President by the Constitution and laws of the United States of America"	National security (national defense and foreign relations)	TS S C	Unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security. Unauthorized disclosure reasonably could be expected to cause serious damage to the national security. Unauthorized disclosure reasonably could be expected to cause identifiable damage to the national security.
EO 12356; 4/2/82 (effective 8/1/82); R. W. Reagan	Same as EO 12065	National security (national defense or foreign relations)	TS S C	Same as EO 12065 except "identifiable" is omitted from the test for Confidential information.
EO 12958; 4/17/95 (effective 10/15/95); W. J. Clinton	Same as EO 12065	Same as EO 12356	TS S C	Same as EO 12356 except that to each "test" for classification another requirement was added: "the original classification authority" had to be "able to identify or describe" the damage. E.g., "'Top Secret' shall be 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."

a. TS = Top Secret, S = Secret, C = Confidential, R = Restricted

Table 3.1.B. Comparison of some aspects of Executive Orders for classification of information

EO; issue date; President	Information classified	Federal agencies, departments, etc., authorized to classify information	People with original classification authority
EO 8381; 3/22/40; F. D. Roosevelt	Information relative to certain vital military and naval installations or equipment, including official military or naval books, pamphlets, documents, etc.	2 [War (Army) and Navy]	Military/civilian officials in War and navy depts.
EO 10104; 2/1/50; H.S. Truman	Essentially the same as in EO 8381.	1 (DoD)	Military/civilian officials in DoD.
EO 10290; 9/24/51 (effective 10/27/51); H. S. Truman	"Official information the safeguarding of which is necessary in the interests of national security" (security information).	All executive branch department and agencies.	Military/civilian officials in all of the federal government.
EO 10501; 11/5/53 (effective 12/15/53); D. D. Eisenhower	"Official information [or material] which requires protection in the interest of national defense" (defense information).	All agencies having responsibility for national defense (47 eventually;[b] 28 fewer than under EO 10290[c]).	59,316 in 1971[d]
EO 11652; 3/7/82 (effective 6/1/72); R. M. Nixon	"Official national security information or material."	Those designated by the President in writing, heads of agencies listed in the EO, and those designated in writing by the agency heads. TS: 12 agencies; S: 25 agencies C: 25 agencies.	21,277 in 1972[d] 13,976 in 1976[d]
EO 12065; 6/28/78 (effective 12/1/78); J. Carter	"Information or material . . . that is owned by, produced for or by, or under the control of, the United States Government, and that has been determined pursuant to this Order or prior Orders to require protection against unauthorized disclosure and that is so designated" ("classified information").	The President, those designated by the President in the Federal Register, agency heads listed in the EO, and officials delegated this authority pursuant to the EO. TS: 13 agencies; S: 17 agencies; C: 19 agencies.	7056 in 1982[d]
EO 12356; 4/2/82 (effective 8/1/82); R. W. Reagan	Same as EO 12065 except that it was called "national security information" instead of "classified information."	The President, those designated by the President in the Federal Register, and officials delegated this authority pursuant to the EO. TS: 24 agencies[e]; S: 30 agencies[e]; C: 33 agencies.[e]	6756 in 1986[d] TS: 1502 S: 4147 C: 1107
EO 12958; 4/17/95 (effective 10/15/95); W. J. Clinton	Similar to EO 12065 but information classified (1) is designated "classified national security information" instead of "national security information," and (2) "is marked to indicate its classified status when in documentary form" (EO 12065 specified that the information had to be "so designated" [as classified information]).	The President, those designated by the President in the Federal Register, and U.S. Government officials delegated this authority pursuant to the EO.	5661 in 1993[f] 3846 in 1999[g] 4130 in 2000[h]

b. Ref. 4, p. 38.
c. Ref. 44.
d. Information Security Oversight Office, *Annual Report to the President, FY 1986*, March 1987, p. 12.
e. Presidential order of May 7, 1982, *Fed. Reg.*, **47**, 20105.
f. Information Security Oversight Office, *Annual Report to the President, FY 1993*.
g. Information Security Oversight Office, *Annual Report to the President, FY 1999*.
h. Information Security Oversight Office, *Annual Report to the President, FY 2000.*

