(U) U.S. Insider Threat
Security Classification Guide

Version 1.0

Effective: 16 December 2013

~~***This document is not approved for public release.***~~

THIS PAGE LEFT INTENTIONALLY BLANK

(U) FOREWORD

(U) The *Insider Threat Security Classification Guide 1.0* provides authoritative classification guidance for U.S. insider threat activities based on Executive Order (EO) 13526 – *Classified National Security Information*, its implementing directive 32 CFR Part 2001, EO 13587, the Atomic Energy Act of 1954 as amended, the National Insider Threat Policy, and the National Insider Threat Minimum Standards. This guide applies to all executive branch agencies that handle classified national security information and **broadly** complements applicable classification guidance from U.S. government agencies involved in insider threat activities.

(U) This *Guide* is the primary source of derivative classification guidance, in the absence of an agency's guidance, that shall be followed in interagency implementation of EO 13587 - *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,* concerning national insider threat policies. The intent of this *Guide* is to provide common terminology and baseline classification guidance to be used among the various U.S. government agencies involved in government insider threat activities pursuant to the Order and the National Insider Threat Minimum Standards. Consistent with EO 13587, nothing herein is intended to supersede or alter the existing procedures, guidelines, or authorities of individual U.S. departments or agencies for classifying their internal insider threat activities.

(U) The *Guide* provides classification and marking guidance for derivative classifiers in protecting U.S. insider threat information from Unclassified to Top Secret. It is not a classification source for Special Access Program (SAP) or Sensitive Compartmented Information (SCI) categories. Classifiers will refer to the applicable agency or program guides for classification guidance involving these categories.

Approved by:

(b)(3)

[redacted]

16 DEC 13

Date

National Counterintelligence Executive
Office of the National Counterintelligence Executive
Office of the Director of National Intelligence

(U) TABLE OF CONTENTS

(U) CHANGE REQUEST LOG

Change log is UNCLASSIFIED

Revision	Date	Description of Change	Change Request(s) Assigned to the Revision*
1.0	Dec 2013	Initial publication	

1.0 (U) INTRODUCTION

1.1 (U) Scope

(U) The *U.S. Insider Threat Classification Guide*, hereafter referred to as the "*Guide*," is the Executive Branch's standard reference for derivative classification determinations on insider threat activities. The *Guide* provides a baseline for protecting United States Government (USG) policy associated with insider threat activities and shall be used in concert with existing agency or program level classification guidance concerning insider threats, as appropriate. The *Guide* provides minimum standards for classification of insider threat information and does not supersede any agency's Original Classification Authority. Nothing in this *Guide* prohibits agencies from establishing classification guidance that is more restrictive than the citations contained in this *Guide*, as necessary to protect sensitive sources or methods. If applicable, users should refer to their respective agency classification guides first before applying guidance contained herein.

(U) The *Guide* covers Unclassified to TOP SECRET information falling under EO 13526-*Classified National Security Information* (referred to as "The Order"). This *Guide* will be used to make derivative classification determinations on national security information generated by insider threat activities pursuant to EO 13526, EO 13587- *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, and the Atomic Energy Act of 1954, as amended.

(U) Classification determinations for SCI or SAP compartmented program information shall be accomplished using the applicable agency or program security guide. Members of the Intelligence Community (IC) should contact the Office of the Director of National Intelligence, Office of the Chief Information Officer, Information Management Division (IMD) for additional guidance. Other USG agencies should consult their Classification Management or Program Management Office for additional guidance.

(U) Users who create classified information that impacts insider threat activities pursuant to EO 13587 are obligated to classify the information based upon this *Guide*, a source document, or an agency or a compartmented program guide/manual. Users are also reminded that dissemination controls must be applied in accordance with their specific agency policies. Agencies are expected to review their internal classification guidance and ensure that their agency guidance is at least at the levels established in this *Guide*. In cases where there may be a conflict with existing insider threat guidance specific to an agency or department, this *Guide* shall apply unless the agency guidance is more restrictive. In that case, the agency guide shall apply. Individuals who fail to protect classified information may be subject to criminal, civil, and administrative sanctions outlined in section 5.5 of EO 13526. Over-classification shall be avoided.

(U) This *Guide* does not alter existing authorities or classification guidance, for specific agency, program, or project-level activities. However, it is understood that, prior to the publication of this

Guide, some agencies may have dealt with insider threat information at the unclassified level. These agencies must now follow the minimum guidance contained herein, unless agency, program or project-level classification guidance is more restrictive, as discussed in the preceding paragraph. The use of this *Guide,* is intended to be prospective in its application. Classification decisions made prior to the effective date of this *Guide* need not be modified to reflect classification levels contained in this *Guide* until the information is reused. At the time of reuse, agencies must reclassify the information according to this *Guide* or as detailed in an approved agency, program or project-level guide.

(U) A list of the documents referenced in and related to this *Guide* is detailed in Appendix A- *Reference Documents*. Appendix B provides a change request form. Appendix C provides a list of acronyms terms of commonly used phrases within classification management.

1.2 (U) Definitions

(U) The following unclassified terms are defined for the purposes of this *Guide* and should be used when possible in interagency documents and communications on insider threats to ensure common understanding:

Access: the ability or opportunity to gain knowledge of classified information.

Agency: any "executive agency," as defined in 5 U.S.C. 105; "military department," as defined in 5 U.S.C. 102; "independent establishment," as defined in 5 U.S.C. 104; intelligence community element as defined in Executive Order 12333; and any other entity within the executive branch that comes into the possession of classified information.

Agency Head: the head of any: "executive agency," as defined in 5 U.S.C. 105; "military department," as defined in 5 U.S.C. 102; "independent establishment," as defined in 5 U.S.C. 104; intelligence community element as defined in Executive Order 12333; and any other entity within the executive branch that comes into the possession of classified information.

Aggregation, Classification by: the amalgamation of separate pieces of information which individually are either unclassified but when taken together become classified; also known as classification by compilation.

