Classified Information Policy and Executive Order 13526

Kevin R. Kosar
Analyst in American National Government

December 10, 2010

Congressional Research Service
7-5700
www.crs.gov
R41528

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Recently, there have been multiple high-profile incidents involving the release of classified government information. Perhaps most prominent was *Wikileaks.org*'s unauthorized publication of more than 600,000 classified Department of Defense documents. Such incidents have further heightened congressional, media, and public interest in classified information policy.

President Barack H. Obama issued Executive Order 13526 on "Classified National Security Information" on December 29, 2009, and Congress enacted P.L. 111-258, the Reducing Over-Classification Act, which President Obama signed into law on October 9, 2010.

This report provides information on classified information policy, which also is called security classification policy and national security classification information policy. It discusses the history, costs, and agencies assigned roles in classified information policy. The report focuses on Executive Order 13526, which establishes much of the current policy, and the report identifies possible oversight issues for Congress.

In broad terms, classified information policy aims to decrease the probability of persons or foreign nations accessing government-held information without authorization and using it to harm the national security of the United States. To this end, many authorities and policies limit access to information held by the federal government. Federal law defines "classified information" as "information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security (50 U.S.C. 426(1))." According to the Information Security Oversight Office, government security classification costs were $8.8 billion in FY2009, although this figure excludes intelligence agencies' expenditures.

Congress has enacted statutes to set aspects of classified information policy. More regularly, Presidents have issued executive orders to establish classified information policies and procedures. Typically, these directives have defined (1) who in the federal government may classify information; (2) what levels of classification and classification markings (e.g., "top secret") may be used; (3) who may access classified information; and (4) how and when classified information is to be declassified.

E.O. 13526 revised the previous policies on these matters and established a National Declassification Center. This center, located at the National Archives and Records Administration, is tasked with eliminating a more than 400 million-page backlog of classified records that are 25 years old and older.

Congress may opt to examine the implementation of E.O. 13526, including issues such as its mandate for agencies to review their security classification guides for fealty to current policy. Additionally, the practice of permitting the executive branch to set much of classified information policy may be subject to examination. Similarly, the enactment of the Reducing Over-Classification Act came less than a year after the issuance of E.O. 13526. Congress may choose to examine to what degree classifying agencies have implemented the new law and the executive order consonantly.

Contents

Figures

Tables

Contacts

Recent Heightened Interest

President Barack H. Obama issued Executive Order 13526 on "Classified National Security Information" on December 29, 2009.[1]

In the months succeeding the issuance of E.O. 13526, multiple incidents have further heightened congressional, media, and public interest in the issue of classified information policy:

1. Shamai Leibowitz, a former Federal Bureau of Investigation contractor, was sentenced to prison for divulging classified materials to a blogger.[2]
2. *Wikileaks.org*, an organization that describes itself as a "public service designed to protect whistleblowers, journalists and activists who have sensitive materials to communicate to the public," published online more than 600,000 classified diplomatic cables and government documents produced during the wars in Afghanistan and Iraq.[3] These disclosures have been condemned by the Obama Administration and other officials.[4]
3. An August 6, 2010, memorandum indicates that the Department of Defense (DOD) is purchasing and destroying the entire first edition of a book by a former employee. The agency believes the book reveals classified information regarding military and intelligence operations in Afghanistan.[5]
4. Jack Goldsmith, a former U.S. assistant attorney general, has alleged that "senior government officials" have leaked classified information to journalist Bob Woodward.[6]

These incidents occurred in the wake of other information releases in the past few years.[7]

---

[1] President Barack H. Obama, "Executive Order 13526, Classified National Security Information," December 29, 2009, 75 *Federal Register* 707, January 5, 2010.

[2] Maria Gold, "Former FBI Employee Sentenced for Leaking Classified Papers," May 25, 2010, at http://www.washingtonpost.com/wp-dyn/content/article/2010/05/24/AR2010052403795.html.

[3] Glenn Kessler, "WikiLeaks's Unveiling of Secret State Department Cables Exposes U.S. Diplomacy," Washington Post, November 29, 2010, at http://www.washingtonpost.com/wp-dyn/content/article/2010/11/28/AR2010112802395.html; Mark Mazzetti et al., "Pakistan Aids Insurgency in Afghanistan, Reports Assert," *New York Times*, July 25, 2010, at http://www.nytimes.com/2010/07/26/world/asia/26isi.html; and Editors, "The Iraq Archive: The Strands of a War," *New York Times*, October 23, 2010, at http://www.nytimes.com/2010/10/23/world/middleeast/23intro.html.

[4] White House Office of the Press Secretary, "Statement by the Press Secretary," November 28, 2010, at http://www.whitehouse.gov/the-press-office/2010/11/28/statement-press-secretary; and White House Office of the Press Secretary, "Statement of National Security Advisor General James Jones on Wikileaks," July 25, 2010, at http://www.whitehouse.gov/the-press-office/statement-national-security-advisor-general-james-jones-wikileaks.

[5] Scott Shane, "Secrets in Plain Sight in Censored Book's Reprint," *New York Times*, September 17, 2010, at http://www.nytimes.com/2010/09/18/us/18book.html; and Ronald L. Burgess, Lieutenant General, Defense Intelligence Agency, "Harm to National Security from Unauthorized Disclosure of Classified Information by U.S. Army Reserve Lieutenant Colonel (LTC) Anthony Shaffer in His Book 'Operation Dark Heart,'" memorandum, August 6, 2010, at http://www.fas.org/sgp/news/2010/09/dia080610.html. See also Steven Aftergood, "Pentagon Delays Publication of New Book," *SecrecyNews.org*, September 15, 2010, at http://www.fas.org/blog/secrecy/2010/09/dark_heart.html.

[6] Jack Goldsmith, "Our Nation's Secrets, Stuck in a Broken System," *Washington Post*, October 22, 2010, at http://www.washingtonpost.com/wp-dyn/content/article/2010/10/21/AR2010102104848.html.

