Order Code RL33494

CRS Report for Congress

Security Classified and Controlled Information: History, Status, and Emerging Management Issues

Updated February 11, 2008

Harold C. Relyea
Specialist in American National Government
Government and Finance Division

Prepared for Members and Committees of Congress

Security Classified and Controlled Information: History, Status, and Emerging Management Issues

Summary

The security classification regime in use within the federal executive branch traces its origins to armed forces information protection practices of the World War I era. The classification system — designating information, according to prescribed criteria and procedures, protected in accordance with one of three levels of sensitivity, based on the amount of harm to the national security that would result from its disclosure — attained a presidential character in 1940 when President Franklin D. Roosevelt issued the initial executive order prescribing these information security arrangements. Refinements in the creation, management, and declassification of national security information followed over the succeeding decades, and continue today. In many regards, these developments represent attempts to narrow the bases and discretion for assigning official secrecy to executive branch documents and materials. Limiting the quantity of security classified information has been thought to be desirable for a variety of important reasons: (1) promoting an informed citizenry, (2) effectuating accountability for government policies and practices, (3) realizing oversight of government operations, and (4) achieving efficiency and economy in government management.

Because security classification, however, was not possible for some kinds of information deemed in some quarters to be "sensitive," other kinds of designations or markings came to be applied to alert federal employees regarding its privileged or potentially harmful character. Sometimes these markings derived from statutory provisions requiring the protection of a type of information; others were administratively authorized with little detail about their use.

In the current environment, still affected by the long shadow of the terrorist attacks of September 11, 2001, several issues have arisen regarding security classified and controlled information. Volume is a concern: 8 million new classification actions in 2001 jumped to 14 million new actions in 2005, while the quantity of declassified pages dropped from 100 million in 2001 to 29 million in 2005. Expense is vexing: $4.5 billion spent on classification in 2001 increased to $7.1 billion in 2004, while declassification costs fell from $232 million in 2001 to $48.3 million in 2004, according to annual reports by the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA). Some agencies were recently discovered to be withdrawing archived records from public access and reclassifying them. Critically evaluating this activity, ISOO has indicated that the federal government needs to apply a more integrated approach among the classifying agencies. The force of, and authority for, information control markings, other than security classification labels, have come under congressional scrutiny, prompting concerns about their number, variety, lack of underlying managerial regimes, and effects. Among those effects, contend the Government Accountability Office and the manager of the Information Sharing Environment for the intelligence community, is the obstruction of information sharing across the federal government and with state and local governments. These and related matters, including remedial legislation (H.R. 984, H.R. 4806), are examined in this report, which will be updated as events warrant.

Contents

Classification Background 2

Control Markings Discovered 5

Control Markings Today 10

Comparison of Sensitive Security Information (SSI) Policies 12
- USDA Marking 12
- USDA Management 14
- TSA/DOT Marking 16
- TSA/DOT Management 16
- Management Regime Comparison 24

Implications for Information Sharing 26

Improving Classified Information Life Cycle Management 27

Remedial Legislation 31

Related Literature 32

List of Tables

Table 1. Management of Security Classified Information and SSI Compared . . 24
Table 2. Information Moving In and Out of Classified Status 28
Table 3. ISCAP Decisions 29

Security Classified and Controlled Information: History, Status, and Emerging Management Issues

Prescribed in various ways, federal policies may require the protection of, or provide a privileged status for, certain kinds of information. For the legislative branch, for example, the Constitution, in Article I, Section 5, 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." In the next section of the article, a privileged status for certain remarks of Members is established when the Constitution indicates that "for any Speech or Debate in either House, they shall not be questioned in any other Place."

Within the executive branch, it seems likely that one of the earliest-felt needs for secrecy concerned preparations and plans for the defense of the country. Following long-standing military practice, General George Washington and other officers in the Continental Army, seeking to ensure the protection of information, had written "Secret" or "Confidential" on strategic communiques to each other in the field and to headquarters. There was no immediate formalization of this practice by the new federal government, but it was from these roots that security classification would emerge. That history is briefly reviewed in the next section of this report.

The application of security classification subsequently came to be regulated through a narrowing of the bases and discretion for assigning official secrecy to executive branch materials. Due to that and other information management developments, new kinds of designations or markings came to be used to alert federal employees about the privileged status or sensitive content of a record or document. Sometimes these markings derived from statutory provisions requiring the protection of a type of information; many others were administratively created, but lacked detailed management regimes. Early congressional experience with these other markings is examined, providing a background for considering some of the current issues they raise.

Finally, the report considers some long-standing difficulties attending the management of security classified information — controlling the volume of such material and attendant costs. It looks, as well, at recent efforts by some agencies to withdraw archived records from public access and reclassify them, activity which the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA) critically evaluated and, as a reform for the underlying problem, suggested a more integrated approach among the classifying agencies.

Classification Background

Current security classification arrangements, prescribed by an executive order of the President, trace their origins to a March 1940 directive issued by President Franklin D. Roosevelt as E.O. 8381.[1] This development was probably prompted somewhat by desires to clarify the authority of civilian personnel in the national defense community to classify information, to establish a broader basis for protecting military information in view of growing global hostilities, and to manage better a discretionary power seemingly of increasing importance to the entire executive branch. Prior to this 1940 order, information had been designated officially secret by armed forces personnel pursuant to Army and Navy general orders and regulations. The first systematic procedures for the protection of national defense information, devoid of special markings, were established by War Department General Orders No. 3 of February 1912. Records determined to be "confidential" were to be kept under lock, "accessible only to the officer to whom intrusted." Serial numbers were issued for all such "confidential" materials, with the numbers marked on the documents, and lists of same kept at the offices from which they emanated. With the enlargement of the armed forces after the entry of the United States into World War I, the registry system was abandoned, and a tripartite system of classification markings was inaugurated in November 1917 with General Orders No. 64 of the General Headquarters of the American Expeditionary Force.

During World War II, in addition to the President's order and prevailing armed forces directives on marking and handling classified information, the Office of War Information, in September 1942, issued a government-wide regulation on creating and managing classified materials. Among other ad hoc arrangements of the era, personnel cleared to work on the Manhattan Project for the production of the atomic bomb, in committing themselves not to disclose protected information improperly, were "required to read and sign either the Espionage Act or a special secrecy agreement," establishing their awareness of their secrecy obligations and a fiduciary trust which, if breached, constituted a basis for their dismissal.[2]

A few years after the conclusion of World War II, President Harry S. Truman, in February 1950, issued E.O. 10104, which, while superseding E.O. 8381, basically reiterated its text, but added to *Restricted*, *Confidential*, and *Secret* a fourth *Top Secret* classification designation, making American information security categories consistent with those of our allies.[3] At the time of the promulgation of this order, however, plans were underway for a complete overhaul of the classification program, which would result in a dramatic change in policy.

---

[1] 3 C.F.R., 1938-1943 Comp., pp. 634-635.

[2] Anthony Cave Brown and Charles B. MacDonald, eds., *The Secret History of the Atomic Bomb* (New York: Dial Press/James Wade, 1977), p. 201.

[3] 3 C.F.R., 1949-1953 Comp., pp. 298-299.

E.O. 10290, issued in September 1951, introduced three sweeping innovations in security classification policy.[4] First, the order indicated the Chief Executive was relying upon "the authority vested in me by the Constitution and statutes, and as President of the United States" in issuing the directive. This formula appeared to strengthen the President's discretion to make official secrecy policy: it intertwined his responsibility as Commander in Chief with the constitutional obligation to "take care that the laws be faithfully executed."[5] Second, information was now classified in the interest of "national security," a somewhat new, but nebulous, concept, which, in the view of some, conveyed more latitude for the creation of official secrets. It replaced the heretofore relied upon "national defense" standard for classification. Third, the order extended classification authority to nonmilitary entities throughtout the executive branch, to be exercised by, presumably but not explicitly limited to, those having some role in "national security" policy.

The broad discretion to create official secrets granted by E.O. 10290 engendered widespread criticism from the public and the press. In response, President Dwight D. Eisenhower, shortly after his election to office, instructed Attorney General Herbert Brownell to review the order with a view to revising or rescinding it. The subsequent recommendation was for a new directive, which was issued in November 1953 as E.O. 10501.[6] It withdrew classification authority from 28 entities; limited this discretion in 17 other units to the agency head; returned to the "national defense" standard for applying secrecy; eliminated the "Restricted" category, which was the lowest level of protection; and explicitly defined the remaining three classification areas to prevent their indiscriminate use.[7]

Thereafter, E.O. 10501, with slight amendment, prescribed operative security classification policy and procedure for the next two decades. Successor orders built on this reform. These included E.O. 11652, issued by President Richard M. Nixon in March 1972,[8] followed by E.O. 12065, promulgated by President Jimmy Carter in June 1978.[9] For 30 years, these classification directives narrowed the bases and discretion for assigning official secrecy to executive branch documents and materials. Then, in April 1982, this trend was reversed with E.O. 12356, issued by President

---

[4] Ibid., pp. 789-797.