Classification Guide: a classification guide is a document prepared by an Original Classification Authority with cognizance over a specific subject to provide derivative classification sourcing for derivative classifiers. Classification guides include specific facts or topical elements within the subject area, the level of classification of those facts or topical elements, and information regarding the duration of classification and any dissemination or other controls that should be applied by derivative classifiers. Unlike source documents, classification guides generally allow for durations of classification that extend from the date that the derivatively classified document is created rather than from the date of the guide itself.

Classified Information (Classified National Security Information; NSI): information that has been determined pursuant to EO 13526 or any predecessor order or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Cleared Employee: a person who has been granted access to classified information, other than the President and the Vice President, employed by, or detailed or assigned to, a department or agency, including members of the armed forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

Controlled Unclassified Information (CUI): as set forth in Executive Order 13556, CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526 or the Atomic Energy Act of 1954, as amended.

Counterintelligence: information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

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

Declassification Event: an event that eliminates the need for continued classification of information.

Declassify On: the portion of the Classification/Declassification Authority Block which indicates the duration of classification of a classified document.

Derivative Classification: the 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 a classified source document or using guidance from a classification guide. The duplication or reproduction of existing classified information is not derivative classification.

Derived From: that portion of the classification authority block that specifies the classification source(s) of other derivative or originally classified documents.

Director of National Intelligence (DNI): the President's principal foreign intelligence adviser appointed by him with the consent of the Senate to be the head of the Intelligence Community (IC) and

to discharge those authorities and responsibilities prescribed by law and by Presidential and National Security Council directives.

Dissemination Controls: markings that define the distribution limitation of a category of information. They are in addition to and separate from the levels of classification defined by E.O. 13526. Some require a control-specific warning notice at the beginning of any document conveying those data. Several are assigned solely by their proponent agency; outside organizations may not be authorized to make those determinations, but may only convey the caveat assigned by the proponent. See the CAPCO Markings Register/Manual (Appendix A, paragraph e).

Downgrading: a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

Employee: employee has the meaning provided in section 1.1(e) of Executive Order 12968; specifically: a person, other than the President and Vice President, employed by, detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

Foreign Government Information (FGI):

(1) Information provided to the USG by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) Information received and treated as "Foreign Government Information" under the terms of EO 13526 or a predecessor order.

For Official Use Only (FOUO): a dissemination control applied to unclassified information that may be withheld from public release requested through the Freedom of Information Act (FOIA).

Freedom of Information Act (FOIA): statute that provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent such records (or portions of them) are protected from public disclosure by one of nine exemptions.

Insider: any person with authorized access to any United States Government resource to include personnel, facilities, information, computer networks or systems.

Insider Threat: the threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through

espionage, terrorism, unauthorized disclosure of national security information, or through loss or degradation of departmental resources or capabilities. The term "insider threat" is used to refer to an individual or group; the term "vulnerability" is used when referring to a system or network.

Insider Threat Response Action(s): activities to ascertain whether certain matters or information indicate the presence of an insider threat, as well as activities to mitigate the threat. Such an inquiry or investigation can be conducted under the auspices of counterintelligence, security, law enforcement, inspector general, or other elements, depending on statutory authority and internal policies governing the conduct of such in each agency.

Key Information Sharing and Safeguarding Indicators: key performance indicators developed under Executive Order 13587 by the Senior Information Sharing and Safeguarding Steering Committee, to serve as the basis for addressing reporting requirements directed by the President, and to assist in tracking progress and identifying areas for attention or additional funding to continue and strengthen the sharing and safeguarding of classified information.

Mission Need: a determination by an authorized holder of information that access to specific information, in their possession, is required by another person to perform a specific and authorized function.

Original Classification Authority (OCA): an individual who has been authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

Redaction: the removal of classified information from copies of a document such that recovery of the information on the copy is not possible using any reasonably known technique or analysis.

Sanitization: the process of editing or otherwise altering intelligence information or reporting to protect sensitive intelligence sources and methods, capabilities, and analytical procedures in order to permit wider dissemination.

Senior Agency Official: "The official designated by the agency head under section 5.4(d) EO 13526 to direct and administer the agency's program under which information is classified, safeguarded, and declassified. (Note: the National Insider Threat Policy and Minimum Standards also require designation of an agency Senior Official responsible for implementation of the agency's insider threat program.)

Sensitive Compartmented Information (SCI): classified information concerning or derived from intelligence sources, methods, or analytical processes that requires handling within formal access control systems established by the Director of National Intelligence. Does not include NATO or Restricted Data information, as defined in Section II, Public Law 83-703 and the Atomic Energy Act of 1954, as amended.

Source Document: a classified document whose information is used as the basis for a new derivative classification decision.

Special Access Program (SAP): any program, which may or may not contain SCI, imposing need-to-know and access controls beyond those normally provided for access to Confidential, Secret and Top Secret information.

Subordinate Entity: an office, command, or similar organization, subordinate to the agency, which manages its own insider threat program.

Unauthorized Disclosure: communication or physical transfer of classified information to an unauthorized recipient.

U.S. National Interests: matters of vital interest to the United States to include national security, public safety, national economic security, the safe and reliable functioning of "critical infrastructure," and the availability of "key resources," as these terms are used in Homeland Security Presidential Directive (HSPD)-7, *Critical Infrastructure, Identification, Prioritization, and Protections*, 17 December 2003.

2.0 (U) USE OF THIS GUIDE

2.1 (U) General

(U) The *Insider Threat Classification Guide 1.0* provides authoritative classification guidance for U.S. Executive Branch insider threat activities based on Executive Order 13526, *Classified National Security Information*, Information Security Oversight Office (ISOO) Implementing Directive, Final Rule" (32 CFR Part 2001), the Atomic Energy Act of 1954 as amended, and Executive Order 13587. The *Guide* complements guidance contained in applicable classification guidance from U.S. Government agencies. Existing guidance concerning insider threat activities shall be updated to conform to the guidance contained herein. Users should consult with the appropriate agency Program Security Officer and/or Program Security Guide for additional guidance.