Table 3.1.C. Comparison of some aspects of Executive Orders for classification of information

EO; issue date; President	Classification categories	Duration of classification	Provisions for downgrading or declassifying	Automatic downgrading or declassifying
EO 8381; 3/22/40; F. D. Roosevelt	None specified	Not specified	None specified	Not specified
EO 10104; 2/1/50; H.S. Truman	None specified	Not specified	None specified	Not specified
EO 10290; 9/24/51 (effective 10/27/51); H. S. Truman	None specified	Could be specified by classifier (declassification after a specified date or event).	Yes	Whenever practical; specified by classifier.
EO 10501; 11/5/53 (effective 12/15/53); D. D. Eisen-hower	None specified (Examples of TS and S information were given)	Same as EO 10290. Amended by President Kennedy's 1961 EO 10964, which provided for automatic declassification of certain classified information.	Yes	To the fullest extent practical; specified by classifier.
EO 11652; 3/7/82 (effective 6/1/72); R. M. Nixon	None specified (Examples of TS and S information were given)	6 to 10 years for some items; indefinite for others.	Yes	Yes, except when exempted.
EO 12065; 6/28/78 (effective 12/1/78); J. Carter	7	Declassification date or event could be specified by classifier. No more than 6 years except when specifically exempted.	Yes	Yes; specified by classifier except when exempted.
EO 12356; 4/2/82 (effective 8/1/82); R. W. Reagan	10	Could be specified by classifier (declassification after a specified date or event).	Yes	Specified by classifier. Automatic declassifications under predecessor EOs to remain valid unless extended.
EO 12958; 4/17/95 (effective 10/15/95); W. J. Clinton	7	Specified by classifier but no longer than 10 years except when specifically exempted. Automatic declassification of documents more than 25 years old, except where exempted.	Yes	Yes, except when exempted.

Table 3.1.D. Comparison of some aspects of Executive Orders for classification of information

EO; issue date; President	Source of policy direction	Implementation responsibility	Administrative sanctions for violations	Misc.
EO 8381; 3/22/40; F. D. Roosevelt	Not specified. (Perhaps Secretaries of War and Navy.)	Not specified. (Perhaps Secretaries of War and Navy.)	None specified. (Perhaps those penalties of the 1938 Statute.)	
EO 10104; 2/1/50; H.S. Truman	Not specified.	Not specified. (Perhaps Secretaries of Defense, Air Force, Army, and Navy.)	None specified. (Perhaps those penalties of the 1938 Statute.)	Added Top Secret as a classification level.
EO 10290; 9/24/51 (effective 10/27/51); H. S. Truman	These "regulations" interpreted by the Attorney General with respect to administrative problems. Source of policy direction not mentioned.	Agency heads. (They could establish higher standards than the EO.)	None specified, although documents sent to certain recipients were to be marked to refer to the U.S. espionage laws, which specified penalties.	Extended classification authority, in peacetime, to non-defense federal agencies.
EO 10501; 11/5/53 (effective 12/15/53); D. D. Eisenhower	Interpreted by the Attorney General.	Agency heads. National Security Council to monitor implementation.	Same as for EO 10290. Amended by Pres. Kennedy's EO 10964 of 9/22/61 to provide sanctions on employees and officers of the U.S. Government for unauthorized disclosure of classified information.	Removed "Restricted" as a classification level. Classification training and orientation programs were required.
EO 11652; 3/7/82 (effective 6/1/72); R. M. Nixon	Interpreted by the Attorney General. Policy direction by the President through the National Security Council.	Agency heads. National Security Council to monitor implementation. Interagency Classification Review Committee to assist the National Security Council.	Sanctions for officers and employees of the U.S. Government for unauthorized disclosures and certain underclassification or overclassification.	A portion-marking requirement was added.
EO 12065; 6/28/78 (effective 12/1/78); J. Carter	National Security Council.	General Services Administration. Delegated to the Information Security Oversight Office.	Sanctions for officers and employees of the U.S. Government for "knowlingly and willfully" violating provisions of the EO.	A "balancing" test for classification was added, for certain instances. Declassification was emphasized.
EO 12356; 4/2/82 (effective 8/1/82); R. W. Reagan	National Security Council.	General Services Administration. Delegated to the Information Security Oversight Office.	For officers and employees of the U.S. Government, its contractors, licensees and grantees. "Negligently" added to one criterion for sanctions.	Abolished duration of classification limitations of prior EOs.
EO 12958; 4/17/95 (effective 10/15/95); W. J. Clinton	Not clear. (See text of this report).	Archivist of the U.S. (via EO 13142) and delegated to the Information Security Oversight Office.	As under EO 12356, plus "certificate holders."	Established time limits on information classification. Classified records more than 25 years old and of permanent historical value to be automatically declassified unless exempted.