[5] In *Environmental Protection Agency* v. *Mink*, Supreme Court Associate Justice Byron White, delivering the majority opinion, proffered that "Congress could certainly have provided that the Executive Branch adopt new procedures" for the security classification of information, "or it could have established its own procedures — subject only to whatever limitations the Executive [or constitutional separation of powers] privilege may be held to impose upon such congressional ordering." 410 U.S. 73, 83 (1973).

[6] 3 C.F.R., 1949-1953 Comp., pp. 979-986.

[7] U.S. Commission on Government Security, *Report of the Commission on Government Security* (Washington: June 1957), pp. 155-156.

[8] 3 C.F.R., 1971-1975 Comp., pp. 678-690.

[9] 3 C.F.R., 1978 Comp., pp. 190-205.

Ronald Reagan.[10] This order expanded the categories of classifiable information, mandated that information falling within these categories be classified, authorized the reclassification of previously declassified documents, admonished classifiers to err on the side of classification, and eliminated automatic declassification arrangements.[11]

President William Clinton returned security classification policy and procedure to the reform trend of the Eisenhower, Nixon, and Carter Administrations with E.O. 12958 in April 1995.[12] Adding impetus to the development and issuance of the new order were changing world conditions: the democratization of many eastern European countries, the demise of the Soviet Union, and the end of the Cold War. Accountability and cost considerations were also significant influences. In 1985, the temporary Department of Defense (DOD) Security Review Commission, chaired by retired General Richard G. Stilwell, declared that there were "no verifiable figures as to the amount of classified material produced in DOD and in defense industry each year." Nonetheless, it concluded that "too much information appears to be classified and much at higher levels than is warranted."[13] In October 1993, the cost of the security classification program became clearer when the General Accounting Office (GAO) reported that it was "able to identify government-wide costs directly applicable to national security information totaling over $350 million for 1992." After breaking this figure down — it included only $6 million for declassification work — the report added that "the U.S. government also spends additional billions of dollars annually to safeguard information, personnel, and property."[14] E.O. 12958 set limits for the duration of classification, prohibited the reclassification of properly declassified records, authorized government employees to challenge the classification status of records, reestablished the balancing test of E.O. 12065 (weighing the need to protect information vis-a-vis the public interest in its disclosure), and created two review panels — one on classification and declassification actions and one to advise on policy and procedure.

Most recently, in March 2003, President George W. Bush issued E.O. 13292 amending E.O. 12958.[15] Among the changes made by this directive were adding infrastructure vulnerabilities or capabilities, protection services relating to national security, and weapons of mass destruction to the categories of classifiable information; easing the reclassification of declassified records; postponing the automatic declassification of protected records 25 or more years old, beginning in

---

[10] 3 C.F.R., 1982 Comp., pp. 166-178.

[11] See Richard C. Ehlke and Harold C. Relyea, "The Reagan Administration Order on Security Classification: A Critical Assessment," *Federal Bar News & Journal*, vol. 30, Feb. 1983, pp. 91-97.

[12] 3 C.F.R., 1995 Comp., pp. 333-356.

[13] U.S. Department of Defense, Department of Defense Security Review Commission, *Keeping the Nation's Secrets* (Washington: GPO, 1985), pp. 48-49.

[14] U.S. General Accounting Office, *Classified Information: Costs of Protection Are Integrated with Other Security Costs*, GAO Report GAO/NSIAD-94-55 (Washington: Oct. 1993), p. 1.

[15] 3 C.F.R., 2003 Comp., pp. 196-218.

mid-April 2003 to the end of December 2006; eliminating the requirement that agencies prepare plans for declassifying records; and permitting the Director of Central Intelligence to block declassification actions of the Interagency Security Classification Appeals Panel, unless overruled by the President.

The security classification program has evolved over 66 years. One may not agree with all of its rules and requirements, but attention to detail in its policy and procedure result in a significant management regime. The operative presidential directive, as amended, defines its principal terms. Those who are authorized to exercise original classification authority are identified. Exclusive categories of classifiable information are specified, as are the terms of the duration of classification, as well as classification prohibitions and limitations. Classified information is required to be marked appropriately along with the identity of the original classifier, the agency or office of origin, and a date or event for declassification. Authorized holders of classified information who believe that its protected status is improper are "encouraged and expected" to challenge that status through prescribed arrangements. Mandatory declassification reviews are also authorized to determine if protected records merit continued classification at their present level, a lower level, or at all. Unsuccessful classification challenges and mandatory declassification reviews are subject to review by the Interagency Security Classification Appeals Panel. General restrictions on access to classified information are prescribed, as are distribution controls for classified information. The ISOO, within NARA, is mandated to provide central management and oversight of the security classification program. If the director of this entity finds that a violation of the order or its implementing directives has occurred, it must be reported to the head of the agency or to the appropriate senior agency official so that corrective steps, if appropriate, may be taken. In general, very little of this management structure attends information control markings other than *Confidential*, *Secret*, and *Top Secret*.

Control Markings Discovered

In March 1972, a subcommittee of the House Committee on Government Operations — now the House Committee on Government Reform — launched the first oversight hearings on the administration and operation of the Freedom of Information Act (FOIA). Enacted in 1966, the FOI Act had become operative in July 1967. In the early months of 1972, the Nixon Administration was developing new security classification policy and procedure, which would be prescribed in E.O. 11652, issued in early March. The subcommittee's strong interest in this directive was reflected in its unsuccessful attempt to receive testimony from one of the directive's principal architects, David Young, Special Assistant to the National Security Council. The subcommittee sought his testimony as it examined the way in which the new order "will affect the economic and efficient operation of our security classification system, the rationale behind its various provisions, and alternatives to the present approach."[16] Although Young, through White House

[16] Letter to David Young, Apr. 24, 1972, appearing in U.S. Congress, House Committee on Government Operations, *U.S. Government Information Policies and Practices — Security* (continued...)

Counsel John Dean III, declined the invitation to testify, the subcommittee was more successful in obtaining department and agency responses to its August 1971 questionnaire, which, among other questions, asked, "What legend is used by your agency to identify records which are *not* classifiable under Executive Order 10501 [the operative order at the time] but which are not to be made available outside the government?"[17] Of 58 information control markings identified in response to this question, the most common were *For Official Use Only* (11 agencies); *Limited Official Use* (nine agencies); *Official Use Only* (eight agencies); *Restricted Data* (five agencies); *Administratively Restricted* (four agencies); *Formerly Restricted Data* (four agencies); and *Nodis*, or no dissemination (four agencies). Seven other markings were used by two agencies in each case.[18] A CRS review of the agency responses to the control markings question prompted the following observation:

> Often no authority is cited for the establishment or origin of these labels; even when some reference is provided it is a handbook, manual, administrative order, or a circular but not statutory authority. Exceptions to this are the Atomic Energy Commission, the Defense Department and the Arms Control and Disarmament Agency. These agencies cite the Atomic Energy Act, N.A.T.O. related laws, and international agreements as a basis for certain additional labels. The Arms Control and Disarmament Agency acknowledged it honored and adopted State and Defense Department labels.[19]

At a May 1, 1972, hearing on the relationship of the FOI Act to the security classification system, Chairman William S. Moorhead of the Foreign Operations and Government Information Subcommittee (Committee on Government Operations) wondered aloud how the act's nine exemptions to the rule of disclosure could be expanded to the multiple information control markings which the departments and agencies had indicated they were using.[20] The following day, when the hearing continued, William D. Blair, Jr., Deputy Assistant Secretary for Public Affairs at the Department of State, explained that some information control markings were used to route otherwise classified information to a limited group of recipients, "those people who have responsibility for the subject matter concerned." He then addressed the relationship question raised by Chairman Moorhead, saying:

> But if a question came in under the Freedom of Information Act or from the Congress or other representative of the public for that given document, the fact that it is marked, let's say, NODIS, is not relevant. What is relevant to the making available of that document to the public is whether or not it was properly

---

[16] (...continued)
Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7), hearings, 92nd Cong., 2nd sess. (Washington: GPO, 1972), pp. 2452-2453.

[17] U.S. Congress, House Committee on Government Operations, *U.S. Government Information Policies and Practices — Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7)*, hearings, 92nd Cong., 2nd sess. (Washington: GPO, 1972), p. 2930 (emphasis in original).

[18] See ibid., pp. 2933-2934.