[7] Shane Harris, "Plugging the Leaks," *Washingtonian*, July 2010, at http://www.washingtonian.com/print/articles/6/0/ (continued...)

This report addresses classified information policy, including its history, costs, and the agencies assigned a role in it. The report focuses on Executive Order 13526, which establishes the current policy, and identifies possible classified information policy oversight issues for Congress.

Overview: Classified Information Policy

Definition

Many authorities and policies limit access to information held by the federal government. Three examples include

- Article I, Section 5, of the U.S. Constitution specifies that each house of Congress "shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy;"
- Federal law keeps personal income tax records confidential (26 U.S.C. 6103); and
- Federal agencies have devised policies to restrict access to information. Agencies have, for example, marked documents as "For Official Use Only," which proscribes their public release.[8]

This report focuses on one of these policies—classified information policy, which also is called *security classification policy* and *classified national security information policy*.

Federal law has defined *classified information* as

> information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security (50 U.S.C. 426(1)).[9]

Broadly speaking, classified information policy refers to a range of federal governmental practices that aim to restrict access to information or documents on the grounds of national security. The purpose in limiting access to this information is to prevent it from being used by persons, organizations, or nations to inflict harm upon the United States.

(...continued)

16336.html.

[8] CRS Report RL33494, *Security Classified and Controlled Information: History, Status, and Emerging Management Issues*, by Kevin R. Kosar, pp. 10-23. On November 4, 2010, President Obama issued an executive order that aims to reduce the diversity of agency-created control markings. Barack H. Obama, "Executive Order 13556, Controlled Unclassified Information," 75 *Federal Register* 68675, November 9, 2010, at http://www.archives.gov/cui/documents/2010-EO-13556-cui.pdf.

[9] This definition only applies to the Intelligence Identities Protection Act (50 U.S.C. 421-426). Similar definitions also may be found at 18 U.S.C. 798(b) and 50 U.S.C. 438(2).

As the two following sections describe, Congress has enacted classified information policy statutes. However, classified information policy largely has been established through executive orders.[10]

Executive Orders

Since 1940, Presidents regularly have issued executive orders to set classified information policies (**Table 1**). As this report later details, President Obama has revised classified information policy through the issuance of E.O. 13526 on December 29, 2009.

Table 1. Executive Orders on Classified Information, 1940-2010

Date Signed	President	Order	Citation
March 22, 1940	Franklin D. Roosevelt	E.O. 8381	4 F.R. 1147 (March 26, 1940)
February 1, 1950	Harry S Truman	E.O. 10104	15 F.R. 597 (February 3, 1950)
September 24, 1951	Harry S Truman	E.O. 10290	16 F.R. 9795 (September 27, 1951)
November 5, 1953	Dwight D. Eisenhower	E.O. 10501	18 F.R. 7049 (November 10, 1953)
May 7, 1959	Dwight D. Eisenhower	E.O. 10816	24 F.R. 3777 (May 12, 1959)
January 9, 1961	Dwight D. Eisenhower	E.O. 10901	26 F.R. 217 (January 12, 1961)
September 20, 1961	John F. Kennedy	E.O. 10964	26 F.R. 8932 (September 22, 1961)
January 12, 1962	John F. Kennedy	E.O. 10985	27 F.R. 439 (January 16, 1962)
February 28, 1963	John F. Kennedy	E.O. 11097	28 F.R. 2021 (March 7, 1963)
March 8, 1972	Richard M. Nixon	E.O. 11652	37 F.R. 5290 (March 10, 1972)
April 24, 1973	Richard M. Nixon	E.O. 11714	38 F.R. 10245 (April 26, 1973)
June 11, 1975	Gerald R. Ford	E.O. 11862	40 F.R. 25197 (June 13, 1975)
June 28, 1978	James E. Carter	E.O. 12065	43 F.R. 28949 (July 3, 1978)
April 2, 1982	Ronald W. Reagan	E.O. 12356	14 F.R. 14874 (April 6, 1982)
November 10, 1994	William J. Clinton	E.O. 12937	59 F.R. 59097 (November 15, 1994)
April 17, 1995	William J. Clinton	E.O. 12958	60 F.R. 19825 (April 20, 1995)
August 2, 1995	William J. Clinton	E.O. 12968	60 F.R. 40245 (August 7, 1995)
November 19, 1999	William J. Clinton	E.O. 13142	64 F.R. 66089 (November 23, 1999)
March 28, 2003	George W. Bush	E.O. 13292	68 F.R. 15315 (March 28, 2003)
December 29, 2009	Barack H. Obama	E.O. 13526	75 F.R. 707 (January 5, 2010)

Source: Compiled by the author from http://www.archives.gov/federal-register/codification/numeric-executive-orders.html and the *Federal Register*.

[10] "While the Supreme Court has stated that the President has inherent constitutional authority to control access to sensitive information relating to the national defense or to foreign affairs, no court has found that Congress is without authority to legislate in this area." CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*, by Jennifer K. Elsea, summary page.

Typically, these directives have defined

- who in the federal government may classify information,
- what levels of classification and classification markings (e.g., "top secret") may be used,
- who may access classified information, and
- how and when classified information is to be declassified.

These executive orders also have limited the use of classification. For example, executive orders have forbidden the use of classification "to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security" (e.g., E.O. 12356, Section 1.6).

In some instances, executive orders have mandated the declassification of documents (E.O. 12937), or established new agencies to implement aspects of classified information policy (E.O. 12065).[11]

Frequently, a new executive order repeals the classified information policies of previous executive orders. One exception to this generalization is E.O. 10104 (1950). This order limits the dissemination of information regarding "certain vital military and naval installations or equipment" and has not been repealed explicitly.[12] President Truman issued this executive order subsequent to the enactment of statutes that remain law (18 U.S.C. 795 and 797).