REFERENCES

[1] "United States," Sect. 47, *American Jurisprudence*, 2nd ed., Vol. 77, The Lawyers Co-operative Publishing Co., Rochester, N.Y., 1975.

[2] *Jenkins v. Collard*, 145 U.S. 546 (1891).

[3] H. C. Relyea, "The Evolution of Government Security Classification Policy: A Brief Overview (1775–1973)," pp. 842-884 in *Government Secrecy, Hearings Before the Subcommittee on Intergovernmental Relations of the Committee on Government Operations*, U.S. Senate, 93d Congress, 2d Sess., 1974, p. 856.

[4] U.S. Congress, House of Representatives, Committee on Government Operations, *Executive Classification of Information–Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act (5 U.S.C. 552)*, Third Report by the Committee on Government Operations, House Report 93-221, 93d Cong., 1st Sess., 1973, p. 62. Hereafter, this report is cited as "HR 93-221."

[5] 61 Stat. 495 (1947), 50 U.S.C. §§401-426.

[6] 50 U.S.C. §403(d)(3).

[7] 50 U.S.C. §783.

[8] Executive Order No. 8381, *Fed. Reg.* **5**, 1147 (Mar. 26, 1940).

[9] Act of January 12, 1938, Ch. 2, §§1-5, 52 Stat. 3; codified at 18 U.S.C. §§795, 796, 797.

[10] Executive Order No. 8381, §3.

[11] Executive Order No. 8381, §1(f).

[12] Executive Order No. 8381, §1.

[13] Executive Order No. 9182, *Fed.Reg.* **7**, 4468 (June 16, 1942).

[14] *First War Powers Act, 1941*, 55 Stat. 838 (Dec. 18, 1941).

[15] A. M. Cox, *The Myths of National Security: The Peril of Secret Government*, Beacon Press, Boston, 1975, p. 37.

[16] HR 93-221, p. 7.

[17] *To the Heads of all Departments and Agencies*, Memorandum from Elmer Davis, Director, Office of War Information, Washington, D.C., September 28, 1942.

[18] *To the Heads of all Departments and Agencies*, Memorandum from Edward Klauber, Acting Director, Office of Waste Information, Washington, D.C., March 13, 1944.

[19] Executive Order No. 9608, *Fed. Reg.* **10**, 11223 (Sept. 1, 1945).

[20] Executive Order No. 10104, *Fed. Reg.* **15**, 597 (Feb. 3, 1950).

[21] Executive Order No. 10104, §§1-3.

[22] Executive Order No. 10290, *Fed. Reg.* **16**, 9795 (Sept. 27, 1951).

[23] Executive Order No. 10290, Part I, §1(a).

[24] Executive Order No. 10290, Part I, §2.

[25] Executive Order No. 10290, Part II.

[26] Executive Order No. 10290, Part VI, §32.

[27] Executive Order No. 10290, Part IV, §25(b).

[28] Executive Order No. 10290, Preamble.

[29] Executive Order No. 10290, Part II, §9.

[30] HR 93-221, pp. 8-9.

[31] Executive Order No. 12090, Preface.

[32] Executive Order No. 10290, Part IV, §26(d).

[33] Executive Order No. 10290, Part IV, §§28(a) and (b).

[34] Executive Order No. 10290, Part IV, §28(c).

[35] Executive Order No. 10290, Part VI, §32(c).