[19] Ibid., p. 2932.

[20] Ibid., p. 2284.

> classified under the Executive order and whether or not the Freedom of Information Act, for example, once we have reviewed the document, still pertains, whether we feel that the need for the classification still pertains and whether, in fact, we are authorized under the act to withhold it.[21]

A moment thereafter, he explained another marking, which was not applied to route classified information, but apparently had the same effect as a security classification protective marking:

> "Limited official use" is not a fixed distribution channel, such as some of these other terms you have mentioned. It simply is an administrative red flag put on that document which means that the document should be given the same degree of protection, physical protection as a classified document even though it is not, under the Executive order, classifiable.[22]

However, when asked if, in applying this particular marking, "you mean to exclude all individuals outside the Department, subject to the Freedom of Information Act, where they can go to court to obtain it," Blair's response indicated that the use of the marking was somewhat more complicated than functioning as a parallel security label, when he said:

> Not necessarily sir. That may be the case. For instance, one set of files on which we use "Limited official use" quite commonly is personnel files. Well, we would be very likely to deny those personnel files if they were requested by a member of the public, on quite different grounds from classification — on grounds of invasion of privacy. But on the other hand we may use a term like "Limited official use" on an internal advisory document which we may be authorized under the Freedom of Information Act to withhold if it were requested; but we might decide not to claim that authority.[23]

Although an attempt was made to obtain further explanation of how information control markings were used, the questioner, a subcommittee staff member, concluded "that all you have convinced me of is to reinforce my belief that a distribution marking is merely a more restrictive or stricter type of classification marking."[24]

Later in the hearing, in an exchange with the subcommittee's staff director, DOD General Counsel J. Fred Buzhardt made another attempt to clarify the use of control markings:

> In the first place, you have a determination as to whether the material is to be classified. Once the decision is made that the information should be classified, then the limitation of access has to do with the protection of that which is classified. We also have the responsibility to control the dissemination. That is what these access limitations are for, to control dissemination, to confine access

---

[21] Ibid., pp. 2477-2478.

[22] Ibid., p. 2478.

[23] Ibid.

[24] Ibid., p. 2479.

> to the people who have a need to know to work with the information. It is a protection device. We must use protective devices of some sort.[25]

Asked if the control markings, such as *eyes only*, were applied to material that was not classified, Buzhardt said:

> I presume you wouldn't find "eyes only" in an authorized way upon any document that was not classified by one of the classifiers. Once it is classified you can use limitations on distribution to protect it. That is a protective device.[26]

To this response, Blair added:

> The purpose of classification is to determine what information is or is not available to the public outside of the government. These labels that you are referring to have nothing to do with that. They have absolutely no value for determining what information or what document may be given to a member of the public. They are simply a mailing device, if you like, a means by which a superior determines which of his subordinates he wishes to deal with this particular matter and be aware of this particular information.[27]

These explanations of information control markings being used as devices to limit the distribution of classified information within DOD and the State Department, however, did not appear to extend to all such markings. Blair, for instance, had testified that the *Limited official use* marking was applied, in his words, "quite commonly" to personnel files, which, for the most part, were not security classifiable materials at that time. Several entities indicating they used information control markings had no original classification authority. These included, among others, the American Revolution Bicentennial Commission (ARBC), the Department of Housing and Urban Development, and the Federal Trade Commission (FTC).[28] Does this situation mean that the control markings of these entities were applied only to limit the distribution of classified information received from other agencies? That is possible, but seems unlikely. The ARBC control marking, *Administratively confidential*, appears to have been designed for information of a different character from national security classified materials, while the FTC label, *For staff use only*, does not appear to have provided much limitation on the distribution of classified information.

Before this phase of the oversight hearings on the FOI Act concluded, the subcommittee received testimony from Assistant Attorney General Ralph E. Erickson of the Office of Legal Counsel, Department of Justice, on May 11, 1972. During the course of his appearance before the subcommittee to discuss E.O. 11652, the use of control markings to limit the distribution of classified information was raised with the following question from the subcommittee's staff director:

---

[25] Ibid., p. 2497.

[26] Ibid.

[27] Ibid., pp. 2497-2498.

[28] See ibid., p. 2935.

> Can you assure us today that these kinds of distribution access stamps will not be used on unclassified material in any Executive agency or department? If you can guarantee that, then I will go along and say [Section] 4(a) is a big improvement. But I do not think that is going to be the case from other testimony we have had. I think people are going to substitute LIMDIS, NODIS, and all these other stamps for the stamps authorized under the Executive order and we are going to proliferate more and more and more.[29]

Erickson offered a two part response:

> First, it is our hope within the Department of Justice and I think in other agencies, too, that the use of this sort of a restricted distribution will be severely limited or removed. But, more importantly, it [Section 4(a)] specifically limits the use of such designations to the point where they must conform with the provision of this order and would have no effect in terms of classification. It will not prevent the information from otherwise being made available. It may in part restrict the distribution within the department but certainly if a request were made under the Freedom of Information Act it has no applicability.[30]

He assured his questioner that control markings used to limit the distribution of classified information "will not have any effect on disclosure" under the FOI Act, and would not, in themselves, be a bar to disclosure.

Later, in May 1973, when reviewing this phase of the subcommittee's oversight hearings, a report by the parent Committee on Government Operations commented:

> One of the difficult problems related to the effective operation of the security classification system has been the widespread use of dozens of special access, distribution, or control labels, stamps, or markings on both classified and unclassified documents. Such control markings were not specifically authorized in Executive Order 10501, but have been utilized for many years by many executive agencies having classification authority and dozens of other agencies who do not possess such authority. The use of such stamps has, in effect, been legitimized in section 9 of the new Executive Order 11652.[31]

On this matter, the report concluded that, "while there is a clear rationale for the use of such access or control markings, the basic problem is the effect of the proliferation of their use on the effective operation of the classification system. This problem," it continued, "fully explored with executive branch witnesses during the hearings, is one that this committee believes should be carefully monitored by the [newly created] Interagency Classification Review Committee and by department

---

[29] Ibid., pp. 2705-2706.

[30] Ibid., p. 2706.

[31] U.S. Congress, House 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),* H.Rept. 93-221, 93rd Cong., 2nd sess. (Washington: GPO, 1973), p. 75.

heads to assure that it does not interfere with the overall effectiveness and integrity of the classification system."[32]

Control Markings Today

That such interference with the security classification program by these types of information control markings — in terms of both their confusion and presumed coequal authority with classification markings — has occurred in the post-9/11 environment may be discerned in a press account. In late January 2005, *GCN Update*, the online, electronic news service of *Government Computer News*, reported that "dozens of classified Homeland Security Department documents" had been accidently made available on a public Internet site for several days due to an apparent security glitch at the Department of Energy. Describing the contents of the compromised materials and reactions to the breach, the account stated the "documents were marked 'for official use only,' the lowest secret-level classification." The documents, of course, were not security classified, because the marking cited is not authorized by E.O. 12958. Interestingly, however, in view of the fact that this misinterpretation appeared in a story to which three reporters contributed, perhaps it reflects, to some extent, the current state of confusion about the origin and status of various new information control markings which have appeared of late.[33] In some instances, the phraseology of the markings is new, and, in at least one case, the asserted authority for the label is, unlike most of those of the past, statutory. Among the problems they generate, however, the one identified over three decades ago by the House Committee on Government Operations endures.

Broadly considering the contemporary situation regarding information control markings, a recent information security report by the JASON Program Office of the MITRE Corporation proffered the following assessment:

> The status of sensitive information outside of the present classification system is murkier than ever.... "Sensitive but unclassified" data is increasingly defined by the eye of the beholder. Lacking in definition, it is correspondingly lacking in policies and procedures for protecting (or not protecting) it, and regarding how and by whom it is generated and used.[34]

A contemporaneous Heritage Foundation report appeared to agree with this appraisal, saying:

> The process for classifying secret information in the federal government is disciplined and explicit. The same cannot be said for unclassified but security-related information for which there is no usable definition, no common

---

[32] Ibid., p. 78.

[33] Patience Wait, "DHS Classified Briefings Leaked Through Energy System," *GCN Update*, Jan. 27, 2005, available at [http://www.gcn.com/online/vol1_no1/34907-1.html]; credited as contributing to this story were GCN staff writers Susan M. Menke and Mary Mosquera.

[34] MITRE Corporation, JASON Program Office, *Horizontal Integration: Broader Access Models for Realizing Information Dominance* (McLean, VA: Dec. 2004), p. 5.

