# DEPARTMENT OF HOMELAND SECURITY

# NATIONAL SECURITY IT SYSTEMS CERTIFICATION AND ACCREDITATION

# SECURITY CLASSIFICATION GUIDE

# (DHS SCG OS-002 (IT))

**March 2004**

**Issued and Approved By:**

**Signed 3/29/2004 Original Signed Copy Maintained at DHS Office of Security**

_____

**Jack L. Johnson, Jr.**

**Chief Security Officer**

**Department of Homeland Security**

**March 29, 2004**

_____

**Date**

# DHS SCG OS-002 (IT)

## National Security IT Systems Certification & Accreditation

## March 2004

## Department of Homeland Security
## Office of Security
## Washington D.C. 20528

| Change Number | Date of Change Notice |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

**NATIONAL SECURITY IT SYSTEMS CERTIFICATION & ACCREDITATION**
**SECURITY CLASSIFICATION GUIDE**
**TABLE OF CONTENTS**

# 1 GENERAL

## 1.1 PURPOSE

This classification guide is issued for the purpose of identifying specific topics of information associated with the certification and accreditation (C&A) of information technology (IT) systems used for storing, transmitting, and processing classified national security information (classified information) and requiring classification and protection in accordance with Executive Order 12958, “Classified National Security Information,” as amended, and its implementing directives. The guide also provides topics of information that do not meet the standards and criteria for classification under E.O. 12958, as amended, but are nonetheless sensitive and require protection against unauthorized disclosure. Such sensitive but unclassified information shall be categorized as “FOR OFFICIAL USE ONLY” (FOUO) and marked as applicable to reflect that status.

## 1.2 AUTHORITY

This guide is approved by Jack L. Johnson, Jr., Chief Security Officer, Department of Homeland Security, a delegated TOP SECRET Original Classification Authority. It is issued in accordance with Executive Order 12958, as amended, and Information Security Oversight Office (ISOO), Directive No. 1 (32 CFR, Part 2001/2004), “Classified National Security Information; Final Rule.”

## 1.3 SCOPE AND APPLICABILITY

This document provides security classification guidance for information associated with the C&A of IT systems used for storing, transmitting, and processing classified information. This guide shall be cited as the basis for classification, reclassification, and declassification of information and materials under DHS cognizance and control related to the C&A process. Changes in classification guidance required for operational necessity will be made immediately upon notification and concurrence of the approving authority and will be disseminated to original recipients of this guide. The provisions of this guide are applicable to all organizational entities and contractors associated with the Department of Homeland Security.

## 1.4 OFFICE OF PRIMARY RESPONSIBILITY

The Office of Primary Responsibility (OPR) for this guide is:

Department of Homeland Security
Office of Security
Administrative Security Division
Washington D.C. 20528

Telephone: (202) 772-5012
Fax: (202) 772-9990

### 1.5 RELATED GUIDANCE

Classification guidance related too or associated with the topical guidance provided in this SCG can be found in DHS SCG OS-001(IT), Homeland Security Data Network. A copy of the related guidance can be requested from the Office of Primary Responsibility identified in Section 1.4 above.

## 2 POLICY

### 2.1 GENERAL

The Certification and Accreditation of DHS National Security IT Systems will be in accordance with MD-4300B, DHS Policy Guide for National Security Systems. Certification of National Security IT Systems establishes the extent to which a particular IT design and implementation meets a specified set of security requirements. Certification primarily addresses software and hardware security safeguards, but also considers procedural, physical, and personnel security measures employed to enforce IT security policy.

Accreditation is the official management authorization to operate an IT system based on a particular mode of operation; a prescribed set of security safeguards; a defined threat with stated vulnerabilities and safeguards; a given operational environment; a stated operational concept; a stated interconnection to other IT; an operational necessity; and an acceptable level of risk for which a Designated Approval Authority (DAA) has formally assumed responsibility.

### 2.2 REASON FOR CLASSIFICATION

Classification is reserved for specific categories of information or the compilation of related information meeting the standards and criteria for classification as defined in E.O. 12958, as amended, and falling within one or more of the categories of information eligible for classification per Section 1.4 of the Order. The topics of information cited in this guide are classified pursuant to:

> Section 1.4(e): scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
>
> Section 1.4(g): vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism

### 2.3 CLASSIFICATION BY COMPILATION

A compilation of unclassified information is normally not classified. However, in certain circumstances, information that would otherwise be marked unclassified may become classified when combined or associated with other unclassified information, if the

compiled information reveals an additional association or relationship that meets the standards and criteria for classification. Under such circumstances, it is the additional association or relationship revealed by the combination or compilation of information that is classified, not the individual items of information. Users of this SCG should be aware of such a possibility when compiling unclassified information. (See 2.4 Below)

Likewise, the compilation of classified information will be classified, at a minimum, at the highest classification within the aggregated data, but may become a higher classification if the compiled information reveals an additional association or relationship that warrants a higher level of classification. (See 2.4 Below)

## 2.4 EXCEPTIONAL CIRCUMSTANCES

Should a situation arise where a holder of information believes the information should be classified but it is not covered by this classification guide, or, a compilation of unclassified information should be classified or, if already classified, classified at a higher level, the information will be handled and safeguarded in accordance with the level of classification the holder believes it to be.

