



U.S. DEPARTMENT OF
ENERGY

National Security Information Fundamental Classification Guidance Review

Report to the Information Security Oversight
Office
June 2012

United States Department of Energy
Washington, DC 20585

Working Group 6 - Cyber Security

Current Policy

The current guidance for cyber security addresses the classification of information about an Information Technology (IT) system that makes it possible to gain unauthorized access to the classified information on the IT system. Within the Department of Energy (DOE), IT systems that process classified information provide potentially lucrative targets for compromise. In conjunction with the security measures required by DOE regulations at IT facilities processing classified information, necessary precautions must be taken to protect information pertaining to security measures, where such information might assist a perpetrator in subverting the measures and penetrating the system. Accordingly, the basic principle underlying classification policy for IT system security is to protect information that is of meaningful assistance in gaining unauthorized access to the classified information being processed on an IT system.

Background

The current guidance is contained in the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4). The guidance contains 14 National Security Information (NSI) topics related to cyber security information. These topics consist of:

- Nine topics that are declassified after 25 years.
- Three topics with an event driven declassification.
- One topic exempt from automatic declassification at 25 years.
- One topic that refers to other guidance.

The current guidance does not clearly explain how this information assists an outsider in gaining unauthorized access to classified information.

Analysis

Two keystones were identified requiring protection:

- Information that could be exploited by an outside adversary to gain access to classified information on a system.
- Information that reveals a link to a foreign intelligence service.

Application of the first keystone requires defining “could be exploited by an adversary”. Classification provides very limited controls on access to the information by an insider (i.e., those associated with an L versus Q clearance). Exploitable does not mean all information that would be useful; rather it is limited to information whose exploitation would clearly result in a national security consequence. While there is a great deal of information that could provide some assistance in gaining access to the information on a classified system, classification of all this information would significantly impair operations and incur substantial costs. Classification is reserved for information that provides significant assistance to an outsider. Other controls, such as designating information Official Use Only, can be applied to information that would be

useful in gaining access, but does not meet the thresholds required to be designated as classified information. Also, classification of a security problem does not mitigate the underlying need to fix the problem. A determination of whether to classify a piece of information requires an assessment by the information owner of the risk assumed in disclosing the information against the cost of protection of the information and the impact on the ability of the Department to meet its mission.

At the time of this report, the Department has not declared any IT systems as mission critical. Because of this, this keystone does not apply to information that would allow an adversary to disable a classified IT system. If, in the future, the Department does declare an IT system as mission critical, an original classification determination will need to be made to classify information that would allow for the disablement of that system.

Because IT systems change significantly in a short time, a maximum classification duration of 10 years was assigned to this information.

Information protected by the second keystone would primarily be the equity of another agency. However, there may be some subset of this information that would be classified by DOE. It includes information identifying the source of a suspected intrusion and countermeasures in place to address these attempts. In addition, because it deals with the identity of the intruder rather than the target, this keystone applies to both classified and unclassified systems.

As these keystones serve as the underlining basis for the classification of information related to cyber security, all the topics in the cyber security guidance should reflect the classification level and duration of these keystones. The topical guidance was then examined to determine how best to apply these keystones to information generated at DOE.

A system-specific password or user generated personal identification number (PIN) code for access to a Department of Energy/National Nuclear Security Administration (NNSA) classified IT system is classified because it is an exploitable element of the security for the IT system. Possession of an authenticator for a DOE/NNSA classified IT system will allow an adversary to reduce the delay time associated with the security for that system provided by the authenticator. While authenticators function as a minor component of security compared to other elements of the security system (the other elements include physical barriers to the classified IT system and encryption technologies that prevent access to the data stream), they are a component of security that can be easily classified to provide some additional control on access to information on the IT system. In a small number of cases, the authenticator is the only barrier to access of the information on the classified IT system. For these few instances, the authenticator requires a higher level of classification to reflect what information possession of the authenticator will provide direct access.

An authenticator cannot be Restricted Data (RD) because, as security information, an authenticator does not meet the definition of RD from the Atomic Energy Act. However, section 8-303 i (1) of DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, dated February 28, 2006, to which DOE is a signatory, requires passwords to be protected at the level and category of the information to which they provide access. This

means, in practice, that while a password may have a lower classification level than the information on the classified IT system, it requires storage and handling commensurate with the level and category of the information on the classified IT system. In addition, the authorization provided by a security clearance to access information of a particular classification level and category does not authorize access to an authenticator that provides access to information of the same classification level and category. Security policies may place additional restrictions, such as limits on the sharing of passwords or PIN codes, independent from the classification.