> understanding about how to control it, no agreement on what significance it has for U.S. national security, and no means for adjudicating concerns regarding appropriate levels of protection.[35]

Concerning the current *Sensitive But Unclassified* (SBU) marking, a 2004 report by the Federal Research Division of the Library of Congress commented that guidelines for its use are needed, and noted that "a uniform legal definition or set of procedures applicable to all Federal government agencies does not now exist." Indeed, the report indicates that SBU has been utilized in different contexts with little precision as to its scope or meaning, and, to add a bit of chaos to an already confusing situation, it is "often referred to as Sensitive Homeland Security Information."[36]

Assessments of the variety, management, and impact of information control markings, other than those prescribed for the classification of national security information, have been conducted by CRS, GAO, and the National Security Archive, a private-sector research and resource center located at The George Washington University. In March 2006, GAO indicated that, in a recent survey, 26 federal agencies reported using 56 different information control markings to protect sensitive information other than classified national security material.[37] That same month, the National Security Archive offered that, of 37 agencies surveyed, 24 used 28 control markings based on internal policies, procedures, or practices, and eight used 10 markings based on statutory authority.[38] These numbers are important in terms of the variety of such markings. GAO explained this dimension of the management problem:

> [T]here are at least 13 agencies that use the designation For Official Use Only [FOUO], but there are at least five different definitions of FOUO. At least seven agencies or agency components use the term Law Enforcement Sensitive (LES), including the U.S. Marshals Service, the Department of Homeland Security (DHS), the Department of Commerce, and the Office of Personnel Management (OPM). These agencies gave differing definitions for the term. While DHS does not formally define the designation, the Department of Commerce defines it to include information pertaining to the protection of senior government officials, and OPM defines it as unclassified information used by law enforcement personnel that requires protection against unauthorized disclosure to protect the

---

[35] James Jay Carafano and David Heyman, "DHS 2.0: Rethinking the Department of Homeland Security," *Heritage Special Report SR-02* (Washington: Dec. 13, 2004), p. 20.

[36] U.S. Library of Congress, Federal Research Division, *Laws and Regulations Governing the Protection of Sensitive but Unclassified Information*, by Alice R. Buchalter, John Gibbs, and Marieke Lewis (Washington: Sept. 2004), p. i.

[37] U.S. Government Accountability Office, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism- Related and Sensitive but Unclassified Information*, GAO Report GAO-06-385 (Washington: Mar. 2006), pp. 5, 25.

[38] National Security Archive, *Pseudo-Secrets: A Freedom of Information Act Audit of the U.S. Government's Policies on Sensitive Unclassified Information* (Washington: Mar. 2006), pp. 9-11.

> sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.[39]

Apart from the numbers, however, is another aspect of the management problem, which GAO described in the following terms:

> There are no governmentwide policies or procedures that describe the basis on which agencies should use most of these sensitive but unclassified designations, explain what the different designations mean across agencies, or ensure that they will be used consistently from one agency to another. In this absence, each agency determines what designations to apply to the sensitive but unclassified information it develops or shares.[40]

Comparison of Sensitive Security Information (SSI) Policies

To identify some of the management problems and concerns attending current information control markings, the following case study comparison is provided. *Sensitive Security Information* (SSI) refers to a specific category of government information that has been deemed to require protection against unauthorized disclosure. It is both a concept and a control marking used by the Department of Agriculture (USDA), on the one hand, and jointly by the Transportation Security Administration (TSA) of the Department of Homeland Security as well as by the Department of Transportation, on the other hand, but with different underlying authorities, conceptualizations, and management regimes for it.

USDA Marking

Sensitive Security Information (SSI) appears to be a relatively new information concept and control marking for USDA. Other similar designations, however, are also in use within the department. An information security program statement indicates that "USDA refers to unclassified sensitive information as 'Sensitive Security Information' (SSI). Basically," it continues, "it's to be treated the same as 'Sensitive But Unclassified Information' or 'For Official Use Only Information.'"[41] As a USDA website page, this document provides links to a USDA SSI cover sheet and the department's SSI management regulation, both of which are printable, and a brief Power Point presentation designed to assist USDA employees in understanding the SSI concept. Another USDA website page provides more details concerning *For Official Use Only* (FOUO) and similar designations. It states at the

---

[39] U.S. Government Accountability Office, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism- Related and Sensitive but Unclassified Information*, p. 24.

[40] Ibid., p. 5.

[41] U.S. Department of Agriculture, Personnel and Document Security Division, Office of Procurement and Property Management, "Information Security Program," undated, available at [http://www.usda.gov/da/infosec/sensitive.htm].

outset that FOUO "is a document designation, not a classification," and explains that this term is used by "a number of other federal agencies to identify information or material which, although unclassified, may not be appropriate for public release." Some of these other agencies are identified, as are some agencies which use different, but comparable, designations, which are provided as well. The discussion of FOUO, which relies upon Department of Defense policy and practice, cautions that information so marked "does not mean it is automatically exempt from public release under" the Freedom of Information Act (FOIA), specifies how unclassified documents and materials containing FOUO shall be marked and safeguarded, and warns that "[a]dministrative penalties may be imposed for misuse of FOUO information," as well as criminal penalties, "depending on the actual content of the information (privacy, export control, etc.)."[42]

Sensitive but Unclassified (SBU) information is discussed in Chapter 10, part 2, of the USDA *Cyber Security Manual, Series 3500*, also known as DM3550-02 of February 17, 2005. SBU information is identified, in part, in terms of examples, which include: "Social Security Numbers, Employee Emergency Data, For Official Use Only Documents, For Limited Official Use Documents, Funding/Budget Documents, Grant/Contract Documents, IT [information technology] Security Plans, Formulas/Trade Secrets, Internet Protocol (IP) Addresses, Network Design Diagrams."[43] Thus, another information control designation, *For Limited Official Use*, is identified, and, furthermore, the chapter states that "SBU information also includes Sensitive Security Information (SSI)," but notes, as the examples reflect, "the SBU category contains information that is not security related but is still sensitive in terms of its risk of exposure."[44] Thereafter, the chapter refers to "SBU/SSI." Various procedures for the processing, handling, and storage of SBU/SSI are specified.[45] Among these is a stipulation that access to SBU/SSI "will be provided to employees with a Need-To-Know," a standard long-governing access to security classified information. Furthermore, "when SBU/SSI data must be shared with contractors and entities outside USDA a *Non-Disclosure Agreement Form* ... must be executed ... to preclude possible organizational or personal conflicts of interest."[46] A copy of this agreement is provided at the end of the chapter. It concludes with a specification of various management responsibilities.

---

[42] U.S. Department of Agriculture, Personnel and Document Security Division, Office of Procurement and Property Management, "For Official Use Only (FOUO) and Similar Designations," undated, available at [http://www.usda.gov/da/ocpm/Security%20Guide/S2unclas/Fouo.htm].

[43] U.S. Department of Agriculture, Office of the Chief Information Officer, *USDA Cyber Security Manual, Series 3500*, Chapter 10, part 2 (DM3550-002), Feb. 17, 2005, p. 8, chapters separately dated and available at [http://www.ocio.usda.gov/directives/index.html].

[44] Ibid., p. 1.

[45] Ibid., pp. 3-4.

[46] Ibid., p. 4 (emphasis in original).

USDA Management

The control and protection of *Sensitive Security Information* (SSI) is discussed in USDA Departmental Regulation 3440-002 of January 30, 2003.[47] The regulation specifies that the "USDA will withhold from release sensitive information that is not appropriate for public disclosure consistent with laws, regulations and court decisions," but also stresses that, "if USDA originates documents that it believes should be classified, Departmental Administration (DA) should be notified as soon as possible." As noted earlier, the Secretary of Agriculture was presidentially authorized to classify information originally as *Secret* (but not *Top Secret*) in September 2002. The regulation also proffers the following proscription: "Information must not be designated as Sensitive Security Information (SSI) to conceal violations of law; inefficiency; administrative error; prevent embarrassment to a person, organization, department or agency; or restrain competition." This ban is similar to one prescribed for security classification.[48]

The regulation provides a lengthy definition of SSI, set out below:

> Sensitive Security Information means unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity; and which describes, discusses, or reflects:
>
> 1. The ability of any element of the critical infrastructure of the United States [also defined in the regulation] to resist intrusion, interference, compromise, theft, or incapacitation by either physical or computer-based attack or other similar conduct that violates Federal, State, or local law; harms interstate, international commerce of the United States; or threatens public health or safety;
> 2. Any current viable assessment, projection, or estimate of the security vulnerability of any element of the critical infrastructure of the United States, specifically including, but not limited to vulnerability assessment, security testing, risk evaluation, risk-management planning, or risk audit; [and]
> 3. Any currently applicable operational problem or solution regarding the security of any element of the critical infrastructure of the United States, specifically including but not limited to the repair, recovery, redesign, reconstruction, relocation, insurance, and continuity of operations of any element.