(U) This *Guide* sets forth minimum classification levels that can be exceeded, based on the sensitivity of the sources and methods associated with the information. In all cases, information shall be classified based on the sensitivity of its content and sensitivity of the circumstances of its acquisition.

2.2 (U) Authority to Cite this SCG

(U) The authority to cite the *Guide* is based upon EO 13526, 32 CFR Part 2001, and EO 13587 "Insider Threat." EO 13526 provides for two types of classification authority: original and derivative. This Guide is to be used as a baseline for derivative classification of U.S Insider Threat activities and related information.

(U) For U.S. insider threat activities undertaken in accordance with EO 13587, the OCA is the National Counterintelligence Executive (NCIX). The NCIX was designated an Original Classification Authority on 23 January 2013 by the DNI. This authority allows for original classification up to and including the Top Secret level.

(U) Portions of the *Guide* may be extracted or reproduced by U.S. Government agencies on a need to know basis. The public release of the *Guide* or any portion of the *Guide* is prohibited. Contact the IMD for additional guidance.

(U//~~FOUO~~) It is the intent of this *Guide* that inquiries and investigations into insider threat activities and concerns will be classified according to the citations contained in the *Guide.* It is recognized, however, that information will flow to agency insider threat program offices from various sources and offices, the preponderance of which may not be classified. It is not the intent of this *Guide* to classify information that enters an insider threat program office if that information is not normally classified by the originating office and does not become part of an insider threat inquiry, investigation, or analytic product. However, if that information is actually employed in an insider threat inquiry or investigation, or is employed in an insider threat analysis, it shall be classified according to this *Guide,* as part of an

insider threat investigative matter or analytic product. It is the connection of the information with an insider threat analytic product or with an insider threat inquiry or investigation that validly may require classification of the information, even though that same information, in its originating office, unconnected with an insider threat concern, may be unclassified. Note that this permits follow-up with the originator to be unclassified as long as the association with an insider threat inquiry is not revealed.

(U) If, as a result of an insider threat inquiry or investigation, an insider threat context is not concluded, then the matter and the association of the subject with the matter may be treated as unclassified or classified, according to existing agency guidelines.

(U) Agencies sharing their insider threat information with other agencies shall classify their information according to this *Guide* or according to their own internal classification guidance, if that guidance proscribes a level of classification equal to or higher than this *Guide.* Recipient agencies shall retain and honor the classification levels and dissemination control markings of the agency originating the information.

(U) If information under the auspices of 10 C.F.R. 1045, Nuclear Classification and Declassification, is commingled with insider threat information, Department of Energy/joint classification guides, and/or appropriate source documents must be used in addition to this *Guide* in order to properly classify Restricted Data (RD), Formerly Restricted Data (FRD), and Transclassified Foreign Nuclear Information (TFNI). RD, FRD and TFNI portions shall not be automatically declassified. Declassification justification for such information must be forwarded to the Director, Office of Classification, Department of Energy (DOE), for approval. Declassification of FRD is a joint decision between DOE and Department of Defense.

2.3 (U) Eligibility for Classification

(U) The Order mandates that information shall not be classified in order to:

- Conceal violations of the law, inefficiency, or administrative error;
- Prevent embarrassment to a person, organization, or agency;
- Restrain competition; or
- Prevent or delay the release of information that does not require protection in the interest of the national security.

(U) Section 1.4 of the Order also states that information shall not be considered for classification unless it concerns:

- 1.4(a) – Military plans, weapons systems, or operations;
- 1.4(b) – Foreign government information;
- 1.4(c) – Intelligence activities (including covert action), intelligence sources or methods, or cryptology;

- 1.4(d) – Foreign relations or foreign activities of the United States, including confidential sources;
- 1.4(e) – Scientific, technological, or economic matters relating to national security;
- 1.4(f) – United States Government programs for safeguarding nuclear materials or facilities;
- 1.4(g) – Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
- 1.4(h) – The development, production, or use of weapons of mass destruction.

2.4 (U) Classification Markings

(U) Classification and dissemination control markings are the usual means of communicating the need to protect national security information. These markings must be uniformly and conspicuously applied to all material regardless of media. Required markings include portion marking, a classification banner and a classification block. Banners, blocks, and portion markings are described in further detail in 32 CFR (Part 2001) and the CAPCO Register and Manual.

(U) The appropriate classification level is predetermined by the derivative citation that applies to the information. The Order states that information may be classified at one of the following three levels:

- "TOP SECRET" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **exceptionally grave** damage to the national security;
- "SECRET" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **serious damage** to the national security;
- "CONFIDENTIAL" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **damage** to the national security.

(U) Declassification. This *Guide* sets forth minimum classification durations for insider threat information. Agencies with approved declassification exemptions shall follow agency or program specific guidance, as appropriate. Information that clearly reveals a confidential human informant/source shall use the "50X1-HUM" declassification instruction pursuant to Section 1.5 of EO 13526. Derivative classifiers shall use the following classification block example when using this *Guide* as their authority to classify the information:

Classified By: Name/position or agency identifier
Derived From: U.S. Insider Threat SCG 2013
Declassify On: 20381231

2.5 (U) Compilation of Unclassified Information

(U) Data that individually are unclassified or classified at a lower level, may become classified or classified at a higher level when aggregated or compiled in a single document, if the compiled information reveals an additional association or relationship that meets the standards for classification under EO 13526, and is not otherwise revealed in the individual data items. When a classification determination is made based on compilation, clear instructions must appear with the compiled information as to the circumstances under which the individual portions constitute a classified compilation, and when they do not.

2.6 (U) Dissemination Control

(U) The President and the DNI have emphasized the need to ensure the timely and efficient flow of information to our closest allies. The *Guide* provides broad guidance on classification and dissemination controls and does not affect those multilateral and bilateral agreements between the U.S. Government and foreign entities concerning insider threat operations. Users should be familiar with requirements to properly secure U.S. information that supports multinational insider threat operations. Users should consult with the appropriate agency Program Security Officer, Foreign Disclosure Office, or specific program guides for additional classification and dissemination control guidance for releasing classified information to foreign entities.