Statutes

As described above, classified information policy largely has been established through executive orders. However, periodically Congress has enacted classified information statutes, including those that

- forbid individuals from gathering, receiving, and transmitting information related to national defense and intelligence activities, and authorize sanctions, including the death penalty in certain instances (62 Stat. 736-738; 18 U.S.C. 793-797);[13]
- forbid the disclosure of classified information regarding intelligence codes, systems, or cryptography (65 Stat. 719; 18 U.S.C. 798);
- protect the identities of covert intelligence agents and criminalize their disclosure (P.L. 97-200, Sec. 2(a); 96 Stat. 122; 50 U.S.C. 421);

[11] This report addresses the agencies involved in classified information policy on pp. 7-9.

[12] President Harry S Truman, "Executive Order 10104—Defining Certain Vital Military and Naval Installations and Equipment as Requiring Protection Against the General Dissemination of Information Relative Thereto," February 1, 1950, 15 *Federal Register* 597, February 3, 1950.

[13] CRS Report RL33502, *Protection of National Security Information*, by Jennifer K. Elsea. Agencies that produce and utilize classified information regularly, such as the DOD, also have devised policies for handling unauthorized disclosures of classified information. For example, see Department of Defense, "Unauthorized Disclosure of Classified Information to the Public," Directive 5210.50, July 22, 2005, at http://www.fas.org/irp/doddir/dod/d5210_50.pdf.

- established the Public Interest Declassification Board (PIDB) and charged it with advising the President and other public officials on information declassification policy (P.L. 106-567, Title VII; 114 Stat. 2856; 50 U.S.C. 435, Amendments);[14] and
- required the establishment of procedures for the protection against unauthorized disclosure of any classified information in the custody of federal courts, including the Supreme Court (P.L. 96-456; 94 Stat. 2025; 18 U.S.C. Appendix).

Congress enacted a particularly significant classified information policy in the FY1995 intelligence authorization act (P.L. 103-359, Sec. 802; 108 Stat. 3435; 50 U.S.C. 435). It assigned to the President the responsibility to establish procedures governing access to classified information. This made into law what had hitherto been a practice—allowing the President to have a lead role in devising classified information policy.

Most recently, Congress enacted P.L. 111-258, the Reducing Over-Classification Act, which President Obama signed into law on October 9, 2010. According to the Senate report accompanying the legislation, this statute aims to

> prevent federal departments and agencies from unnecessarily classifying information or classifying information at a higher and more restricted level than is warranted, and by doing so to promote information sharing across departments and agencies and with State, local, tribal and private sector counterparts, as appropriate.[15]

To these ends, the statute advances multiple measures, including requiring executive branch agencies' inspectors general to assess whether their agencies are following current classified information policies (P.L. 111-258, Section 6(b)).

Estimated Annual Federal Expenditures

The federal government's total annual expenditures for classifying and declassifying information are not publicly available.

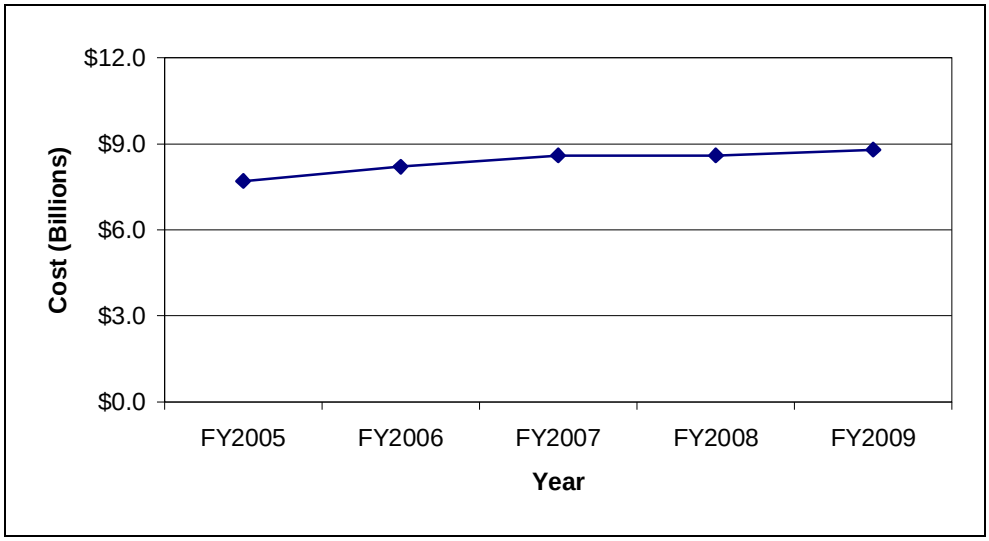
The Information Security Oversight Office (ISOO), an agency within the National Archives and Records Administration (NARA), annually releases a report on agencies' estimated classified information policy costs. However, these estimates are drawn from the agencies' own estimates, which are not audited by ISOO or any other agency. Additionally, the ISOO report figures do not include the costs of the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), Office of the Director of National Intelligence (ODNI), the National Geospatial-Intelligence Agency (NGIA), the National Reconnaissance Office (NRO), and the National Security Agency (NSA). The classified information policy cost estimates for these latter agencies are provided to the President in a classified addendum to the report.

[14] The PIDB's statute was amended by P.L. 108-458, Sec. 1102 (118 Stat. 3699) , and P.L. 110-53, Sec. 602 (121 Stat. 335).

[15] Senate Committee on Homeland Security and Governmental Affairs, *Reducing Overclassification Act, Report of the Committee on Homeland Security and Governmental Affairs, U.S. Senate, to Accompany H.R. 553*, S.Rept. 111-200, 111th Cong. 2nd sess., May 27, 2010, p. 1.

The ISOO reports that total government classified information policy costs were $8.8 billion in FY2009. This amount is slightly higher than the estimated costs in each of the four previous years (**Figure 1**).

Figure 1. Estimated Federal Government Classified Information Policy Costs, FY2005-FY2010



Source: Information Security Oversight Office, 2009 Cost Report.

Notes: Estimated costs do not include the classified information policy costs of CIA, DIA, ODNI, NGIA, NRO, and the NSA.