---

[47] U.S. Department of Agriculture, *Control and Protection of "Sensitive Security Information,"* Departmental Regulation 3440-002, Jan. 30, 2003, available at [http://www.ocio.usda.gov/directives/doc/DR3440-002.htm].

[48] Section 1.7 of E.O. 12958, as amended, states, in part: "(a) In no case shall information be classified in order 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. (b) Basic scientific research information not clearly related to the national security shall not be classified."

As a fourth item in the above quoted definition of SSI, the regulation provides the following categories "for illustration purposes only as examples of the types of information (regardless of format) that may be categorized as SSI."

1. Physical security status of USDA laboratories, research centers, field facilities, etc., which may also contain vulnerabilities;
2. Investigative and analytical materials concerning information about physical security at USDA facilities such as the above-named facilities;
3. Information that could result in physical risk to individuals;
4. Information that could result in serious damage to critical facilities and/or infrastructures; [and]
5. Cyber Security information, which includes, but is not limited to
    a. Network Drawings or Plans
    b. Program and System Security Plans
    c. Mission Critical and Sensitive Information Technology (IT) Systems and Applications
    d. Capital Planning and Investment Control Data (I-TIPS)
    e. IT Configuration Management Data and Libraries
    f. IT Restricted Space (Drawings, Plans and Equipment Specifications as well as actual space)
    g. Incident and Vulnerability Reports
    h. Risk Assessment Reports, Checklists, Trusted Facilities Manual and Security Users Guide [and]
    i. Cyber Security Policy Guidance and Manual Chapters

Specific responsibilities are prescribed for senior USDA officials, heads of department organizations, the Office of the Chief Information Officer, and the Office of the General Counsel. Among the responsibilities specified for USDA agencies and staff offices are the following:

- Ensure that adequate security measures and procedures are implemented to protect SSI.
- Ensure that employees of their organization are aware of their responsibility to protect SSI.
- Determine the potential harm resulting from the loss, misuse, or unauthorized access to or modification of SSI in their custody.
- Ensure that prompt and appropriate disciplinary action is taken against personnel responsible for unauthorized disclosure of SSI.

Regarding FOIA requests for access to SSI, the regulation instructs that these should be processed "in accordance with USDA regulations and the Attorney General's FOIA Memorandum of October 12, 2001," which is appended to the regulation, "with consideration of all applicable FOIA exemptions, including" four identified as "Potentially Applicable to SSI."

The departmental regulation does not cite any statutory authority for its issuance.

TSA/DOT Marking

Originally established within the Department of Transportation (DOT) by the Aviation and Transportation Security Act (ATSA) of 2001,[49] the Transportation Security Administration (TSA) was subsequently transferred to the newly created Department of Homeland Security (DHS) by the Homeland Security Act of 2002.[50] The ATSA was signed into law two months after the September 11 terrorist attacks on the World Trade Center and the Pentagon. Shortly thereafter, in a February 15, 2002, notice, DOT announced that TSA was assuming civil aviation security functions and responsibilities as provided by the ATSA, as well as those being transferred which had previously been performed by the Federal Aviation Administration (FAA), another DOT subunit.[51] A week later, DOT issued in final form, without prior notice or opportunity for public comment, new civil aviation security rules.[52] These rules were prompted by the enactment of the ATSA and the assumption of FAA civil aviation security functions and responsibilities by the TSA. Among them was a new part 1520 of Title 49 of the *Code of Federal Regulations* concerning the protection of "Sensitive Security Information." This new concept, it was explained, "includes information about security programs, vulnerability assessments, technical specifications of certain screening equipment and objects used to test screening equipment, and other information."[53] A little over two years later, however, these rules were superseded.

TSA/DOT Management

On May 18, 2004, DOT and DHS jointly published, as an interim, final rule with request for comments, revised regulations concerning the protection of SSI. In the summary, it was noted that "TSA is revising its regulation governing the protection of sensitive security information (SSI) in order to protect the confidentiality of maritime security measures adopted under the U.S. Coast Guard's regulations, published on October 22, 2003, implementing the Maritime Transportation Security Act (MTSA) and other activities related to port and maritime security." It was further explained that, "with this revision to the regulations, TSA is requiring employees, contractors, grantees, and agents of DHS and DOT to follow the same requirements governing protection of SSI as those in the transportation sector who are subject to the regulation."[54] The interim rule was issued as 49 C.F.R. Part 15 for the Office of the Secretary of Transportation and as 49 C.F.R. Part 1520 for the TSA.

In the review of the statutory and regulatory background to the rule, the observation was proffered that, "situations in which information constitutes both SSI

---

[49] 115 Stat. 597.

[50] 116 Stat. 2135 at 2185.

[51] *Federal Register*, vol. 67, Feb. 20, 2002, pp. 7939-7940.

[52] Ibid., Feb. 22, 2002, pp. 8340-8384.

[53] Ibid., p. 8342.

[54] Ibid., vol. 69, May 18, 2004, p. 28066.

and CII," the latter being another type of data known as critical infrastructure information, "may be limited." Pursuant to the Critical Infrastructure Information (CII) Act, a subtitle of the Homeland Security Act,[55] CII, it was explained, "is voluntarily submitted by the private sector to the Federal Government" and the statute "generally prohibits Federal agencies from disclosing such information, except within the Federal Government and to State and local governments in order to protect critical infrastructure." The following comparison was then offered:

> information constituting SSI generally is not voluntarily submitted to the government, which is required for the CII designation. In addition, SSI relates to both critical and noncritical infrastructure assets. There may be cases, however, where the owner or operator of a critical transportation asset voluntarily submits information, such as a vulnerability assessment, to TSA or the Coast Guard. If that information were to be designated by DHS as CII, it would be governed by the requirements of handling of CII, rather than by the SSI regulation.
>
> Another key difference between SSI and CII is the extent to which a Federal employee may disclose such information. Under the SSI regulation, TSA may disclose SSI to persons with a need to know in order to ensure transportation security. This includes persons both within and outside the Federal Government. The CII Act, however, generally prohibits disclosure of properly designated CII outside the Federal Government. Thus, the interim final rule clarifies that in cases where information is both SSI and CII, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by the CII Act and any implementing regulations, by not the interim final rule.[56]

The interim final rule was composed of 10 subsections. The first of these pertained to the scope of the part, explaining it "does not apply to the maintenance, safeguarding, or disclosure of classified national security information," and the second defined terms used in the part.[57] The third subsection explained what constituted SSI in the following terms:

> (a) *In general....* SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which ... would —
>
> (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);
>
> (2) reveal trade secrets or privileged or confidential information obtained from any person; or
>
> (3) Be detrimental to transportation safety.
>
> (b) *Information constituting SSI.* Except as otherwise provided in writing ... in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:
>
> (1) *Security programs and contingency plans.* Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including —

---

[55] See 116 Stat. 2150.

[56] *Federal Register*, vol. 69, May 18, 2004, p. 28069.

[57] Ibid., pp. 28078, 28082.

(i) Any aircraft operator or airport operator security program or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iv) Any security incident response plan established under 46 U.S.C. 70104.

(2) *Security Directives.* Any Security Directive or order —

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority;

(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.* Related to maritime security; or

(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) *Information Circulars.* Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any —

(i) Information Circular issued by TSA under 49 CFR 1542.303 or 1544.305, or other authority; and

(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) *Performance specifications.* Any performance specification and any description of a test object or test procedure, for —

(i) Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirement of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) *Vulnerability assessments.* Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) *Security inspection or investigative information.* (i) Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(7) *Threat information.* Information held by the Federal government concerning threats against transportation or transportation systems and sources

and methods used to gather or develop threat information, including threats against cyber infrastructure.

(8) *Security measures.* Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including —

(i) Security measures or protocols recommended by the Federal government;

(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and

(iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and number of Federal Flight Deck Officers aggregated by aircraft operator.

(9) Security screening information. The following information concerning security screening under aviation or maritime transportation security requirements of Federal law:

(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.

(ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system.

(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI.

(iv) Any security screener test and scores of such tests.

(v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(10) *Security training materials.* Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by DHS or DOT.

(11) *Identifying information of certain transportation security personnel.*

(i) Lists of the names of or other identifying information that identify persons as —

(A) Having unescorted access to a secure area of an airport or a secure or restricted area of a maritime facility, port area, or vessel; or

(B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport;

(C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(D) Holding a position as a Federal Air Marshal; or

(ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

(12) *Critical aviation or maritime infrastructure asset information.* Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is —

(i) Prepared by DHS or DOT; or

(ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.

(13) *Systems security information.* Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) *Confidential business information.* (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

(15) *Research and development.* Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.