Information regarding a plan and/or schedule for conducting an upcoming IT system security test (procedures, dates, times, etc.) for the purpose of assessing computer security measures is classified when such knowledge would significantly assist in an attack on a classified IT system. Because classification does not provide a significant barrier to access of the information by an insider, this information must significantly assist an outside adversary in an attack in order to be classified. Information about a completed test is classified when this information can be used to determine exploitable information about a future test.

Information about methods to circumvent existing hardware and supporting software that provides security for a classified network is owned by the NSA and should be referred to that agency for classification determinations.

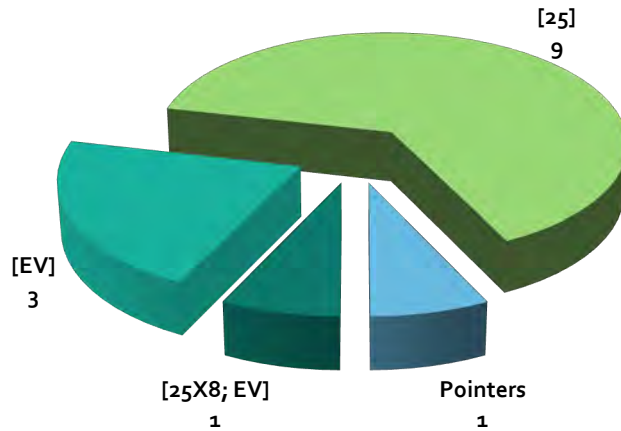
Recommendations

Rewrite the guidance to reflect the classification of the keystones. In addition, clarify throughout the guidance that while authenticators cannot be classified RD, they will be protected as such in accordance with the NISPOM. Topics should be added to refer information that reveals a link to a foreign intelligence service to the cognizant counterintelligence organizations. This would result in the following changes in guidance:

- 10 topics would be eliminated because of redundancy.
- 2 topics would be changed from a 25-year duration to an event or 10 years, whichever occurs first.
- 1 topic would replace 2 classification determinations with instructions to refer the information to another agency.

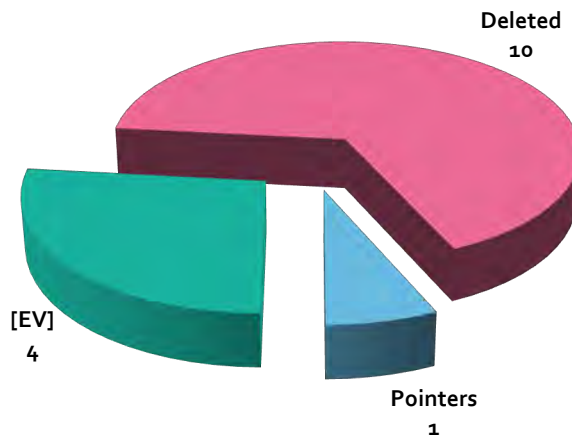
The following chart identifies the declassification instructions used in the current guidance:

Current Guidance Attributes



The following chart identifies the changes from the current guidance:

Recommended Guidance Attributes



Working Group 7 - Information Security

Current Policy

Five sections of *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4) contain topics that address non-Information Technology information security. These sections are titled Incidents of Security Concern, Protection Program Operations, Classification Change Notices, Operations Security, and Nuclear Material Control and Accountability. These topics address the classification of compromise information, information related to investigations of security incidents, the loss of classified matter, combinations, classification change notices, operational security assessments, and the fact of a missing item of SNM. In some cases, it is not clear how the information classified by these topics would cause damage to national security if disclosed. Other topics seem to identify some information as NSI that should be protected as Restricted Data or Formerly Restricted Data.

Background

The topics in the Incidents of Security Concern section attempt to address the classification of all information generated in the inquiry into a security incident. The section begins with topics covering the classification of compromises that occur by e-mail or other electronic means. It then moves to the classification of FBI involvement in an investigation at a DOE facility. The section also contains topics for missing classified matter and compromises of classified information. These topics consist of:

- Nine exempt from automatic declassification at 25 years.
- Ten with an event driven classification.
- One that points to other guidance.

In the Protection Program Operations section, one topic classifies combination and codes. This topic classifies a combination or code at the level and category of the information to which the combination or code provides access. A note to the topic instructs that a combination or code be designated at the highest level, category, and access caveats associated with the material in the security container. This topic has an event driven declassification. Four topics in this section classify the fact of an attempted theft or diversion of a nuclear weapon or SNM of a certain quantity or greater. Three of these topics have an event driven declassification. One is exempt from automatic declassification at 25 years.