[36] Executive Order No. 10290, Part I, §1.
[37] Executive Order No. 10290, Part V, §(d).
[38] Executive Order No. 10290, Part VII, §36.
[39] Executive Order No. 10290, Part IV, §25(c).
[40] Executive Order No. 10501, *Fed. Reg.* **18**, 7049 (Nov. 10, 1953).
[41] Executive Order No. 10501, §1(a).
[42] Executive Order No. 10501, §1(b).
[43] Executive Order No. 10501, §1(c).
[44] R. C. Ehlke and H. C. Relyea, "The Reagan Administration Order on Security Classification: A Critical Assessment," *Fed. Bar News J.* **30** (2), 91-97 (February 1983), p. 92. Hereafter, this article is cited as "Ehlke and Relyea."
[45] Executive Order No. 10501, §10.
[46] Executive Order No. 10501, §5(h).
[47] Executive Order No. 10290, Part V, §30(a).
[48] Executive Order No. 12356, Part 4, §4.1(a).
[49] Executive Order No. 12958, Part 4, §4.1(c).
[50] Executive Order No. 10501, §17.
[51] Executive Order No. 10501, §18.
[52] Executive Order No. 10501, §16.
[53] Executive Order No. 10501, §11.
[54] Executive Order No. 10964, *Fed. Reg.* **26**, 8932 (Sept. 22, 1961).
[55] Executive Order No. 11652, *Fed. Reg.* **37**, 5209 (Mar. 10, 1972).
[56] Executive Order No. 11652, §1(A).
[57] Executive Order No. 11652, §1(B).
[58] Executive Order No. 11652, §1(C).
[59] Ehlke and Relyea, p. 93.
[60] Executive Order No. 11652, §4.
[61] Executive Order No. 11652, §4(A).
[62] Executive Order No. 11652, §4(B).
[63] Executive Order No. 11652, §4(A).
[64] Executive Order No. 10501, §3(a).
[65] Executive Order No. 11652, §5(A).
[66] Executive Order No. 11652, §5(B).
[67] Executive Order No. 11652, §5(C).
[68] Executive Order No. 11652, §5(E).
[69] Executive Order No. 11652, §5(E)(1).
[70] Executive Order No. 11652, §7(A).
[71] Executive Order No. 11652, §7, Par. (A)(2).
[72] Executive Order No. 11652, §7(B)(3).
[73] Executive Order No. 11652, §13(B).
[74] Executive Order No. 10964, Item 6.
[75] Executive Order No. 12065, *Fed. Reg.* **43**, 28949 (July 3, 1978).
[76] Executive Order No. 12065, §6-104.
[77] Executive Order No. 12065, §1-101.
[78] Executive Order No. 12065, §1-301.

[79] Executive Order No. 12065, §§1-301(a)-(g).
[80] Executive Order No. 12065, §1-302.
[81] Executive Order No. 11652, §5(B).
[82] Executive Order No. 11652, §5(B).
[83] Executive Order No. 12065, §1-607.
[84] Executive Order No. 12065, §2-101.
[85] Executive Order No. 12065, §5-403.
[86] Executive Order No. 12065, §2-202.
[87] Executive Order No. 12065, §3-301.
[88] Executive Order No. 12065, §3-303.
[89] Executive Order No. 12065, §5-101.
[90] Executive Order No. 12065, §5-102.
[91] Executive Order No. 12065, §5-202(b).
[92] Executive Order No. 12065, §5-202(b) and (c).
[93] Executive Order No. 12065, §5.5.
[94] Executive Order No. 12065, §5-3.
[95] Executive Order No. 12065, §5-303.
[96] Executive Order No. 12356, *Fed. Reg.* **47**, 14874 (Apr. 6, 1982).
[97] Executive Order No. 12356, §1.3(b).
[98] A. F. Van Cook, "Information Security and Technology Transfer (An OUSD Overview of Executive Order 12356 and DoD's View Concerning Implementation)," *J. Natl. Class. Mgmt. Soc.* **18**, 1-7 (1982), p. 3.
[99] Executive Order No. 10290, Part IV, §26(d). Executive Order No. 10501, §3(a).
[100] Executive Order No. 12065, §1-604.
[101] Executive Order No. 12356, §1.5(b).
[102] Executive Order No. 12356, §4.1(a).
[103] Executive Order No. 12065, §4-101.
[104] Executive Order No. 12356, §5.1.
[105] Executive Order No. 12356, §5.4(c).
[106] Executive Order No. 12065, §5-502.
[107] Executive Order No. 12356, §5.4(b).
[108] Executive Order No. 12356, §5.4(b)(1).
[109] Ehlke and Relyea, pp. 91, 94, 96.
[110] Executive Order No. 12958, *Fed. Reg.* **60**, 19823-19843 (April 20, 1995).
[111] *Statement by the President* upon the release of Executive Order 12598, The White House, April 17, 1995.
[112] Executive Order No. 12958, Part 1, §1.1(b).
[113] Executive Order No. 12958, Part 1, §1.1(c).
[114] Executive Order No. 12356, §6.1(c).
[115] Executive Order No. 12958, Part 1, §1.1(l).
[116] Executive Order No. 12972, *Fed. Reg.* **60**, 48863 (Sept. 21, 1995).
[117] Executive Order No. 12958, Part 1, §1.2(a)(4).
[118] Executive Order No. 12958, Part 1, §1.3(b).
[119] Executive Order No. 12958, Part 1, §1.3(c).
[120] Executive Order No. 12356, §1,1(c).
[121] Executive Order No. 12065, §1-101.