(16) *Other information.* Any information not otherwise described in this section that TSA determines is SS under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the Secretary of DOT may designate as SSI information not otherwise described in this section.[58]

The fourth subsection generically identified persons subject to the requirements of the part, and restrictions on the disclosure of SSI by these "covered persons" were prescribed in the fifth subsection. These included taking "reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure," and, when not in physical possession of SSI, storing it in "a secure container, such as a locked desk or file cabinet, or in a locked room." Unless otherwise authorized in writing, SSI could be disclosed "only to covered persons who have a need to know," who were described in the sixth subsection. "If a covered person receives a record containing SSI that is not marked," he or she must so mark the material and inform the sender of the need to so identify SSI. Furthermore, when a covered person "becomes aware that SSI has been released to unauthorized persons," he or she "must promptly inform TSA or the applicable DOT or DHS component or agency."[59]

The seventh subsection pertained to marking records containing SSI, including the front and back covers, the title page, and each page of the document with the

---

[58] Ibid., pp. 28079-28080, 28082-28084.

[59] Ibid., pp. 28080-28081, 28084.

Sensitive Security Information label. A distribution limitation statement was also prescribed for inclusion with the marked record.[60]

SSI disclosure was discussed in the eighth subsection. Pursuant to "a proper Freedom of Information Act or Privacy Act request," a responsive record may be disclosed "with the SSI redacted, provided the record is not otherwise exempt from disclosure" under other provisions of these laws. The part did not preclude the disclosure of SSI "to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General." Discretionary allowance was made for the disclosure of SSI in an administrative enforcement proceeding, but provision was made for requiring a security background check for parties to the proceedings to whom SSI would be disclosed.[61]

The ninth subsection indicated that violation of the part "is grounds for a civil penalty and other enforcement or corrective action ..., and appropriate personnel actions for Federal employees." The subsection continued, saying: "Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure."[62]

Finally, the 10th subsection, while acknowledging Federal Records Act requirements to preserve records containing documentation of a federal agency's policies, decisions, and essential transactions, authorized the destruction of SSI when it is no longer needed to carry out agency functions. "A covered person," according to the subsection, "must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures," but this provision "does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law."[63]

As produced in the 2004 edition of Title 49, *Code of Federal Regulations*, Part 15 cited one statutory provision as authority for its issuance: 49 U.S.C. 40119, directing the conduct of research and development activities to develop, modify, test, and evaluate a system, procedures, facility, or device to protect passengers and property against acts of criminal violence and piracy in transportation. Part 1520, however, cited several statutory provisions in this regard:

- 46 U.S.C. §§ 70102-70106, basically deriving from the MTSA, and authorizing United States facility and vessel vulnerability assessments, a national maritime transportation security plan, security incident response plans for vessels and facilities that may be involved in a transportation security incident, the issuance of

---

[60] Ibid., pp. 28081, 28085.

[61] Ibid., pp. 28081, 28085.

[62] Ibid., pp. 28082, 28085.

[63] Ibid.

transportation security cards, and the establishment of maritime safety and security teams.[64]

- 46 U.S.C. § 70117, basically deriving from the MTSA, and establishing a civil penalty for violations of the port security chapter or any regulation issued pursuant to it.[65]

- 49 U.S.C. § 114, basically deriving from the ATSA and mandating the TSA and the related DOT Transportation Security Oversight Board,[66] and which was subsequently amended by the Homeland Security Act to authorize (with the addition of Subsection 114(s)) the prescribing of "regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of" the ATSA "if the Under Secretary decides that disclosing the information would (A) be an unwarranted invasion of personal privacy; (B) reveal a trade secret or privileged or confidential commercial or financial information; or (C) be detrimental to the security of transportation."[67]

- 49 U.S.C. § 40113, prescribing general authority for the Secretary of Transportation, Under Secretary of Transportation for Security, or Administrator of the FAA, as appropriate, to take necessary action to carry out this part, including conducting investigations, prescribing regulations, standards, and procedures, and issuing orders.

- 49 U.S.C. §§ 44901-44907, prescribing security requirements for the Administrator of the FAA to prescribe regulations concerning the screening of passengers and property, the conditions for refusal of transport by intrastate and foreign air carriers, and the protection of passengers and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence or aircraft piracy; to assess, in conjunction with the Director of the FBI, current and potential threats to the domestic air transportation system; and to not approve a security program of a foreign air carrier unless it requires the foreign air carrier, in its operations to and from airports in the United States, to adhere to the identical security measures that the Administrator requires air carriers serving the same airports to adhere to. These provisions also require, under guidelines prescribed by the Secretary of Transportation, that an air carrier, airport operator, ticket agent, or an individual employed by same, receiving information about a threat to civil aviation provide that information promptly to the Secretary; and direct the Secretary,

---

[64] See 116 Stat. 2064 at 2068-2075.

[65] 116 Stat. 2084.

[66] 115 Stat. 597.

[67] 116 Stat. 2135 at 2312.

at intervals considered necessary, to assess the effectiveness of the security measures at foreign airports served by an air carrier from which a foreign air carrier serves the United States or that poses a high risk of introducing danger to international air travel, as well as other airports the Secretary considers appropriate.

- 49 U.S.C. §§ 44913-44914, concerning the deployment and purchase of explosives detection equipment and the development of airport construction guidelines.

- 49 U.S.C. §§ 44916-44918, directing the Administrator of the FAA to require each air carrier and airport that provides for intrastate, interstate, or foreign air transport to conduct periodic vulnerability assessments of the security systems of that air carrier or airport, to perform periodic audits of such assessments, and to conduct periodic and unannounced inspections of security systems of airports and air carriers to determine the effectiveness and vulnerabilities of such systems;[68] authorizing the Under Secretary for Transportation Security to deploy and otherwise provide for the training, supervision, equipping, and air carrier accommodation of federal air marshals; and authorizing the development of detailed guidance for a scheduled passenger air carrier flight and cabin crew training program to prepare crew members for potential threat conditions.[69]

- 49 U.S.C. §§ 44935-44936, directing the Administrator of the FAA to prescribe standards for the employment and continued employment of, and contracting for, air carrier personnel and airport security personnel, as well as requiring by regulation employment investigations, including criminal history record checks, for individuals employed in, or applying for, positions in airport operations and security.

- 49 U.S.C. § 44942, authorizing the Under Secretary for Transportation Security to establish performance goals and objectives for aviation security.

- 49 U.S.C. § 46105, concerning the effectiveness of prescribed regulations and orders of the Secretary of Transportation, Under Secretary for Transportation Security, and Administrator of the FAA regarding security duties and powers, as well as the amendment, modification, suspension, or superseding of such issuances.

This represents a slight increase in statutory authority cited in support of Part 1520 as it appears in the 2004 *Code of Federal Regulations* when compared with the version appearing in the 2002 edition.

---

[68] Added by 110 Stat. 3253.

[69] Added by 115 Stat. 606 and 610.

Management Regime Comparison

Presidentially prescribed arrangements for the management of classified national security information have been operative for over half a century. The initial directive in this regard, as noted earlier, was issued in March 1940, and, thereafter, successor orders largely narrowed the bases and discretion for assigning official secrecy, and increasingly detailed the management regime for security classified materials. In **Table 1** below, various aspects of the current management regime for classified information, as prescribed by E.O. 12958, as amended, are set out in comparison with the SSI management arrangements prescribed by USDA and TSA/DOT.

Table 1. Management of Security Classified Information and SSI Compared

Management Consideration	E.O. 12958, as amended	USDA SSI (Reg. 3440-002)	TSA/DOT SSI (49 CFR 15) (49 CFR 1520)
Principal terms defined	Yes	Yes	Yes
Original users of marking authority specified	Yes	Yes	No - generic covered persons
Delegation of marking authority in writing	Yes	Not clear	No
Exclusive categories of protectable information specified	Yes	Yes	Yes
Duration of marking or protection specified	Yes	Yes	No
Date or event for termination of marking/protection specified	Yes	No	No
Identity of original marker specified	Yes	No	No
Prohibitions and limitations for markings specified	Yes	Yes	No
Authorized challenges on propriety of marking	Yes	No	No
Mandatory reviews to determine continued need for protection	Yes	No	No
Appellate review of unsuccessful challenges or mandatory review outcomes	Yes	No	No
System oversight vested in specified entity or official	Yes	Yes	No

In general, the management regime for SSI prescribed by USDA does not appear to be as detailed as the regime prescribed by E.O. 12958, as amended, for classified national security information. However, the USDA regime for SSI does appear to be more detailed than the one prescribed by TSA for SSI, particularly regarding specification of users of the marking authority, limiting the duration of marking or protection, specifying prohibitions and limitations on the use of marking, and vesting system oversight in Departmental Administration (DA). This comparison is based upon the content of relevant regulations, but does not take into consideration actual implementation or administrative practice regarding those regulations.