In such instances, the information will be marked with the tentative level of classification and the notation *"Pending Classification Review."*

The information will be transmitted, by a means approved for the level of classification, to the OPR identified in Section 1.4 of this guide, for a classification determination.

## 2.5 CHALLENGES TO CLASSIFICATION

If at any time security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until such time as a formal decision by an appropriate authority is made. Classification challenges should be addressed to the OPR identified in Section 1.4 of this guide. Appeal procedures to classification determinations are found in 32 CFR Part 2001/2004, "Classified National Security Information," Directive No. 1, Final Rule.

## 2.6 USE OF THIS GUIDE

This guide is for the use of DHS employees and contractors performing derivative classification actions when addressing the elements of information covered by this guide. For the purpose of marking documents containing classified information covered by this guide, derivative classifiers will cite "DHS SCG OS-002 (IT), Dated March 2004," on the "Derived From" line, followed by the declassification instruction as specified in the guide. For Example:

> *Derived From: DHS SCG OS-002 (IT), March 2004*
> *Declassify On: (Insert declassification instruction as cited for the particular Topic in the SCG)*

If classified information covered by this guide, as well as classified information from other classified sources, is included in the same document, the document will be marked as follows:

> *Derived From: Multiple Sources*

*Declassify On: (Carry forward the single most restrictive declassification instruction from all source documents)*

NOTE: If "Multiple Sources" are used for a derivatively classified document, a record of the sources used will be maintained with the file copy of the document.
Where the declassification instruction of a source(s) is marked "OADR" or "Originating Agency Determination Required," or, the declassification instruction from a source(s) cites X-1 thru X-8, the declassification instructions for the newly created document will state: "Source Marked OADR," followed by the date of the most recent source; or, "Source Marked X-(applicable exemption number)" followed by the date of the most recent source. For example:

*Derived From: Multiple Sources*
*Declass On: Source Marked OADR, Date of Source Sep 21, 1995*

*Derived From: Multiple Sources*
*Declass On: Source Marked X-1, Date of Source Sep 21, 2003*

### 2.7 CLASSIFIED PROCESSING

Classified information will not be processed on any automated IT equipment unless the equipment has been specifically accredited and approved for classified processing. Consult office/organizational element security officials for instructions on what equipment may be used.

### 2.8 MARKING

Detailed instructions for marking classified materials can be found in the DHS Security Manual and the ISOO pamphlet titled "Marking." Training on marking classified materials can be obtained by contacting the DHS Office of Security at (202) 358-1438. The ISOO Marking Pamphlet is available for download at http://www.archives.gov/isoo/index.html. You can also download it from the DHS internal intra-net, DHSOnline, by going to the Security portal, Information Security, "ISOO Marking Booklet 2003."

### 2.9 REPRODUCTION AND DISSEMINATION

This guide may be reproduced and disseminated within DHS as needed. However, to ensure receipt of updates, revisions, and classification changes, whenever the guide is disseminated beyond an initial addressee, notify the OPR.

Coordinate dissemination to government agencies outside of DHS through the OPR.

## RELEASE OF INFORMATION

### 3.1 PUBLIC RELEASE

The fact that this guide indicates that some information may be unclassified does not imply that the information is automatically releasable to the public. Request for public release of information will be processed in accordance with the DHS MD Number 0460.1, “Freedom of Information Act Compliance.”

This guide is designated “FOR OFFICIAL USE ONLY” and will not be released to the public. Requests for copies of this guide by non-governmental officials will be processed under the Freedom of Information Act.

### 3.2 SENSITIVE UNCLASSIFIED INFORMATION

The classification guide applies to information that requires protection to prevent damage to the national security and thus requires classification in accordance with E.O. 12958, as amended. In addition to classified information, there are certain types of sensitive but unclassified information for which Executive Branch agencies require application of controls and protective measures for a variety of reasons. FOR OFFICIAL USE ONLY (FOUO) is the designation that is applied by DHS to sensitive but unclassified information that may be exempt from mandatory release to the public under Section 552 of Title 5, U.S.C., “Freedom of Information Act (FOIA).”