Nearly 55% ($4.8 billion) of the FY2009 estimated costs are attributed by agencies to "information security," an administrative category that includes the information systems (e.g., computer hardware and software) used to collect, store, and utilize classified information, and administrative expenses related to information security classification activities.[16]

Approximately 15% ($1.3 billion) of classified information policy costs are attributed to "security management, oversight, and planning." The remaining 30% ($2.7 billion) of costs goes toward the costs of personnel security (e.g., background checks on persons with access to classified information), the training of personnel in the proper handling of classified information, and the physical security of facilities holding classified information.

In FY2009, the federal government is estimated to have spent $44.7 million to declassify information. This amounts to 0.5% of the FY2009 total classified information policy costs ($8.8 billion).

Classified Information Policy: Who Does What?

Generally speaking, authorized executive branch agencies are to classify information in accordance with standing classified information policy. Agencies also are obliged to secure this

[16] Information Security Oversight Office, *2009 Cost Report* (NARA/ISOO: June 25, 2010), pp. 1-4, at http://www.archives.gov/isoo/reports/2009-cost-report.pdf.

information and to train their personnel in its proper handling. Executive branch inspectors general, as noted previously, must assess their agencies' compliance with classified information policy.

However, four entities have been established and assigned classified information policy responsibilities: (1) the Information Security Oversight Office (ISOO), (2) the Public Interest Declassification Board (PIDB), (3) the Interagency Security Classification Appeals Panel (ISCAP), and (4) the National Declassification Center (NDC). The authorizations that established these entities and their responsibilities are described below.

Information Security Oversight Office

President James E. Carter established the Information Security Oversight Office via E.O. 12065, which he issued on June 28, 1978.[17] The ISOO is located within the NARA.[18]

Under E.O 13526, Part 5, the ISOO is responsible for issuing the directives necessary to implement the executive order, and for reviewing agencies' compliance therewith.[19] More specifically, the ISOO establishes the standards for

1. classification, declassification, and classification marking principles;
2. safeguarding classified information;[20]
3. agencies' security education and training programs;
4. agencies' self-inspection programs; and
5. agencies' classification and declassification guides.

The ISOO also is authorized to conduct on-site evaluations of agencies' compliance with E.O. 13526 and to act upon complaints regarding agencies' implementation of the executive order. Annually, the ISOO produces a report on the implementation of classified information policy and another on the federal government's information classification and declassification costs.[21]

Interagency Security Classification Appeals Panel

President Clinton established the Interagency Security Classification Appeals Panel via E.O. 12958, which he issued on April 20, 1995.[22] While President Obama's E.O. 13526 made modest

[17] E.O. 12065, Section 5-2, 43 *Federal Register* 28949, July 3, 1978.

[18] At the time ISOO was established, the NARA was the National Archives Record Service (NARS) and was located with the General Services Administration. The 1984 National Archives and Records Administration Act (P.L. 98-497; 98 Stat. 2292; 44 U.S.C. 2102) established the NARA and transferred the NARS to it.

[19] The ISOO's directives are binding upon agencies, although the Office of the Director of National Intelligence (ODNI) retains some authority on these matters. The ODNI may, in consultation with the ISOO, issue its own directives to protect intelligence sources, methods, and activities.

[20] E.O. 13526, Section 4 provides basic guidance to agencies regarding the safeguarding and dissemination of classified information to authorized holders.

[21] See "ISOO Reports," at http://www.archives.gov/isoo/reports/.

[22] President William J. Clinton, "Executive Order 12958, Classified National Security Information," April 17, 1995, 60 *Federal* Register 19825, April 20, 1995,

augmentations to the ISCAP's role, its membership and duties remain largely as they were upon establishment.[23]

The ISCAP's members include the director of the ISOO, who serves as its executive secretary, and senior-level representatives from the Departments of State, Defense, and Justice, and the National Archives, the Office of the Director of National Intelligence, and the National Security Advisor. (The President designates the ISCAP chair from among the aforementioned persons.) The CIA may appoint a temporary member in instances where information classified by the CIA is under consideration. The ISOO provides administrative support to the ISCAP.

The ISCAP was designed to serve as a forum for resolving declassification disputes. The ISCAP decides in instances involving (1) disputes over or challenges of the proper classification level of information; (2) agencies wishing to exempt information from automatic declassification; and (3) persons or entities (private or governmental) appealing an agency's decision to keep information classified after said person or entity has requested its declassification.

Public Interest Declassification Board

Congress established the Public Interest Declassification Board on December 27, 2000 (P.L. 106-567, Sec. 703; 114 Stat. 2856; 50 U.S.C. 435 Amendments). This independent executive branch agency has nine members, five of whom are appointed by the President, and four of whom are appointed by Congress. The Director of the ISOO serves as the PIDB's executive secretary.

The law requires the PIDB to

1. advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and such other executive branch officials as the Board considers appropriate on the systematic, thorough, coordinated, and comprehensive identification, collection, review for declassification, and release to Congress, interested agencies, and the public of declassified records and materials (including donated historical materials) that are of archival value, including records and materials of extraordinary public interest.
2. promote the fullest possible public access to a thorough, accurate, and reliable documentary record of significant United States national security decisions and significant United States national security activities in order to (A) support the oversight and legislative functions of Congress; (B) support the policymaking role of the executive branch; (C) respond to the interest of the public in national security matters; and (D) promote reliable historical analysis and new avenues of historical study in national security matters.
3. provide recommendations to the President for the identification, collection, and review for declassification of information of extraordinary public interest that does not undermine the national security of the United States, to be undertaken in accordance with a declassification program that has been established or may be established by the President by executive order.

[23] E.O. 13526, Sec. 5.3, 75 *Federal Register* 707, January 5, 2010.

4. advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and such other executive branch officials as the Board considers appropriate on policies deriving from the issuance by the President of executive orders regarding the classification and declassification of national security information (50 U.S.C. 435 Amendments).