(U) It is expected that some insider threat activities will remain U.S.-only and maintain NOFORN dissemination control. In cases where individual agency guides or guidance specify more restrictive foreign release decisions for given information, users should coordinate with the appropriate agency foreign disclosure authorities for guidance.

(U) The fact that information may be unclassified does not authorize the public release of that information. Prior to public release of unclassified information, the unclassified information must undergo a pre-publication review, following procedures established for such reviews within the individual agency. Also, until the implementation of Executive Order 13556, *Controlled Unclassified Information*, it is the responsibility of the individual agency to review unclassified information, prior to public release, to determine if the agency wishes to add any specific caveats to the unclassified information.

(U) A wide variety of additional markings is used to limit the dissemination of unclassified information. The use of such markings is governed by agency policy. The most widely used of these markings is For Official Use Only (FOUO). FOUO is generally used to indicate information that may fall within the following Freedom of Information Act exemptions:

- (b)(2) – Records that relate solely to the internal rules and practices of an agency;

- (b)(3) – Records that are protected by another law that specifically exempts the information from public release (for example, the sources and methods provision of the National Security Act or the CIA Information Act);
- (b)(4) – Trade secrets and commercial or financial information obtained from a private source which would cause substantial competitive harm to the source if disclosed;
- (b)(5) – Internal records that are pre-decisional and deliberative in nature, or exempt as attorney-client or attorney-work product privileged records;
- (b)(6) – Records which, if released, would result in a clearly unwarranted invasion of personal privacy;
- (b)(7) – Investigatory records compiled for law enforcement purposes;
- (b)(8) – Records used by agencies responsible for the regulation or supervision of financial institutions;
- (b)(9) – Records containing geological and geophysical information regarding wells.

2.7 (U) Foreign Government Information

(U) The unauthorized disclosure of foreign government information (FGI) is presumed to cause damage to U.S. national security. It thus requires that FGI shall retain its original classification markings or shall be assigned a U.S. classification providing a degree of protection at least equivalent to that required by the entity that furnished the information. Additional guidance may be found in 32 CFR Part 2001, and the CAPCO *Markings Register/Manual* available from the ODNI (ODNI/CIO/IMD).

2.8 (U) Responsibility for Maintaining this Guide

(U) The ODNI is responsible for maintaining the *Guide*. Change requests may be sent to the NCIX or the IMD using the *Change Request Form* provided in Appendix B. Requests will be reviewed within seven business days. Determinations will be made as soon possible, but no more than 90 days from the date of receipt. Additionally, change requests will be coordinated with the Insider Threat Task Force agencies for comment. Requestors will receive written notice of determination on each change request. If a request is denied the rationale for the denial will be included in the notification. All change requests will be coordinated with the IMD.

(U) Accepted requests will be incorporated into the next revision of the *Guide*. Revisions will be accomplished periodically and as circumstances require, but at least once every five years.

2.9(U) Contact Information

(U) Users are encouraged to contact ODNI/CIO/IMD for any questions concerning classification guidance, dissemination control, changes to classification or any other questions or concerns. Please use the following contacts to address any issues you may have:

Agency/Office	JWICS e-mail	Secure Phone	Unclassified Phone
NCIX/NITTF	NITTF-Assistance[redacted]	[redacted]	[redacted]
ODNI/CIO/IMD	DNI-Classification_[redacted]	[redacted]	[redacted]

(b)(3)

3.0 (U) CLASSIFICATION TABLES

3.0.1 (U) GENERAL GUIDANCE

(U) Users should review the classification tables for the subject area pertaining to their topic. Match the citation item to your situation. The level column provides the classification level of that item. The remaining items are self explanatory.

(U) The *Guide* uses three levels of detail to assist users in properly classifying information: **General** information, **Specific** information and **Detailed** information. The following definitions should be used to provide increased understanding of the use of these levels in the classification tables:

(U) **General Information**: Broad information describing a topic area with no specific information on that topic area. General information is usually UNCLASSIFIED or CONFIDENTIAL.

(U) **Specific Information**: In this context, specific information is that which reveals information beyond the general level but not providing detailed operational planning, strategic policy, or U.S. vulnerabilities that, if known to an adversary, would cause exceptionally grave damage to national security. Specific information is usually classified SECRET.

(U) **Detailed Information**: This usually provides detailed operational planning, strategic policy, or U.S. vulnerabilities that, if known to an adversary, would cause exceptionally grave damage to national security. Detailed information is usually classified TOP SECRET.

(U) Users are reminded that the *Guide* provides common terminology and common classification baselines that can be used among the various U.S. Government departments and agencies involved in insider threat activities. USG departments and agencies are encouraged to supplement the *Guide* with specialized classification guidance/instructions tailored to their particular programs or requirements. Nothing herein is intended to supersede or alter the existing procedures, guidelines, or authorities of the individual U.S. departments or agencies for their internal insider threat activities. In cases where there may be a conflict with existing guidance specific to an agency or department, users must follow whichever guidance is the most restrictive.

(U) Three footnotes (marked with one, two or three asterisks) applicable to many of the entries in the classification tables appear at the end of the tables.

3.1 (U) ADMINISTRATION

3.1.1 (U) POLICY AND SCOPE:

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
1. The fact that the United States has an abiding interest in detecting insider threat activity, protecting against such activity, and mitigating the effect of such activity.	U*				
2. The fact that the executive branch has established a national policy and minimum standards governing insider threat detection and prevention.	U*				
3. The content of the national insider threat policy and minimum standards.	U*				
4. The fact that agencies are required to establish insider threat detection and prevention policy and programs.	U*				
5. The content of agency insider threat policies and procedures, including agency guidelines and procedures for documenting each insider threat issue and response taken.	U*				
6. Agency guidelines and procedures for documenting insider threat issues and responses taken, when the content identifies sensitive sources and methods.	S	1.4(c) (g)		Current date plus 25 years	
7. General organizational structure of an agency insider threat program.	U*				Except for Intelligence Community organizations, which may be classified; refer to the appropriate agency classification guidance.
8. The fact that national insider threat policy and minimum standards apply to industrial contractors.	U*				
9. The fact that agencies are required to investigate and respond to suspected insider threat activity.	U*				Classify details according to content.
10. Vulnerability information concerning an agency whose core mission is a national security function, if exploitation of the vulnerability could potentially halt or disrupt execution of this function.	TS	1.4(c) (g)		Current date plus 25 years	See section 3.3 for additional discussion of vulnerabilities.