## 4 EFFECTIVE DATE AND IMPLEMENTATION

This classification guide is effective immediately upon release.

## National Security IT Systems Certification & Accreditation

## Security Classification Guidance
## (DHS SCG OS-002 (IT))

| 1. GENERAL | | | |
|---|---|---|---|
| **TOPIC** | **CLASSIFICATION** | **DURATION** | **REMARKS** |
| a. Information revealing the location of a Special Compartmented Information Facility (SCIF) in association with the categories of SCI information processed on classified IT system(s) in those locations. | CONFIDENTIAL | 15 Years From Date of Origin | |
| b. . Information revealing the location of a collateral classified IT systems, sites, remote terminals, etc. | FOUO (See Remarks) | (See Remarks) | Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance. |
| c. Classified IT systems accounting or appropriation data, budget estimates, and/or funding levels. | FOUO (See Remarks) | (See Remarks) | Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance. |
| d. Classified IT systems program/project milestone schedule. | FOUO (See Remarks) | (See Remarks) | Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance. |
| **2. SYSTEMS INFORMATION** | | | |
| a. Location of servers, routers, switches, or other systems management equipment or devices. | FOUO (See Remarks) | (See Remarks) | Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance. |

| TOPIC | CLASSIFICATION | DURATION | REMARKS |
|---|---|---|---|
| b. Types of servers, routers, switches, etc., in use. | FOUO (See Remarks) | (See Remarks) | Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance. |
| c. Identification of software used on the system. | FOUO (See Remarks) | (See Remarks) | Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance. |
| d. Type of Intrusion Detection software and/or hardware used on the system. | FOUO (See Remarks) | (See Remarks) | Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance. |
| e. Identification of cryptographic and encryption equipment/infrastructure. | FOUO (See Remarks) | (See Remarks) | Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance. |
| f. Network Diagrams, drawings, flow charts that depict non-specific classified IT connectivity. | FOUO (See Remarks) | (See Remarks) | Information will be designated as FOUO unless it is otherwise classified under authorities associated with a classified program or process that is itself classified. In this instance, classification and declassification will be applied in accordance with the program guidance. |
| g. Network Diagrams, drawings, flow charts that depict the complete classified system IT connectivity, node information, port information, and geographic locations. | SECRET | 15 Years from date of origin | |

| TOPIC | CLASSIFICATION | DURATION | REMARKS |
|---|---|---|---|
| h. System Test and Evaluation (ST&E) results containing information classified pursuant to this guide. | (See Remarks) | (See Remarks) | Classify and declassify in accordance with the applicable instructions provided in this guide.<br><br>ST&E documentation containing no information classified pursuant to this guide will, at a minimum, be categorized as FOUO.<br><br>(See Section 3) |
| **3. VULNERABILITIES** | | | |
| a. Identification of specific architecture or application vulnerabilities which, if exploited, could result in the compromise of the confidentiality, integrity or availability of the classified IT system. | SECRET | 10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks) | If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations. |
| b. Details of an exploitable security system vulnerability that, if disclosed, could lead to the compromise of classified information. | SECRET | 10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks) | If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations. |
| c. Details of an exploitable physical security vulnerability that, if disclosed, could lead to the compromise of classified information. | SECRET<br>CONFIDENTIAL<br>Or<br>FOUO<br>(See Remarks) | 10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. | Classify as Secret if the exploitable vulnerability offers direct and unimpeded access to classified information with a negligible chance of detection.<br><br>Classify as Confidential if the exploitable vulnerability offers potential access to classified information with minimal effort.<br><br>Categorize as FOUO if the exploitable vulnerability is one of multiple layers of a defense in depth with minimal chance of an unauthorized person gaining access to classified information. |

| TOPIC | CLASSIFICATION | DURATION | REMARKS |
|---|---|---|---|
| d. Status of corrective action to address vulnerabilities of applications or operating systems (COTS or GOTS) that are used by and associated by name with the classified IT system. | SECRET | 10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks) | If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations. |
| e. Status of corrective action to address vulnerabilities of applications or operating systems (COTS or GOTS) that are used by but not associated by name with the classified IT system. | FOUO | N/A | |
| f. Vulnerabilities of data links that are used by and associated by name with the classified IT system. | SECRET | 10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks) | If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations. |
| g. Vulnerabilities of data links that are used by but not associated by name with the classified IT system. | UNCLASSIFIED | N/A | |
| h. Classified IT system vulnerabilities not listed in this guide which, if exploited, could result in the compromise of classified information or the confidentiality, integrity or availability of HSDN. | SECRET | 10 years from date of discovery, or, upon confirmed elimination of the vulnerability, whichever occurs sooner. (See Remarks) | If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations. |
| **4. INCIDENTS** | | | |
| a. Existence of a penetration to the classified IT system without further elaboration. | FOUO | N/A | |