[122] Executive Order No. 12958, Part 1, §1.4(d).
[123] Executive Order No. 12958, Part 1, §1.7(a).
[124] Executive Order No. 12958, Part 1, §1.7(a)(5).
[125] Executive Order No. 12958, Part 1, §1.7(a)(2).
[126] Executive Order No. 12958, Part 1, §1.7(g).
[127] *Report of the Commission on Protecting and Reducing Government Secrecy*, S. Doc. 105-2, Daniel Patrick Moynihan, Chairman; Larry Combest, Vice Chairman, Commission on Protecting and Reducing Government Secrecy, U.S. Government Printing Office, Washington, D.C., 1997.
[128] Executive Order No. 12356, §1.3(c).
[129] Executive Order No. 12958, Part 1, §1.6(a).
[130] Executive Order No. 12958, Part 1, §1.6(b).
[131] Executive Order No. 12958, Part 1, §1.6(d).
[132] Executive Order No. 12958, Part 1, §1.7(a)(4).
[133] Executive Order No. 12958, Part 1, §1.7(c).
[134] Executive Order No. 12958, Part 1, §1.8(c).
[135] Executive Order No. 12958, Part 1, §1.9.
[136] Executive Order No. 12958, Part 2, §2(c).
[137] Executive Order No. 12958, Part 3, §3.2(b).
[138] Executive Order No. 12958, Part 3, §3.2(c).
[139] Executive Order No. 13142, *Fed. Reg.* **64**, 63169 (Nov. 23, 1999).
[140] Executive Order No. 12958, Part 3, §3.5(a).
[141] Executive Order No. 12958, Part 4, §3.8(a).
[142] Executive Order No. 12958, Part 4, §3.8(c).
[143] Executive Order No. 12958, Part 5, §5.2.
[144] Executive Order No. 13142, §3 and §4.
[145] *Federal Panel Declassified Selected Historically Valuable Document Accomplishments Acknowledged by President Clinton in Oval Office Ceremony*, National Archives and Records Administration News Release, Oct. 11, 2000.
[146] *Memorandum for Steven Garfinkel, Director, Information Security Oversight Office*, from Randolph D. Moss, U.S. Department of Justice, Oct. 5, 1999.
[147] Steven Aftergood, *Secrecy News*, Federation of American Scientists, Washington, D.C., Jan. 23, 2001.
[148] Executive Order No. 12958, Part 5, §5.5(a).
[149] Executive Order No. 12958, Part 5, §5.5(b).
[150] Executive Order No. 12958, Part 5, §5.7(b).
[151] Executive Order No. 12958, Part 5, §5.7(b)(4).
[152] Executive Order No. 12958, Part 5, §5.7(d).
[153] Executive Order No. 12958, Part 5, §6.1(a).
[154] *1999 Report to the President*, Information Security Oversight Office, National Archives and Records Administration, Wash., D.C., Aug. 15, 2000.
[155] ISOO Directive No. 1, *Fed. Reg.* **60**, 53491 (October 13, 1995).