(Table is U//~~FOUO~~)

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
11. Details of countermeasures involved in protecting classified national security systems that could be exploited by an insider.	S	1.4(c) (g)		Current date plus 25 years	Information regarding the weaknesses or vulnerabilities of countermeasures should be classified according to section 3.3.
12. The contents of agency insider threat policies or programs that reveal information on sources and methods employed to detect insider threat activity.	S	1.4(c) (g)		Current date plus 25 years	
13. Information regarding the contents of executive branch and agency insider threat policies and programs which reveal the identity of any suspected insider threat perpetrator.	S**	1.4(c) (g)		Current date plus 25 years	
14. Information regarding the contents of executive branch or agency insider threat policies and programs that reveals whether an agency has, is, or intends to conduct an insider threat inquiry or investigation with respect to a specific individual or group of individuals.	S**	1.4(c) (g)		Current date plus 25 years	If, as a result of an insider threat inquiry or investigation, an insider threat context is not established, then the matter and the association of the subject with the matter may be treated as unclassified or classified, according to existing agency guidelines.
15. Non-specific information concerning executive branch, department, or agency insider threat requirements that reveals existing U.S. insider threat activities, or capabilities.	C	1.4(c) (g)		Current date plus 25 years	For example, the fact particular agencies are developing or seeking to upgrade technology to monitor classified systems. When the information does not identify an element of a U.S. government program or interest and does not reveal USG activities or capabilities, it may be treated as unclassified.
16. Specific information concerning executive branch, department, or agency insider threat requirements that reveals US insider threat activities or capabilities.	S	1.4(c) (g)		Current date plus 25 years	For example, the specific functional requirements of a system under development to monitor classified systems.
17. Specific information pertaining to the staffing levels of agency insider threat programs.	U*				Classification may vary based on individual agency or Community guidance.
18. The fact and content of legal authorities governing executive branch insider threat activities.	U*				

(Table is U//~~FOUO~~)

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
19. Any information regarding insider threat detection and prevention programs, which might give an adversary insight that could interfere with or impede the ability to authorize or conduct insider threat operations or activities.	C	1.4(c) (g)		Current date plus 25 years	
20. Specific impediments that impact an agency's ability to authorize or conduct insider threat activities.	S	1.4(c) (g)		Current date plus 25 years	This applies only when specific enough to assist an insider threat in escaping detection. General statements (e.g. "the Miranda Rule sometimes impedes criminal investigation") would be unclassified
21. Procedures to report suspected malicious insider activity.	U*				May be classified higher based on specific agency/program-level classification guidance.

(Table is U//~~FOUO~~)

3.1.2 (U) PLANNING

(Table is UNCLASSIFIED)

Item	Level	Reason	Dissemination***	Declass On	Remarks
1. The fact that agencies are required to develop implementation plans for insider threat programs.	U*				
2. General information or assessments regarding insider threat plans, intentions, capabilities, or activities of the U.S., agencies, U.S. allies, coalition partners or foreign adversaries.	C	1.4(c) (d)		Current date plus 25 years	May be classified higher depending on content and sensitivity.
3. Specific information or assessments regarding insider threat plans, intentions, capabilities, or activities of U.S. agencies, or details about U.S. insider threat planning activities.	S	1.4(c) (d)		Current date plus 25 years	Classification may vary based on individual agency or Community guidance.
4. Specific details of commercially-available insider threat detection hardware or software, when associated with a particular agency insider threat program's interest or employment or a classified network.	S	1.4(c) (g)		Current date plus 25 years	
5. The fact that agencies seek to identify and monitor employee activities and behaviors that may be indicative of insider threat concerns.	U*				
6. Specific agency criteria or processes used to identify triggers or indicators for monitoring employee behavior.	S	1.4(c) (g)		Current date plus 25 years	
7. The fact that a portion of an agency annual budget includes funding for insider threat detection and prevention.	U*				
8. Individual agency budget or financial information, directly tied to the National Intelligence Program (NIP).	S	1.4(c)	NOFORN	Current date plus 25 years	Budget information that is purely administrative in nature and does not reveal intelligence priorities may be UNCLASSIFIED depending on individual agency guidance.

(Table is UNCLASSIFIED)

(Table is UNCLASSIFIED)

Item	Level	Reason	Dissemination***	Declass On	Remarks
9. Information regarding insider threat fiscal matters inclusive of budget, staffing levels, expenditures, funding, and appropriations data, to include related guidance, procedures, agreements, or disbursement techniques, the release of which would provide the level of effort committed or insight into U.S. insider threat capabilities.	**U***				Unclassified unless specifically identified as classified in an agency classification guide that deals with fiscal and budgetary matters. NIP information is treated as SECRET.
10. The fact that the U.S. conducts insider threat dialogue and planning with foreign partners.	**U***				
11. The fact of broad, general insider threat cooperation with a country or group of countries with which the U.S. maintains formal military alliances or agreements (e.g., NATO).	**U***				In most cases, written agreements between the U.S. and other countries concerned will include provisions that govern classification levels. If there is a written agreement with a country that includes classification instructions, those instructions shall take precedence over this *Guide*.
12. Details of U.S. insider threat cooperation with a country or group of countries.	**S**	1.4(c) (d)		Current date plus 25 years	May be classified higher based on USG policy, CONOP or sensitivity. Consult appropriate classification guide.