| TOPIC | CLASSIFICATION | DURATION | REMARKS |
|---|---|---|---|
| b. Details of a penetration or attempted penetration of a classified IT system that if disclosed, could lead to the compromise of classified information. | SECRET | 10 years from date of discovery, or, upon confirmed and successful deployment or installation of countermeasures that prevent similar events from occurring, whichever occurs sooner. (See Remarks) | If the vulnerability exists at multiple locations, declassification will not occur until the vulnerability has been eliminated at all locations. |
| c. Information concerning the loss or mishandling of classified information:<br>• Report of the compromise of classified information without elaboration.<br>• Report of the compromise of classified information that is specific and details the classified information compromised. | FOUO<br>(See Remarks) | N/A<br>(See Remarks) | Classify and declassify in accordance with the classification/declassification instructions cited on the compromised material. |
| • Report confirming that classified information was sent to an unauthorized recipient or over an unclassified network.<br>• Report that identifies by name the individual who obtained unauthorized access to classified information and/or the classified IT system. | CONFIDENTIAL<br>CONFIDENTIAL | 5 years from date of incident, or, upon execution of a non-disclosure agreement by the unauthorized recipient or upon successful sanitization of the classified material from the system.<br>5 years from date of incident, or, upon execution of a non-disclosure agreement by the unauthorized recipient or upon successful sanitization of the classified material from the system. | |

## DEFINITIONS

**Access.** The ability and opportunity to obtain knowledge of classified information.

**Accreditation.** The official management authorization to operate an IT system based on a particular mode of operation; a prescribed set of security safeguards; a defined threat, with stated vulnerabilities and safeguards; a given operational environment; a stated operational concept; a stated interconnection to other IT; an operational necessity; and an acceptable level of risk for which the DAA has formerly assumed responsibility.

**Applicable Associated Markings.** Markings, other than those which designate classification level, that are required to be placed on classified documents. These include the "Derived From" line, downgrading and declassification instructions, special control notices, Special Access Program caveats, etc.

**Automatic Declassification.** The declassification of information based upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under Executive Order 12958, as amended.

**Certification.** The comprehensive testing and evaluation of the technical and non-technical IT security features, and other safeguards used in support of the accreditation process.

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

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

**Classification Guide.** A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

**Classified National Security Information.** Information that has been determined pursuant to E.O. 12958, as amended, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Also known as classified information.

**Classifier.** An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority (OCA) or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

**Communications Security (COMSEC).** The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC materials and information.

**Compilation.** An aggregation of pre-existing unclassified items of information. Compilations of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that qualifies for classification pursuant to E.O. 12958, as amended, and is not otherwise revealed by the individual information. Classification by compilation must meet the same standards and criteria as other original classification actions.

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

**Configuration Management.** The process involving identifying, controlling, accounting for, and auditing all changes made to the baseline system architecture. Included are hardware, firmware, and software.

**Cryptology.** The branch of knowledge which treats the principles of cryptography and cryptanalytics; and the activities involved in producing signals intelligence (SIGINT) and maintaining communications security (COMSEC).

**Damage to the National Security.** Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information.

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

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

**Derivative Classification.** Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance provided in a security classification guide. The duplication or reproduction of existing classified information is not derivative classification.

**Designated Accrediting Authority (DAA).** Senior management official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

**Document.** Any physical medium in or on which information is recorded or stored, to include written or printed matter, audio-visual materials, and electromagnetic storage media.

**Event.** An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.

**For Official Use Only.** The term used within DHS to identify sensitive but unclassified information, in any form, the release of which could cause harm to a persons privacy or welfare, adversely impact economic or industrial institutions or infrastructure, compromise programs or operations essential to the safeguarding of our national interests, or violate a statute, treaty, or other agreement enforceable by law. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, “Classified National Security Information,” as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

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

**Information Security.** The system of policies, procedures, and requirements established under the authority of E.O. 12958, as amended, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

**Material.** Any product or substance on or in which information is embodied.

**National security.** The national defense or foreign relations of the United States.

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

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

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

**Regrade.** To raise or lower the classification assigned to an item of information.

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

**Telecommunications.** The preparation, transmission, or communication of information by electronic means.

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