In June 2005, the Government Accountability Office (GAO) completed an assessment of TSA management of SSI. Among the results of that assessment are the following comments:

- TSA does not have written policies and procedures, beyond its SSI regulations, providing criteria for determining what constitutes SSI.[70]

- In addition to lacking written guidance concerning SSI designation, TSA has no policies and procedures specifying clear responsibilities for officials who can designate SSI.[71]

- TSA lacks adequate internal controls to provide reasonable assurance that its SSI designation process is being consistently applied across TSA and for monitoring compliance with the regulations governing the SSI designation process, including ongoing monitoring of the process.[72]

- TSA has not developed policies and procedures for providing specialized training for all of its employees making SSI designations on how information is to be identified and evaluated for protected status.[73]

With a view to bringing "clarity, structure, and accountability to TSA's SSI designation process," GAO recommended "that the Secretary of the Department of Homeland Security direct the Administrator of the Transportation Security Administration to take the following four actions":

- establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI;

- establish clear responsibility for the identification and designation of information that warrants SSI protection;

---

[70] U.S. Government Accountability Office, *Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information*, GAO Report GAO-05-677 (Washington: June 2005), p. 3.

[71] Ibid., p. 4.

[72] Ibid., p. 5.

[73] Ibid., p. 6.

- establish internal controls that clearly define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and communicate that responsibility throughout TSA; and

- establish policies and procedures within TSA for providing specialized training to those making SSI designations on how information is to be identified and evaluated for protected status.[74]

Implications for Information Sharing

The importance of information sharing for combating terrorism and realizing homeland security was emphasized by the National Commission on Terrorist Attacks Upon the United States.[75] When fashioning the Homeland Security Act of 2002, Congress recognized that the variously identified and marked forms of sensitive but unclassified (SBU) information could be problematic with regard to information sharing. Section 892 of that statute specifically directed the President to prescribe and implement procedures for the sharing of information by relevant federal agencies, including the accommodation of "homeland security information that is sensitive but unclassified."[76]

On July 29, 2003, the President assigned this responsibility largely to the Secretary of Homeland Security.[77] Nothing resulted.

The importance of information sharing was reinforced two years later in the report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.[78] Congress again responded by mandating the creation of an Information Sharing Environment (ISE) when legislating the Intelligence Reform and Terrorism Prevention Act of 2004.[79] Preparatory to implementing the ISE provisions, the President issued a December 16, 2005, memorandum recognizing the need for standardized procedures for SBU information and directing department and agency officials to take certain actions relative to that objective.[80] In May 2006, the newly appointed manager of the ISE agreed with a

---

[74] Ibid., p. 7.

[75] See U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington: GPO, 2004), pp. 416-419.

[76] 116 Stat. 2135 at 2253.

[77] E.O. 13311 in 3 C.F.R., 2003 Comp., pp. 245-246.

[78] See U.S. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington: GPO, 2005), pp. 429-450.

[79] 118 Stat. 3638 at 3664.

[80] The White House Office, Memorandum for the Heads of Executive Departments and Agencies, "Guidelines and Requirements in Support of the Information Sharing (continued...)

March GAO assessment[81] that, oftentimes, SBU information, designated as such with some marking, was not being shared due to concerns about the ability of recipients to protect it adequately.[82] In brief, it appears that pseudo-classification markings have, in some instances, had the effect of deterring information sharing for homeland security purposes.

Improving Classified Information Life Cycle Management

In the current environment, still affected by the long shadow of the terrorist attacks of September 11, 2001, some long-standing difficulties attending the life cycle management of security classified information have become particularly acute. In July 2005, the *New York Times* observed editorially that the "Bush Administration is classifying the documents to be kept secret from public scrutiny at the rate of 125 a minute. The move toward greater secrecy," it continued, "has nearly doubled the number of documents annually hidden from public view — to well more than 15 million last year, nearly twice the number classified in 2001."[83] As the number of classification actions has been largely increasing, the editorial also noted, the volume of declassified material has been decreasing, as the data in **Table 2** below indicate. The situation appears to have slightly improved in 2005. These activities have related costs. Security classification expenses — which include personnel security, physical security, education and training, and management and planning — far exceed expenditures for declassification.

Some relief of the situation may result from the automatic action — declassification, exemption for continued protection, or referral to other agencies — on classified records 25 or more years old mandated by the Clinton executive order and now scheduled to occur by December 31, 2006. Using agencies' supplied information concerning their efforts to meet the deadline, ISOO, as of September 21, 2005, estimated that 155 million pages of classified records were subject to automatic action, and "believes, for the most part, that the Executive branch is progressing toward fulfilling its responsibilities for these records by the deadline." Of 46 agencies affected, "ISOO was confident that 22 of those agencies will be prepared to implement the Automatic Declassification program by the deadline" and will

---

[80] (...continued)
Environment," Dec. 16, 2005, Washington, DC.

[81] U.S. Government Accountability Office, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism- Related and Sensitive but Unclassified Information*, p. 25.

[82] Prepared statement of Thomas E. McNamara, Program Manager for the Information Sharing Environment, Office of the Director of National Intelligence, before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, May 10, 2006, Washington, D.C., pp. 8-9.

[83] Editorial, "The Dangerous Comfort of Secrecy," *New York Times*, July 12, 2005, p. A22.

"work closely with the remaining 24 agencies to ensure that they allocate sufficient resources to meet the requirement."[84]

Table 2. Information Moving In and Out of Classified Status

Fiscal Year	New Classification Actions	Declassified Pages	Classification Cost	Declassification Cost
2001	8,650,735	100,104,990	$4.5 billion	$232 million
2002	11,271,618	44,365,711	$5.5 billion	$113 million
2003	14,228,020	43,093,233	$6.4 billion	$54 million
2004	15,645,237	28,413,690	$7.1 billion	$48 million
2005	14,206,773	29,540,603	$7.7 billion	$57 million
2006	20,556,445	37,647,993	$8.2 billion	$44 million

Source: Data from U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2001* (Washington: Sept. 2002), pp. 7-8, 16; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2002* (Washington: June 2003), pp. 14-15, 26; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2003* (Washington: Mar. 2004), pp. 20, 25; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2004* (Washington: Mar. 2005), pp. 15, 17; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2005* (Washington: May 2006), pp. 13, 15; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2006* (Washington: May 2007), pp. 6, 22, 29-30; U.S. National Archives and Records Administration, Information Security Oversight Office, *2003 Report on Cost Estimates for Security Classification Activities* (Washington: July 2004), pp. 2-3; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report on Cost Estimates for Security Classification Activities for 2004* (Washington: May 2005), p. 3; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report on Cost Estimates for Security Classification Activities for 2005* (Washington: 2006), pp. 2, 5.

Whereas the automatic declassification effort is aimed at reducing the quantity of older records which no longer merit protected status or preservation, the Interagency Security Classification Appeals Panel (ISCAP), also created by the Clinton order, is available to address qualitative issues concerning classified information. ISCAP is composed of senior level representatives of the Secretary of State, Secretary of Defense, Attorney General, Director of Central Intelligence, Archivist of the United States, and Assistant to the President for National Security Affairs. The President selects the panel's chair from among its members. The director of the Information Security Oversight Office (ISOO), which is the government-wide overseer of the security classification program, serves as the ISCAP executive secretary. The panel makes final determinations on classification challenges appealed to it by government employees or the public; approves, denies, or amends exemptions from automatic declassification sought by agencies; makes final determinations on mandatory declassification review requests appealed to it;

---

[84] U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2005* (Washington: May 2006), p. 19.

and generally advises and assists the President in the discharge of his discretionary authority to protect the national security of the United States. The recent review activities of ISCAP are detailed in **Table 3**.

Table 3. ISCAP Decisions

Year	Documents Reviewed	Declassified in Full	Declassified in Part	Affirmed Classification
2001	34	8 (23%)	21 (62%)	5 (15%)
2002	49	9 (18%)	17 (35%)	23 (47%)
2003	106	3 (3%)	80 (75%)	23 (22%)
2004	159	11 (7%)	30 (19%)	118 (74%)
2005	81	21 (26%)	44 (54%)	16 (20%)
2006	675	139 (21%)	294 (43%)	242 (36%)

Source: Data from U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2001*, p. 5; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2002*, p. 9; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2003*, p. 9; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2004*, p. 7; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2005* (Washington: May 2006), p. 5; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2006* (Washington: May 2007), p. 6.