In December 2007, the PIDB published a report, *Improving Declassification*, and participated in the process that led to the issuance of E.O. 13526.[24] The PIDB also has held public meetings to discuss declassification issues.[25]

National Declassification Center

President Obama established the National Declassification Center via E.O. 13526. The NDC, which is described below, is responsible for expediting the declassification of information deaccessioned (or released) to the NARA.

The Obama Administration's Review of Classified Information Policy

When President Obama took office in January 2009, classified information policy was established by E.O. 12958 as amended by E.O 13292. President William J. Clinton issued E.O. 12958 on April 17, 1995, and his successor President George W. Bush amended it via E.O. 13292 on March 28, 2003.[26]

President Obama ordered a review of classified information policy on May 27, 2009.[27] The President wrote,

> [M]y Administration is committed to operating with an unprecedented level of openness. While the Government must be able to prevent the public disclosure of information where such disclosure would compromise the privacy of American citizens, national security, or other legitimate interests, a democratic government accountable to the people must be as transparent as possible and must not withhold information for self-serving reasons or simply to avoid embarrassment.[28]

[24] Public Interest Declassification Board, *Improving Declassification: A Report to the President from the Public Interest Declassification Board* (PIDB/ISOO, December 2007), at http://www.archives.gov/pidb/improving-declassification.pdf.

[25] Public Interest Declassification Board, "Meetings," at http://www.archives.gov/pidb/meetings/.

[26] President Bush's executive order enacted a number of policies that increased and lengthened the classification of government information. For example, E.O. 12958 required documents to be declassified 10 years after their issuance. E.O. 13292 abolished the former policy and changed the latter from 10 to 25 years. CRS Report 97-771, *Security Classification Policy and Procedure: E.O. 12958, as Amended*, by Kevin R. Kosar, p. 10.

[27] President Barack H. Obama, "Memorandum of May 27, 2009—Classified Information and Controlled Unclassified Information," 74 *Federal Register* 26277, June 1, 2009.

[28] Ibid.

To achieve these goals, the Assistant to the President for National Security Affairs (commonly known as the National Security Advisor) was to submit to the President "recommendations and proposed revisions" to the current policy (E.O. 12958) regarding[29]

> (i) Establishment of a National Declassification Center to bring appropriate agency officials together to perform collaborative declassification review under the administration of the Archivist of the United States;
>
> (ii) Effective measures to address the problem of over classification, including the possible restoration of the presumption against classification, which would preclude classification of information where there is significant doubt about the need for such classification, and the implementation of increased accountability for classification decisions;
>
> (iii) Changes needed to facilitate greater sharing of classified information among appropriate parties;
>
> (iv) Appropriate prohibition of reclassification of material that has been declassified and released to the public under proper authority;
>
> (v) Appropriate classification, safeguarding, accessibility, and declassification of information in the electronic environment, as recommended by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction and others; and
>
> (vi) Any other measures appropriate to provide for greater openness and transparency in the Government's security classification and declassification program while also affording necessary protection to the Government's legitimate interests.[30]

The National Security Advisor's response was due in 90 days.

At the request of the National Security Advisor, the Public Interest Declassification Board established a website to solicit public input on improving classified information policy.[31] The PIDB asked the public to limit their comments to (1) declassification policy, (2) a national declassification center, (3) classification policy, and (4) technology issues and challenges.[32] Approximately 150 comments were submitted to the PIDB during the two weeks of the submission period (June 29, 2009 to July 10, 2009). The PIDB also held a public meeting in Washington, DC, on July 8, and then transmitted the comments it received to the National Security Advisor.[33]

---

[29] The memorandum also ordered a review of the government's policy for controlled unclassified information (CUI), a topic this report does not address. For an introduction to CUI, see the National Archives, "What is Controlled Unclassified Information?" at http://www.archives.gov/cui/.

[30] President Barack H. Obama, "Memorandum of May 27, 2009—Classified Information and Controlled Unclassified Information," p. 26277.

[31] James L. Jones, National Security Adviser, letter to Martin Faga, Chairman of the Public Interest Declassification Board, June 2, 2009, pp.1-2, at http://www.archives.gov/pidb/letter06-02-09.pdf.

[32] Martin Faga, Chairman, Public Interest Declassification Board, "Declassification Policy Forum—Introduction," June 29, 2009, at http://www.whitehouse.gov/blog/Declassification-Policy-Forum-Introduction/.

[33] National Archives and Record Administration, "Public Interest Declassification Board (PIIDB); Meeting," 74 *Federal Register* 29729, June 23, 2009; and Public Interest Declassification Board, "Recommendations and Reports" web page, at http://www.archives.gov/pidb/recommendations/.

After an interagency review process, the Obama Administration issued its revisions to classified information policy in Executive Order 13526 on December 29, 2009, along with an accompanying memorandum and order.[34]

Current Classified Information Policy: E.O. 13526

E.O 13526 revoked E.O. 12958 as amended by E.O. 13526 and "prescribe[d] a uniform system for classifying, safeguarding, and declassifying national security information."[35] The major components of this new policy are enumerated below.[36]

Classification Levels

E.O. 13526 maintains the three long-standing classification levels, or classification markings, of top secret, secret, and confidential.

> (1) "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;
>
> (2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe; [and]
>
> (3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe (Section 1.2(a)).

The term *original classification authority* refers to the person or agency who initially classified a piece of information.

To improve the accuracy of classification activities, E.O. 13526, Section 1.9 requires agencies to complete a "comprehensive review" of their internal classification guidance within two years. Previously, there has been evidence to indicate that many agencies use classification guides that are out of date and not fully in alignment with current classification policy.[37]

[34] President Barack H. Obama, "Executive Order 13526, Classified National Security Information," December 29, 2009, 75 *Federal Register* 707, January 5, 2010; President Barack H. Obama, "Implementation of the Executive Order, 'Classified National Security Information,'" December 29, 2009, 75 *Federal Register* 733, January 5, 2010; and President Barack H. Obama, "Original Classification Authority," December 29, 2009, 75 *Federal Register* 735, January 5, 2010.