(Table is UNCLASSIFIED)

3.2 (U) INSIDER THREAT METHODS AND EQUIPMENT

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
1. The general fact that agencies employ specialized tools to monitor individual user activities on classified computers.	U*				
2. Information on a commercially available off-the-shelf insider threat tool, equipment, technique, or method, not associated with agency or USG insider threat activity.	U*				
3. General information about insider threat detection tools, equipment, techniques, or methods that are not commercially available off-the-shelf.	C	1.4(c) (g)		Current date plus 25 years	
4. The fact that a specific commercially available, off-the-shelf insider threat detection tool, equipment, technique, or method is in use or being considered for use by the U.S. Government.	U*				Details may be classified higher.
5. Details about an insider threat tool, equipment, technique, or method which an agency or the USG is conducting research for eventual use in an insider threat program.	S	1.4(c) (g)		Current date plus 25 years	Example: Information about an agency's research to modify commercial hardware products for use in insider threat detection is a minimum of SECRET.
6. Technical details pertaining to insider threat detection hardware and software that is not commercially available.	S	1.4(c) (g)		Current date plus 25 years	May be TS in accordance with guidance from the agency that developed it, even when used by another agency as part of a program operating at the SECRET level.
7. Specific details of commercially-available insider threat detection hardware or software, when associated with a particular agency insider threat program, whether or not the hardware or software is actually employed by the agency.	S	1.4(c) (g)		Current date plus 25 years	

(Table is U//~~FOUO~~)

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
8. Details about an insider threat tool, equipment, technique, or method that is associated with an agency or USG insider threat activity.	**S**	1.4(c) (g)		Current date plus 25 years	Includes current and/or planned hardware/software on classified systems. Agency use of commercially available hardware or software is UNCLASSIFIED when not explicitly associated with insider threat or when operating on an unclassified network. Example: Indicating that the product is or will be employed on a specific classified network, as part of the agency's insider threat program, would be SECRET.
9. The fact that triggers or indicators are used to identify insider threat concerns or activities.	**U***				
10. The fact that monitoring tools employ triggers, indicators, or flags to highlight certain computer activities for additional scrutiny.	**U***				
11. The specific triggers, indicators, or flags that an agency employs to identify insider threat activity or that it employs in its user monitoring when the triggers are not associated with an insider threat program investigation or inquiry.	**U***				May be classified higher based on content. These would be decision rules that distinguished between behaviors calling for training/counseling and behaviors calling for an insider threat investigation. For example, at a specific agency, bringing a cell phone into a SCIF calls for counseling, but inserting a non-approved thumb drive into a classified computer, if combined with either irregular work hours or indications of financial difficulty, could trigger an insider threat investigation.
12. The specific triggers, indicators, or flags that an agency employs to identify insider threat activity or that it employs in its user monitoring when the triggers are associated with an insider threat program investigation or inquiry.	**S**	1.4(c) (e) (g)		Current date plus 25 years	Classify SECRET when specific trigger, indicators, or flags are tied to a person(s) who is the subject of an insider threat investigation or inquiry.

(Table is U//~~FOUO~~)

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
13. Methodology through which user activity monitoring (UAM) triggers, indicators, or flags are developed or adjusted.	**S**	1.4(c) (g)		Current date plus 25 years	
14. Technical specifications of an individual agency's capability to monitor the computer activity of individual users.	**S**	1.4(c) (e) (g)		Current date plus 25 years	
15. The fact that the U.S. Government uses behavioral science techniques to mitigate insider threat risks.	**U***				
16. The fact that an agency uses psychologists or behavioral scientists in its vetting of employees.	**U***				
17. General information pertaining to the actual or prospective behavioral science techniques that an agency may employ to mitigate insider threat risks, to include analysis and reports generated.	**C**	1.4(c) (g)		Current date plus 25 years	
18. Specific information pertaining to the behavioral science techniques, to include analysis and reports that an agency employs, or may employ, to mitigate insider threat risks.	**S**	1.4(c) (g)		Current date plus 25 years	
19. Behaviors indicative of possible insider threat activities.	**U***				
20. The fact that an agency may employ polygraph examinations for any purpose, including the detection of malicious insiders.	**U***				May be classified higher when this fact is compiled with other sensitive methods or techniques.
21. The results of individual polygraph examinations, which reveal insider threat anomalies, potential insider threats to classified national security information and information classified under the Atomic Energy Act of 1954.	**C****	1.4(c) (g)		Current date plus 25 years	Classify higher as content or agency policy dictates.
22. The fact that agencies have, or intend to develop, processes to automate its insider threat analysis center or hub.	**U***				Details of the processes will be classified according to content.

(Table is U//~~FOUO~~)

3.3 (U) VULNERABILITIES

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
1. General statements about widespread vulnerabilities in U.S. Government and National Security Systems without specific details.	U*				For example, a statement that since the Government uses ordinary commercial desktop software, even a disciplined patching program cannot guard against an authorized user (insider) launching a zero-day attack.
2. General statement about a specific agency's vulnerabilities.	U*				For example, a statement that the Department of Good Works was only able to manage its recent expansion by granting a very large number of interim security clearances.
3. Identification of a general vulnerability.	U*				For example statistics on the extent to which security re-investigations are behind schedule.
4. Identification of a specific vulnerability with enough detail to facilitate its exploitation by an insider.	S	1.4(c) (g)		Current date plus 25 years	For example, the schedule on which a conference room accredited for classified meetings is "swept" for hidden microphones.
5. Identification of a specific vulnerability, with enough detail to facilitate its exploitation by an insider, if that vulnerability could permit compromise of TS, SCI, or SAP information.	TS	1.4(c) (g)		Current date plus 25 years	For example, details of a specific vulnerability in an agency's file protection protocol and the methods to bypass the protocol enabling a user to potentially view files they otherwise would not have access to.