Finally, an issue recently arose concerning the selective withdrawal of declassified records from public access at the National Archives and Records Administration (NARA) for reclassification. This activity came to public attention on February 21, 2006, when the National Security Archive, a private sector research and resource center located at The George Washington University, published a report about the discovery on its website.[85] A news account was also simultaneously published in the *New York Times*.[86] Initial reported indications were that, beginning in 1999, intelligence agencies, pursuant to a secret agreement with the National Archives and Records Administration (NARA), began secretly removing declassified records from public access and had reclassified more than 55,000 of them. The effort was apparently an attempt to reverse what some regarded as a hasty compliance with the Automatic Declassification program prescribed in the Clinton order and directed at classified records more than 20 years old. It was discovered, however, that several

---

[85] Matthew M. Aid, *Declassification in Reverse: The U.S. Intelligence Community's Secret Historical Document Reclassification Program*, National Security Archive Report (Washington: Feb. 21, 2006), available at [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB179/].

[86] Scott Shane, "U.S. Reclassifies Many Documents in Secret Review," *New York Times*, Feb. 21, 2006, pp. A1, A16.

of the reclassified documents had been previously published in the Department of State's history series, *Foreign Relations of the United States*. Other reclassified records were regarded to be rather innocuous, such as a 1948 memorandum on a Central Intelligence Agency (CIA) plan to float balloons over communist countries in Eastern Europe and drop propaganda leaflets; a premature CIA assessment in October 1950 that Chinese intervention in the Korean War was "not probable in 1950," but actually occurred late in that month; and a 1962 telegram from Ambassador to Yugoslavia George F. Kennan containing an English translation of a Belgrade newspaper article on the Chinese nuclear weapons program. The *Times* story indicated that the director of ISOO, after reviewing 16 withdrawn records and concluding that none of them should have been reclassified, had ordered an audit of the reclassification effort.

The results of the ISOO audit were released on April 26, 2006. Agencies conducting the re-reviews of withdrawn records since 1995 included the CIA, the Department of Energy, the Department of the Air Force (USAF), and the Federal Emergency Management Agency. Their efforts "resulted in the withdrawal of at least 23,315 publicly available records; approximately 40 percent were withdrawn because the reviewing agency purported that its classified information had been designated unclassified without its permission and about 60 percent were identified by the reviewing agency for referral to another agency for declassification or other public disclosure review."[87] In reviewing a sample of 1,353 of the withdrawn records, ISOO concluded that 64 percent of them "did, in fact, contain information that clearly met the standards for continued classification," said the audit report. ISOO also found that 24% of the sampled records "were clearly inappropriate for continued classification," and "an additional 12 percent were questionable." Overall, said the audit report, "Depending upon the review effort, the sample of records withdrawn clearly met the standards for continued classification anywhere from 50 percent to 98 percent of the time."[88]

Why did this withdrawal and reclassification of records happen? ISOO offered the following explanation:

> There are a number of contributing factors to the issues identified by this audit. Sufficient quality control and oversight by both the agencies and ISOO has been lacking, as has proper documentation for declassification decisions. In addition, NARA has, at times, acquiesced too readily to the re-review efforts or withdrawal decisions of agencies. Additionally, NARA has not had the necessary resources available to keep pace with agencies' re-review activity, let alone the overall declassification activity of the recent past which has resulted

---

[87] U.S. National Archives and Records Administration, Information Security Oversight Office, *Audit Report: Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes* (Washington: Apr. 26, 2006), p. 1; also see Christopher Lee, "Some Archives Files Wrongly Kept Secret," *Washington Post*, Apr. 27, 2006, p. A25; Scott Shane, "National Archives Says Records Were Wrongly Classified," *New York Times*, Apr. 27, 2006, p. A24.

[88] U.S. National Archives and Records Administration, Information Security Oversight Office, *Audit Report: Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes*, p. 1.

> in the accumulation of hundreds of millions of previously classified pages which require processing by NARA. The most significant deficiency identified by this audit, however, was the absence of standards, including requisite levels of transparency, governing agency re-review activity at NARA. Absent these, NARA along with CIA and USAF resorted to ad hoc agreements that, in retrospect, all recognize should never have been classified in the first place.[89]

Regarding remedial actions, the audit report offered the following:

> As a result of this audit, the affected agencies have agreed to abide by interim guidance that includes provisions that require the public to be informed that records have been formally withdrawn from public access at NARA due to classification action as well as how many records are affected. Prior to official promulgation in regulation, this interim guidance will be fully coordinated, to include an opportunity for public comment. In addition, in response to many of the challenges highlighted by this audit, the principal agencies involved in conducting classification reviews of records accessioned into NARA have agreed, in principle, to create a pilot National Declassification Initiative, in order to more effectively integrate the work they are doing in this area. This initiative will address the policies, procedures, structure, and resources needed to create a more reliable Executive branch-wide declassification program.
>
> * * * * * * * * * *
>
> In response to the findings of this audit, the Director [of ISOO] is writing to all agency heads asking for their personal attention in a number of critical areas, to include facilitating classification challenges and routinely sampling current classified information in order to determine the validity of classification actions. In addition, ISOO will be initiating a number of training efforts in support of these objectives. Finally, agency heads will be requested to provide a status report within 120 days on the action taken with respect to these initiatives as well as with regard to the recommendations contained within this audit report. ISOO will report publicly on these actions.[90]

Remedial Legislation

H.R. 984 (Waxman)

Executive Branch Reform Act of 2007. Among other provisions, Section 7 would require each federal agency, not later than six months after the date of the enactment of the legislation, to submit to the Archivist of the United States and specified congressional committees a report, with certain details, describing their use of "pseudo" classification designations; would require the Archivist, not later than nine months after the date of the enactment of the legislation, to issue to specified congressional committees a report based on the agency submissions, as well as input from the Director of National Intelligence, federal offices, and contractors, with an opportunity for public comment on this report; would require the Archivist, not later

---

[89] Ibid., p. 2.

[90] Ibid.

than 15 months after date of the enactment of the legislation, to promulgate regulations banning the use of "pseudo" classification designations, with standards for exceptions for control markings other than those used for classifying national security information; and would require the Archivist to review existing statutes that allow agencies, offices, and contractors to control, protect, or otherwise withhold information based on security concerns, and make recommendations on potential changes to the statutes so reviewed with a view to improving public access to information governed by them. Introduced February 12, 2007, and referred to the Committee on Oversight and Government Reform.

H.R. 4806 (Harman)

Reducing Over-Classification Act. Requires the Secretary of Homeland Security to develop a strategy that will (1) allow the security classification of records only after unclassified, shareable versions of intelligence have been produced; (2) develop a new "sensitive and shared" information program that will provide protections for certain sensitive and unclassified information for limited periods of time under narrowly tailored circumstances; (3) propose new incentives and disincentives to encourage Department of Homeland Security personnel to classify records properly and to use "sensitive and shared" markings sparingly; (4) create training programs and auditing mechanisms for all department employees in order to ensure that the mandated strategy is being implemented properly; (5) establish an independent department declassification review board to expedite the declassification of records when the need for public access outweighs the need to classify; and (6) propose legislative solutions to ensure that the strategy is implemented in a way that not only promotes security, but also fosters both information sharing and the protection of privacy and other civil rights.[91] Introduced December 18, 2007, and referred to the Committee on Homeland Security.

Related Literature

National Security Archive. *Pseudo-Secrets: A Freedom of Information Act Audit of the U.S. Government's Policies on Sensitive Unclassified Information.* Washington: March 2006. 50 pp.

U.S. Congress. House Committee on Government Reform. Subcommittee on National Security, Emerging Threats, and International Relations. *Emerging Threats: Overclassification and Pseudo-Classification.* Hearing, 109th Congress, 1st Session. March 2, 2005. Washington: GPO, 2005. 205 pp.

U.S. Government Accountability Office. *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information.* GAO Report GAO-06-385. Washington: March 2006. 72 pp.

[91] See *Congressional Record*, daily edition, vol. 153, Dec. 19, 2007, p. E2611.

——. *Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved.* GAO Report GAO-06-369. Washington: March 2006. 23 pp.

——. *Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information.* GAO Report GAO-05-677. Washington: June 2005. 57pp.

U.S. Office of the Director of National Intelligence. *Information Sharing Environment Implementation Plan.* Washington: November 2006. 160pp.

CRS Report RL33303. *"Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information*, by Genevieve J. Knezo.

——. Federal Research Division. *Laws and Regulations Governing the Protection of Sensitive but Unclassified Information.* By Alice R. Buchalter, John Gibbs, and Marieke Lewis. Washington: September 2004. 28 pp.

U.S. National Archives and Records Administration. Information Security Oversight Office. *Audit Report: Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes.* Washington: April 26, 2006. 28 pp.