[35] President Barack H. Obama, "Executive Order 13526, Classified National Security Information," p. 1.

[36] More specific guidance to E.O. 13526 may be found in the regulations "Classified National Security Information; Final Rule" at 32 C.F.R. 2001, 75 *Federal Register* 37254, June 28, 2010.

[37] Information Security Oversight Office, *Report to the President 2009* (Washington, DC: NARA/ISOO, March 31, 2010), p. 19, at http://www.archives.gov/isoo/reports/2009-annual-report.pdf.

The Types of Information That May Be Classified

In keeping with previous executive orders, E.O. 13526 limits classification to information that pertains to

> (a) military plans, weapons systems, or operations;
>
> (b) foreign government information;
>
> (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;
>
> (d) foreign relations or foreign activities of the United States, including confidential sources;
>
> (e) scientific, technological, or economic matters relating to the national security;
>
> (f) United States Government programs for safeguarding nuclear materials or facilities;
>
> (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
>
> (h) the development, production, or use of weapons of mass destruction (Section 1.4).

Additionally, E.O. 13526 continues the prohibition on the use of classification to

> (1) conceal violations of law, inefficiency, or administrative error;
>
> (2) prevent embarrassment to a person, organization, or agency;
>
> (3) restrain competition; or
>
> (4) prevent or delay the release of information that does not require protection in the interest of the national security (Section 1.7).

Section 1.7 of the order also forbids the classification of "[b]asic scientific research information not clearly related to the national security."

Challenges to Classification and Classification Levels

Persons who are authorized by E.O. 13526 or statute to hold classified information may challenge the classification of a piece of information (Section 1.8).[38] They also may challenge its level of classification. Thus, for example, if two agencies classified the same piece of information at different levels (e.g., top secret and secret), each agency may contest the other's classification marking. Such disputes are resolved by the ISCAP.

[38] These persons do not include only the original classification authority; rather, they include any person who has been approved to have access to a piece of classified information. So, for example, the Secretary of Defense may originally classify a piece of information, but a Department of Defense analyst who has been authorized to access the information may challenge its classification level.

Persons Authorized to Classify Information and Derivative Classification

Original classification refers to an instance when a government official classifies a piece of information that hitherto had not been classified. *Derivative classification* refers to an instance when originally classified information is reproduced or used in the course of producing other classified information. Original classifiers and their delegates may produce derivatively classified information, but most derivatively classified material likely is produced by other persons whose positions require them to work with classified information (e.g., intelligence analysts).[39] E.O. 13526 sets forth policies for both original and derivative classification.

E.O. 13526 empowers the President, Vice President, and "agency heads and officials" with original classification authority (Section 1.3). An individual with original classification authority may delegate his or her power to other U.S. government officials, though any such delegations must be made known to the Director of the ISOO. The guidance that accompanied E.O. 13526 enumerates the more than two dozen "agency heads and officials" who possess original classification authority.[40] It also clarifies which officials may classify information at the three classification levels. Thus, for example, the Director of National Drug Control Policy is authorized to classify information at the top secret level (or any lower level), but the Secretary of Commerce may not classify above the secret level.[41]

Both original and derivative classifiers must mark information that they classify with a classification marking, their name, their official position and agency, the date of classification, and the duration of classification (Section 1.6). Additionally, all persons with classification authority must be trained in classification and declassification policy. Persons so trained must study both executive-branch-wide policies (such as E.O. 13526) and their individual agency's classification guide (which holds agency-specific policies). Original classifiers must receive this training annually, and derivative classifiers must receive it every two years.

Duration of Classification

Section 1.5 of E.O. 13526 requires a public release date to be set when information is classified. Specifically, a classifier must designate a "specific date or event for declassification based upon the duration of the national security sensitivity of the information."

Under the previous executive order (E.O. 13142), classified information was to remain classified for not less than 25 years, absent agency action to declassify it.[42] E.O. 13526 caps the duration for classification at 10 years, except in the instance of information that can "clearly or demonstrably

[39] The policies for approving persons to access to classified information were set via executive order. See President William J. Clinton, "Executive Order 12968, Access to Classified Information," 60 *Federal Register* 40245, July 28, 1995.

[40] President Barack H. Obama, "Original Classification Authority," p. 735.

[41] A previous executive order, E.O. 13958, did not list the agency heads and officials with classification authority. Rather, the order provided the President and Vice President with original classification authority, and authorized the President to designate persons with original classification authority. E.O. 13958 did not delineate the levels at which designees could classify information, and the President could empower an agency head or other designee with "top secret" original classification authority. 68 *Federal Register* 15316, March 28, 2003.

[42] E.O 13142, 64 *Federal Register* 66089, November 23, 1999.

be expected to reveal the identity of a confidential human source or key design concepts of weapons of mass destruction." Such information is to be classified for 25 years, and in accordance with policies set forth in Section 3.3, may remain classified for up to an additional 50 years.

Declassification

Declassification refers to the process by which classified information becomes unclassified. Usually, the onus of declassification falls upon the agency or persons who originally classified a piece of information. Said agency or person (or a delegate thereof) reviews the information to see whether it should be (1) declassified, (2) exempted from declassification by an exception within current classified information policy, or (3) referred to another agency that may seek to keep the information classified. In the end, the information might be wholly declassified, partially declassified (e.g., redacted), or remain wholly classified.

E.O. 13526 provides five means through which national security information may be declassified.[43] First, whoever has classified a piece of information may declassify it when the reason(s) for its classification no longer hold. Second, declassification also may occur when an agency challenges the propriety of another agency's classification of information. (As mentioned previously, these "classification challenges" are resolved by the ISCAP.)

Part 3 of E.O. 13526 sets forth three additional means: automatic declassification, systematic declassification review, and mandatory declassification review.