(Table is U//~~FOUO~~)

3.4 (U) AGENCY ACTIVITIES

3.4.1 (U) ANALYSIS AND ASSESSMENTS

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
1. The fact that agencies analyze information from various sources to detect insider threat concerns.	U*				
2. Analytic results that identify general or specific insider threat concerns.	S**	1.4(c)		Current date plus 25 years	
3. Analytic results that provide details pertaining to specific insider threat concerns involving information that is TS, SCI, or SAP.	TS	1.4(c)		Current date plus 25 years	
4. Analytic results that identify specific individuals that are or may be of concern to an agency from an insider threat perspective.	S**	1.4(c)		Current date plus 25 years	
5. Analytic results that identify specific vulnerabilities of an agency.	S	1.4(c)		Current date plus 25 years	Information regarding weaknesses or vulnerabilities should be classified according to section 3.3., and Agency or Community classification guidance.
6. Analytic results that reveal information about the insider threat posture across the executive branch or across the entire U.S. government.	S	1.4(c)		Current date plus 25 years	
7. Analytic results that portray the insider threat posture of an individual an agency.	S**	1.4(c)		Current date plus 25 years	
8. The fact that Key Information Sharing and Safeguarding Indicators (KISSI) are periodically submitted to agencies for response.	U*				This classification guidance pertains to KISSI and any successor information survey directed to individual agencies for response.
9. The fact that KISSI response information is analyzed for insider threat detection purposes.	U*				
10. Specific insider threat-related questions contained in the Key Information Sharing and Safeguarding Indicator (KISSI).	U*				

(Table is U//~~FOUO~~)

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
11. Analysis that is derived from KISSI data.	S	1.4(c) (g)		Current date plus 25 years	Classified a minimum of SECRET if KISSI analysis provides information regarding weaknesses or vulnerabilities.
12. The fact that agencies conduct insider threat self-assessments.	U*				

(Table is U//~~FOUO~~)

3.4.2 (U) LEVERAGING AND INTEGRATING INFORMATION FROM ACROSS AN AGENCY

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
1. The fact that the agency insider threat program will have access to employee information drawn from all offices within the agency.	U*				
2. The fact that an agency will review any and all types of information to assess insider threats.	U*				
3. The association of information pertaining to an individual employee with an insider threat analysis, inquiry, or investigation when national security information or systems appear to be at risk or foreign intelligence entity involvement is suspected.	S**	1.4(c) (g)		Current date plus 25 years	By its definition an insider threat concern involves a possible risk to national security information or systems or when foreign intelligence entity involvement is suspected.
4. The results of analysis by insider threat program personnel of information pertaining to individual employees when national security information or systems appear to be at risk or foreign intelligence entity involvement is suspected.	S**	1.4(c) (g)		Current date plus 25 years	By its definition an insider threat concern involves a possible risk to national security information or systems or when foreign intelligence entity involvement is suspected.
5. Content and details of service level agreements between agencies and their respective national security system service providers.	U*				
6. Procedures through which information, from whatever source, is integrated and analyzed within the insider threat program.	U*				Unless the information reveals a method of circumvention of the procedures that would result in a vulnerability. In that case the information should be classified SECRET.
7. Referrals to other agencies that identify insider threats or systems appear to be at risk or foreign intelligence entity involvement is suspected.	S**	1.4(c) (g)		Current date plus 25 years	As an example, referrals to the FBI under section 811 of the Intelligence Authorization Act of 1995. By its definition an insider threat concern involves a possible risk to national security information or systems or when foreign intelligence entity involvement is suspected.

(Table is U//~~FOUO~~)

3.4.3 (U) INSIDER THREAT INQUIRIES AND INVESTIGATIONS

(Table is U//~~FOUO~~)

Item	Level	Reason	Dissemination***	Declass On	Remarks
1. The identity of specific individual(s) as the subject of an insider threat investigation or inquiry.	S**	1.4(c) (g)		Current date plus 25 years	
2. Details of investigations or inquiries into activities that indicate a specific insider threat concern.	S**	1.4(c) (g)		Current date plus 25 years	See section 2.2 for additional guidance.
3. The investigative methods and techniques that an agency employs to conduct insider threat inquiries and investigations.	U*				Shall be classified according to the investigative policies and guidance of that agency. See section 2.2 for additional guidance.
4. The fact of external assistance to counter an insider threat or the fact that an investigative referral on an insider threat matter has been made to outside the agency, when the subject of the investigation or inquiry has not been divulged.	C**	1.4(c) (g)		Current date plus 25 years	By its definition, an insider threat concern involves a possible risk to national security information or systems or when foreign intelligence entity involvement is suspected. See section 2.2 for additional guidance.
5. The fact of external assistance to counter an insider threat or the fact that an investigative referral on an insider threat matter has been made to outside the agency, when the subject of the investigation or inquiry has been divulged.	S**	1.4(c) (g)		Current date plus 25 years	By its definition, an insider threat concern involves a possible risk to national security information or systems or when foreign intelligence entity involvement is suspected. See section 2.2 for additional guidance.
6. Results or findings of an insider threat investigation.	S**	1.4(c) (g)		Current date plus 25 years	

(Table is U//~~FOUO~~)

(Table is U//~~FOUO~~)

3.4.4 (U) USER ACTIVITY MONITORING (UAM)

Item	Level	Reason	Dissemination***	Declass On	Remarks
1. The fact that an agency conducts UAM.	U*				
2. The pre-analysis, raw results derived from UAM.	U*				Minimum For Official Use but classified according to content.
3. Analytic results derived from UAM conducted on classified systems.	S	1.4(c) (g)		Current date plus 25 years	
4. Information pertaining to triggers, indicators, flags, and methodologies employed by an agency in UAM.	S	1.4(c) (g)		Current date plus 25 years	This applies whether the UAM is conducted internally by an agency or provided for through a Service Level Agreement with another agency.
5. Metadata regarding UAM results that does not reveal triggers, indicators, flags or methodologies employed by an agency in UAM.	U*				
6. The fact that an agency may receive UAM services from one or more service providers.	U*				
7. General information about service level agreements that document UAM relationships between an agency and service provider(s).	U*				
8. The fact that agencies employ logon consent banners and require employees to acknowledge, in writing, that they are subject to UAM.	U*				

(Table is U//~~FOUO~~)

3.4.5 (U) EMPLOYEE AWARENESS TRAINING

(Table is Unclassified)

Item	Level	Reason	Dissemination***	Declass On	Remarks
1. General indicators of insider threat activity.	U*				
2. The fact that agencies are required to establish an internal network site through which to provide employees with insider threat awareness materials and through which to provide employees with procedures through which to report insider threat concerns.	U*				
3. The identity of employees that report insider threat concerns.	U*				This information generally should not be disclosed if the release of the information will result in an unwarranted harm to personal privacy of the employee who reported the concern such that the information may be withheld pursuant to Exemption 6 or 7(C) of the Freedom of Information Act.
4. The content of insider threat "frequently asked questions."	U*				Generally unclassified, classify based on content and sensitivity.