The section titled, Classification Change Notices contains three topics that point to other guidance. The remaining topic classifies change notices until all the classified matter has been upgraded and there is a reasonably certainty that no compromise occurs. This topic is exempt from automatic declassification at 25 years.

In the Operations Security section, the topics classify information related to an operations security (OPSEC) assessment (OA). This includes statements of the threat, descriptions of OPSEC procedures, methods to defeat countermeasures, OA planning information, OA results, critical program information, and indicators. These topics consist of:

- Seven exempt from automatic declassification at 25 years.
- One that is declassified at 10 years.
- Seven with an event driven declassification.
- Five that point to other guidance.

The section titled Nuclear Material Control and Accountability contains four topics that address the fact of a missing item of SNM. Two of these topics are exempt from automatic declassification at 25 years. The remaining two topics have an event driven declassification.

Analysis

The following three keystones were identified for the information:

- Information that would assist an adversary in acquiring classified information.
- Information that would assist an adversary in acquiring material (SNM, a weapon, a part).
- Information that can damage foreign relations.

When DOE or a DOE contractor cannot account for either SNM or a classified document (i.e., any medium that conveys classified information, such as printed matter, an e-mail, a CD-ROM, or a hard drive), meaning that it is not immediately known what happened to the SNM or classified document, a search is initiated. If the search fails to locate the SNM or classified document or there is evidence to suggest theft, the Federal Bureau of Investigation (FBI) is notified and provided an opportunity to conduct an investigation.

The FBI may classify the fact of their involvement in an investigation at a specific site or facility. The FBI may also classify details of the investigation. Once FBI involvement begins, FBI classifies information about the investigation and that agency should be contacted for guidance. At the conclusion of the investigation or if the FBI chooses not to conduct an investigation, the Office of Classification should be contacted to determine if any unique information regarding the incident requires classification. This could include information that was classified by the FBI during but not after completion of the investigation. It could also include information that is still classified by the FBI where it has been determined a separate DOE equity exists. In any case, specific classification guidance for the incident will be generated either during or after the completion of the FBI investigation.

In the event of a suspected overt theft, the Emergency Operations Center (EOC) and the Tactical Operations Center (TOC) at the site would be activated. The protective force staffs the TOC, which supports the security incident commander (IC) in tactical matters. The TOC serves as the primary focal point for the security IC and the point of contact for outside law enforcement agencies. The EOC coordinates between the incident commander and the site manager, the individual in charge of coordination of site/facility response activities.

During the theft, the IC determines how information will be controlled. This includes what information can be transmitted over unencrypted radios and what information can be shared with local law enforcement. The IC bases these determinations on assumptions of what the target of

the theft is and a judgment that release of the information will assist in disruption of the suspected theft or the recapture or recovery of the stolen matter. After disruption of the theft or recapture or recovery of the matter, the site manager determines what information to release about the incident to local law enforcement and the local government through the EOC.

If, after the incident, there is a decision to classify information related to the theft, the information released by the IC and the site manager will be examined to determine whether it can be returned to Government control. An original classification authority will decide what information to classify related to an incident based on the results of this examination.

When given a piece of classified foreign government information (FGI), the Government agrees to protect the information in the same manner as U.S. classified information of an equivalent level. As the disclosure that the U.S. Government may have mishandled specific FGI could cause damage to foreign relations, particularly with the foreign government whose information may have been compromised, the fact that FGI belonging to a specified country cannot be accounted for is classified. Any information that identifies a specific classified document as unaccounted for when that document contains FGI is classified.

A determination that a classified document is missing occurs after the Government has concluded there was no act of theft and has performed an exhaustive search with the assistance of other agencies and local and state law enforcement of all potential locations of the document. As the resources of the Government were not able to locate the document with all available information, it is not credible for an adversary to locate the document with the same information. Because of this, most of the information about a document determined to be missing is not classified.

Information that significantly assists an adversary in locating classified information in the open literature or public domain (such as a web site, book, or a periodical) where the information is immediately available and there is no Government restriction to accessing the information is classified. Once the information contained in a document has been compromised, placing the document back under Government security controls does not recover the information. If the Government is unable to re-control the information through a mechanism such as a nondisclosure agreement, information that allows an adversary to locate the document, including information that identifies the document, is classified.

Combinations for security container locks that contain classified information are classified at the level of the information inside the container. Combinations cannot be RD or FRD as combinations are security components and do not meet the definition for RD or FRD in the Atomic Energy Act. The determination to protect the information at the level of the information inside the container comes from the National Industrial Security Program Operating Manual (NISPOM) to which the DOE is a signatory. See section 5-308 of the NISPOM for details. The NISPOM does not contain protection requirements for SNM, but the combinations for security containers that contain a Category I or II quantity of SNM are classified to limit dissemination of the combination between employees at the facility.