Automatic declassification: Under automatic declassification, information 25 years or older moves to declassified status.[44] This, however, does not mean that the records become immediately available to the public. The NDC must review the agency's declassification activities to see that they are in accordance with current policy. Additionally, other agencies' declassifiers may need to review the records for information that their agency believes should be kept classified. Finally, E.O. 13526, Section 3.3(b) provides nine such instances under which an original classifying authority may request that a piece of automatically declassified information remain classified.[45]

---

[43] There are at least two other means for declassifying information. Congress may enact a statute requiring particular information to be declassified; and Freedom of Information Act (5 U.S.C. 552) requests may result in the declassification of information.

[44] E.O. 12958, issued by President William J. Clinton in 1994, mandated automatic declassification. It required most forms of classified information to be declassified 10 years after their initial classification date.

[45] The exemptions cover instances when declassification would

> (1) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development; (2) reveal information that would assist in the development, production, or use of weapons of mass destruction; (3) reveal information that would impair U.S. cryptologic systems or activities; (4) reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system; (5) reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans; (6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States; (7) reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of

(continued...)

Systematic declassification: According to E.O. 13526, Section 3.3 (h) and (j), an agency seeking to exempt information from automatic declassification must submit a detailed request to ISOO's director, and the ISCAP will adjudicate the request. If the ISCAP approves the request, the information in question is subject to systematic declassification review. Under this process, the information remains classified for up to an additional 50 years, after which it will be automatically declassified unless the classifying agency seeks another exemption.

Mandatory declassification review: Finally, E.O 13526, Section 3.5 sets the rules for mandatory declassification review, a process that is instigated in response to a request for declassification. As with Freedom of Information Act (5 U.S.C. 522) requests, a mandatory declassification review request may be sought by a member of the public. The process requires the original classifier to assess whether the classified information still meets the standards for continued classification enumerated in Section 1.2(a) of E.O. 13526.[46] Certain types of information are exempt from mandatory declassification requests, such as information exempted from disclosure under the Freedom of Information Act (5 U.S.C. 552), information originated by the President or Vice President and some of the individuals who work with them, and documents required to be submitted for prepublication review (e.g., memoirs by intelligence agents).

A New Entity: National Declassification Center

E.O. 13526, Section 3.7 established the National Declassification Center (NDC) at the National Archives in College Park, MD. The NDC is headed by a director, who is appointed by the Archivist in consultation with the secretaries of the agencies that classify significant quantities of information (i.e., the Departments of State, Defense, Energy, Homeland Security) and the Attorney General and Director of National Intelligence. Currently the NDC has 75 employees, and it is charged with expediting both automatic and systematic declassification.[47]

Although a new entity, the NDC has been in development since 2006.[48] It was devised as a means for reducing the significant backlog of classified government records that have been released by agencies to the National Archives but not yet declassified. The NDC recently estimated this backlog to be 418 million pages, and the memorandum to agency heads that accompanied E.O. 13526 requires the NDC to eliminate the backlog by December 31, 2013.[49]

(...continued)

> the national security, are authorized; (8) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or (9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

[46] Section 1.2(a) establishes the three levels of classification—confidential, secret, and top secret—based upon the severity of damage to the United States' national security that might be expected to result. See pages 11-12 of this report.

[47] Sheryl J. Shenberger, Director, National Declassification Center, "The National Declassification Center," briefing materials, October 29, 2010, p. 11.

[48] Allan Weinstein, Archivist, "National Declassification Initiative," *Organization of American Historians Newsletter*, August 2007, at http://www.oah.org/pubs/nl/2007aug/weinstein.html; and National Archives, *2009 Performance Budget*, pp. II-23-II-27, at http://www.archives.gov/about/plans-reports/performance-budget/2009/2009-performance-budget.pdf.

[49] Sheryl J. Shenberger, Director, National Declassification Center, "The National Declassification Center," p. 12; and President Barack H. Obama, "Implementation of the Executive Order, 'Classified National Security Information,'" (continued...)

One of the causes for delay in declassification is what is often called "multiple agency equity" in classified information. Put simply, when an agency moves to declassify a document, it may contain information that other agencies may wish to keep classified. Thus, for example, a document that describes a foreign nation's clandestine efforts to acquire nuclear materials may be of interest to the Central Intelligence Agency, and the Departments of Energy and State. In these instances, the declassifying agency is obliged to refer the information to these other agencies and wait for their review of it and agreement to declassify it.

The NDC aims to speed up this process through multiple means, such as allowing declassifiers from multiple agencies to work more closely to review these multiple-agency-equity materials, and by implementing processes to reduce unnecessary referrals.

Safeguarding Classified Information

Generally speaking, agencies that produce and utilize classified information are obliged to safeguard it.[50] E.O. 13526, Part 4 sets the basic standards for access to classified information by government employees and other persons:

> (a) A person may have access to classified information provided that:
>
> (1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;
>
> (2) the person has signed an approved nondisclosure agreement; and
>
> (3) the person has a need-to-know.

This part of the executive order also requires regular training and retraining in the handling and safekeeping of classified information. E.O. 13526 also sets the conditions for the distribution of classified information outside of the original classifying agency, and Part 5 of the order empowers the ISOO to issue binding regulations that prescribe the standards for safeguarding, storing, distributing, transmitting, destroying, and accounting for classified information. The ISOO also must prescribe the standards for agencies' programs for training employees in classified information security and for carrying out self-inspection programs.

Possible Issues for Congress

E.O. 13526 and its accompanying memorandum and order were issued less than a year ago, so it may be premature to attempt an assessment of its success as a policy. However, several aspects of its implementation may be worthy of congressional attention.

1. E.O. 13526 continues the tradition of congressional deference to the executive branch in setting classified information policy. Since 1995, three Presidents (Clinton, Bush, Obama) have issued

(...continued)

memorandum, December 29, 2009, 75 *Federal Register* 733, January 5, 2010.