*(U) The fact that information may be unclassified does not authorize the public release of that information. Prior to public release, the unclassified information must undergo a pre-publication review, following established agency procedures. Also, until the implementation of Executive Order 13556, *Controlled Unclassified Information,* it is the responsibility of the individual agency to review unclassified information, for appropriate public release.

**(U) In the absence of agency guidance or other source documentation, information pertaining to an individual(s) that indicates a potential insider threat should be classified in accordance with this *Guide*. If analysis or inquiry substantiates this concern, the association of the individual with an insider threat matter will remain classified. If analysis or inquiry indicates that improper behavior may have taken place, but that no threat or nexus to national security exists, the matter should be declassified and addressed as a matter of suitability or law enforcement. If analysis or inquiry leads to a belief that the individual is not an insider threat, the matter should be safeguarded in accordance with agency policy.

***(U) Additional information pertaining to dissemination control markings may be found in section 2.6 of this *Guide*. Due to varying policies affecting the use of foreign disclosure and dissemination control markings employed across the USG, the determination and use of applying these restrictive markings, for insider threat information, is left to the responsibility of individual agencies. Users of this guide shall ensure appropriate coordination of information involving other agency equities is undertaken prior to dissemination.

(U) APPENDIX A: REFERENCE DOCUMENTS

*All entries are **UNCLASSIFIED**.*

(a) **32 CFR Part 2001,** "Classified National Security Information; Final Rule," Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA)

(b) **10 CFR Part 1045,** "Nuclear Classification and Declassification"

(c) **Atomic Energy Act of 1954**, as amended

(d) **Committee on National Security Systems,** CNSS Instruction No. 4009, "National Information Assurance (IA) Glossary"

(e) **Controlled Access Program Coordination Office (CAPCO)**, ODNI, "Intelligence Community Authorized Classification and Control Markings Register and Manual." This document appears online at several different classification levels. Since changes are made in the online versions without explicit notice to all users, only a current online version should be considered authoritative.

(f) **DoD 5105.21-M-1**, "Sensitive Compartmented Information Administrative Security Manual," August 1998

(g) **DoD Manual 5200.01 (Volumes 1 through 4) "DoD Information Security program," February 2012**

(h) **DoD 5220.22-M**, "National Industrial Security Program; Operating Manual (NISPOM)."

(i) **DoD Regulation 5400.7-R,** "DoD Freedom of Information Act Program," dated September 1998

(j) **Executive Order 12333**, "United States Intelligence Activities," December 8, 1981, as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)

(k) **Executive Order 12829**, "National Industrial Security Program," January 6, 1993

(l) **Executive Order 12968**, "Access to Classified Information." August 2, 1995

(m) **Executive Order 13526**, "Classified National Security Information," 29 December 2009

(n) **Executive Order 13549**, "Classified National Security Information Program for State, Local, Tribal and Private Sector Entities," August 18, 2010

(o) **Executive Order 13556**, "Controlled Unclassified Information," November 4, 2010

(p) **Executive Order 13587**, "Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011

(q) Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012

(r) **Information Security Oversight Office** booklet, "Marking Classified National Security Information," December 2012

(s) **Intelligence Community Directive (ICD) 403**, "Foreign Disclosure and Release of Classified National Intelligence"

(t) **Intelligence Community Directive (ICD) 710**, "Classification Management and Control Markings System"

(u) **Homeland Security Presidential Directive (HSPD)-7**, *Critical Infrastructure, Identification, Prioritization, and Protections*, 17 December 2003.

(U) APPENDIX B: CHANGE REQUEST FORM

CHANGE REQUEST
For the U.S. Insider Threat Classification Guide

To: National Insider Threat Task Force Program Manager
Date of Request: _____

From (Originator of request):

Name: _____

Organization: _____

Office: _____

Proposed Change:

☐ New item ☐ Modification ☐ Challenge

Item to be changed:	Change description
Page:	
Topic:	
Derivative Item:	

Rationale for Change:

This Section is to be completed by ONCIX Staff and coordinated with CIO/IMD as appropriate

Change Request Number: _____
Date of response: _____
Action Officer: _____

NCIX decision: Yes ☐ (approved) No ☐ (not approved)

If "No" justification for denial of change request:

THIS PAGE LEFT INTENTIONALLY BLANK

(U) APPENDIX C: ACRONYM LIST

*All entries are **UNCLASSIFIED***

CAPCO	Controlled Access Program Coordination Office
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CONOP	Concept of Operations
CUI	Controlled Unclassified Information
DNI	Director of National Intelligence
DoD	Department of Defense
DoE	Department of Energy
EO	Executive Order
FBI	Federal Bureau of Investigation
FGI	Foreign Government Information
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FRD	Formerly Restricted Data
HSPD	Homeland Security Policy Directive
IC	Intelligence Community
ICD	Intelligence Community Directive
IMD	Information Management Director (ODNI)
ISOO	Information Security Oversight Office
ITPO	Insider Threat Program Office
KISSI	Key Information Sharing and Safeguarding Indicators
NCIX	National Counterintelligence Executive; (Office of the; ONCIX)
NIP	National Intelligence Program
NISPOM	National Industrial Program Operating Manual
NITTF	National Insider Threat Task Force
NOFORN	Not Releasable to Foreign Nationals
NSI	National Security Information
OCA	Original Classification Authority
ODNI	Office of the Director of National Intelligence
RD	Restricted Data
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
UAM	User Activity Monitoring
USC	United States Code
USG	United States Government