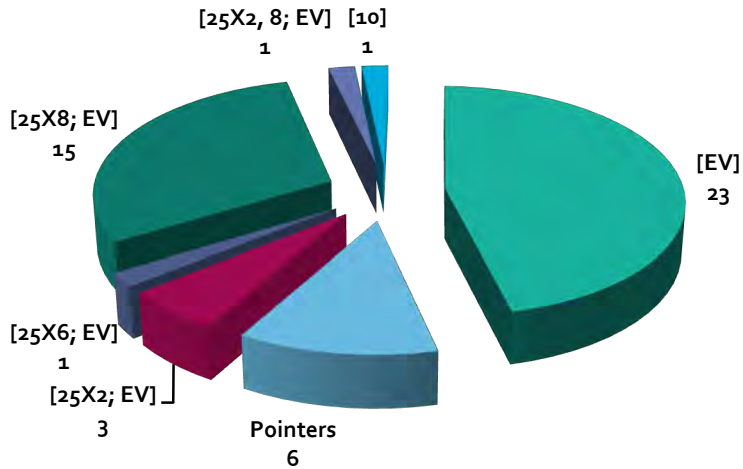
Recommendations

Rewrite the guidance to reflect the working group analysis. These changes results in new guidance that contains 29 NSI topics. The topics consist of the following:

- Twenty-one topics will be deleted.
- Six topics will be exempt from automatic declassification at 25 years.
- Five will have an event driven declassification.
- Eighteen will point to other guidance.

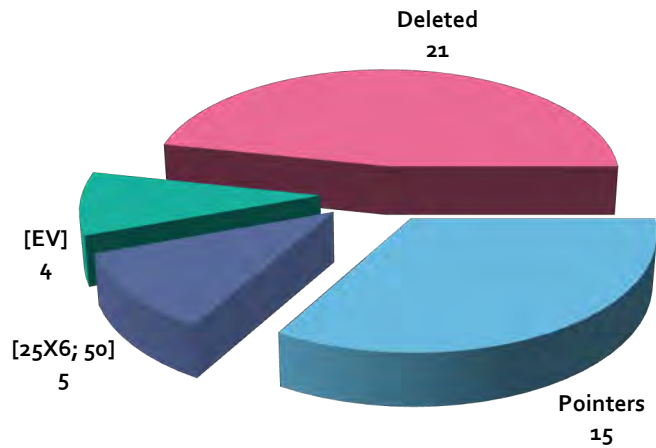
The following chart identifies the declassification instructions used in the current guidance:

Current Guidance Attributes



The following chart identifies the changes from the current guidance:

Recommended Guidance Attributes



Working Group 8 - TEMPEST, COMSEC, and Cryptology

Current Policy

Communications security (COMSEC) is the measures and controls taken to deny unauthorized individuals information derived from telecommunications while ensuring the authenticity of such telecommunications. These measures include TEMPEST, a short name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment, and cryptology, the science and study of codes and cipher systems. With the introduction of Secure Terminal Equipment (STE) in government, the Atomic Energy Commission (AEC), the predecessor agency to the Department of Energy (DOE), developed classification guidance with the concurrence of the National Security Agency (NSA), the owners of the STE information. The current guidance for TEMPEST, COMSEC, and Cryptology Information provides classification guidance for the protective measures in place to deny unauthorized individuals information derived from telecommunications of the U.S. Government that is related to national security.

Background

In 1985, DOE decided to combine a variety of safeguards and security classification guidance into a single document entitled, "CG-SS-1, Safeguards and Security Classification Guide". The topics from the STE guidance were updated and coordinated with NSA before being incorporated as a chapter in this guide. CG-SS-1 has been updated several times since 1985 and is now the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4), change 6.

CG-SS-4 contains 102 topics that address the classification of TEMPEST, COMSEC, and Cryptology Information. These topics consist of:

- Thirty-five topics exempt from automatic declassification at 25 years that are declassified at 50 years.
- Fifty-three topics exempt from automatic declassification at 25 years with an event driven declassification.
- One topic with an event driven declassification.
- Thirteen topics that point to other guidance.

Analysis

The NSA, the equity owner for COMSEC information, reviewed the guidance in CG-SS-4 as part of that agency's FCGR activities. They recommended removing the topics from DOE guidance as they have made their classification guides available electronically.

Recommendations

- Remove the topics from DOE guidance in accordance with the NSA recommendation.

The following chart identifies the declassification instructions used in the current guidance:

Current Guidance Attributes