[50] As noted in the "Statutes" section of this report (pp. 4-5), both federal laws and agencies have set policies for the safeguarding of classified information and the prosecution of individuals who violate these policies.

three executive orders (E.O. 12958, E.O. 13292, and E.O. 13526) requiring agencies to make significant revisions to their security classification policies and practices. Congress may opt to reevaluate the benefits and costs of the decision to permit significant changes in classified information policy via executive order.

2. As with previous executive orders, E.O. 13526 bases the classification levels on the criterion of damage. The differing levels of classification markings represent varying levels of possible "damage to national security." Thus, the classification marking of "'Confidential' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe." Meanwhile, a document may be given the highest security protection if its release "could reasonably be expected to cause exceptionally grave damage." No other values or criterion are to be taken into account.

The terms *damage* and *national security* are inherently broad concepts. Neither damage nor the state of relations among nations are easily quantified or determinable with precision. E.O. 13526 carries these two terms under a unified definition that defines *national security* to include the United States' international relations.

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

Congress might examine the utility of the continued use of the singular criterion of harm and the concept of *damage to national security*.[51] It also could assess the utility of the parameters of the term *damage to the national security* to determine whether they are overly or insufficiently broad.

3. As described above, E.O. 13526 assigns significant classified information policy responsibilities to the ISOO, NDC, and NARA. An executive order cannot be used to appropriate funds from the U.S. Treasury;[52] hence, Congress may assess whether these agencies have sufficient resources to carry out their work.

4. E.O. 13526, Section 1.9 requires classifying agencies to review their classification guides to ensure they comport with current classified information policy. This must be done within two years. One objective of this practice is to reduce the incidences of information being classified needlessly. Over-classification, or the act of classifying material that need not be classified, not only is a violation of government policy, it also creates unnecessary costs related to safe-keeping, handling, and declassification. Congress may ask agencies to report on their progress toward completing this task.

5. In the memorandum accompanying E.O. 15326, the President ordered the National Declassification Center to clear the more than 400 million pages of classified records more than

[51] For a recent example of the elasticity of security classification, see Steven Aftergood, "Behind the Censorship of Operation Dark Heart," *SecrecyNews.org*, September 29, 2010, at http://www.fas.org/blog/secrecy/2010/09/behind_the_censor.html.

[52] Article I, Section 9 of the U.S. Constitution states, "No Money shall be drawn from the Treasury, but in Consequence of Appropriations made by Law."

25 years old by December 31, 2013.[53] The NDC's role is to facilitate agencies' review of these documents and their determinations to release records (in whole or in part), or to keep them classified.

To date, agencies' declassification of information has lagged behind their production of it. According to an NDC estimate, each year 15 million new pages of classified material are accessioned to the NARA, and only 11 million pages complete the declassification process and are made available to the public.[54] The President's memorandum would require more than 400 million pages of information to move through this process in four years, a rate of approximately 100 million pages per year.

Congress may choose to monitor the NDC's progress toward achieving the reduction of the backlog.

6. Congress enacted the Reducing Over-Classification Act in October 2010, four months after the ISOO released its regulations (32 C.F.R. 2001) for implementing E.O. 13526. The Senate Committee on Homeland Security and Governmental Affairs wrote:

> The Committee wishes to emphasize that none of the provisions in this Act is intended to supplant the Executive Branch's longstanding authority to determine what information should be appropriately classified within the framework established in Executive Order 13526 and its predecessors. Indeed, the Committee believes that the provisions of the Act complement and do not conflict with Executive Order 13526, and that both the Order and the Act will promote the goals of increased transparency, information sharing, and security.[55]

Section 4 of this new statute requires the Secretary of DHS to appoint a classified information advisory officer, who has the authority to "develop and disseminate educational materials and to develop and administer training programs" to assist sub-federal actors (i.e., state, local, and tribal governments and private-sector firms) that utilize classified information. It is unclear whether this new official must have these materials and programs approved by the ISOO, which is authorized to set the standards for agencies' security education and training programs (E.O. 13526, Part 5). Congress may consider examining whether agencies have faced any challenges in implementing the new law and the executive order consonantly.

7. The Reducing Over-Classification Act aims to increase information-sharing among agencies. The illicit release of over 250,000 State Department cables, possibly by a Department of Defense employee, may indicate the inherent difficulty of balancing information sharing and information protection. Already, some agencies have announced new security controls.[56] Furthermore, the Office of Management and Budget has ordered agencies that handle classified information to "establish a security assessment team consisting of counterintelligence, security, and information assurance experts to review the agency's implementation of procedures for safeguarding

[53] President Barack H. Obama, "Implementation of the Executive Order, 'Classified National Security Information,'" 75 *Federal Register* 733.

[54] Sheryl J. Shenberger, Director, National Declassification Center, "The National Declassification Center," p. 12.

[55] Senate Committee on Homeland Security and Governmental Affairs, *Reducing Overclassification Act*, S.Rept. 111-200, p. 4.

[56] White House Office of the Press Secretary, "Fact Sheet: U.S. Government Mitigation Efforts in Light of the Recent Unlawful Disclosure of Classified Information," December 1, 2010, at http://www.whitehouse.gov/the-press-office/2010/12/01/fact-sheet-us-government-mitigation-efforts-light-recent-unlawful-disclo.

classified information against improper disclosures."[57] Congress may move to hold a hearing where it can aggregate agency reports on their improvements to classified information safeguarding.

8. The incidents of unauthorized leaks cited at the beginning of this report appear to share a common feature—they involve persons authorized to have access to classified information. Congress may wish to survey these and other cases to determine whether there were further commonalities in these instances. Were, for example, the individuals' motivations similar? Were these individuals little supervised in their handling of classified information? Would increasing the negative consequences for the unauthorized release of classified information be likely to discourage further incidents? Was most of the information in electronic format?

Author Contact Information

Kevin R. Kosar
Analyst in American National Government
kkosar@crs.loc.gov, 7-3968

[57] Jacob J. Lew, Director, Office of Management and Budget, "WikiLeaks—Mishandling of Classified Information," memorandum, November 28, 2010, at http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/wikileaks.pdf.