FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1320183-1

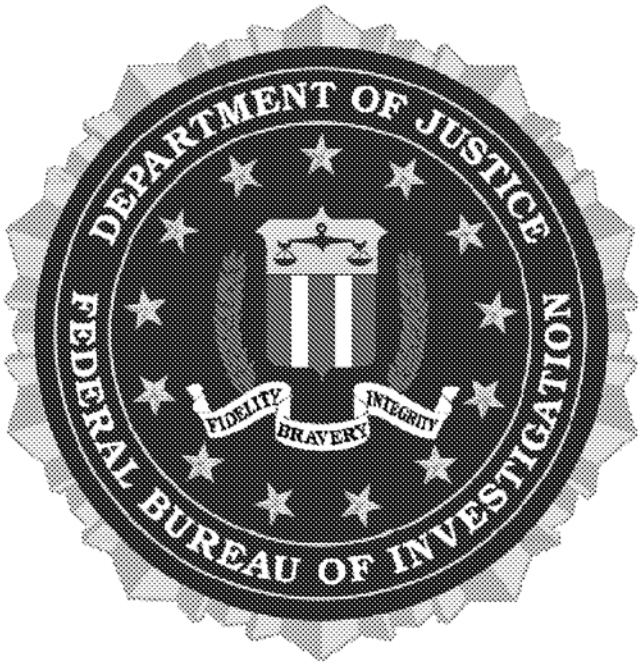
Total Deleted Page(s) = 9
Page 16 ~ b1; b3; b7E;
Page 17 ~ b1; b3; b7E;
Page 18 ~ b1; b3; b7E;
Page 19 ~ b1; b3; b7E;
Page 20 ~ b1; b3; b7E;
Page 21 ~ b1; b3; b7E;
Page 22 ~ b1; b3; b7E;
Page 23 ~ b1; b3; b7E;
Page 24 ~ b1; b3; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

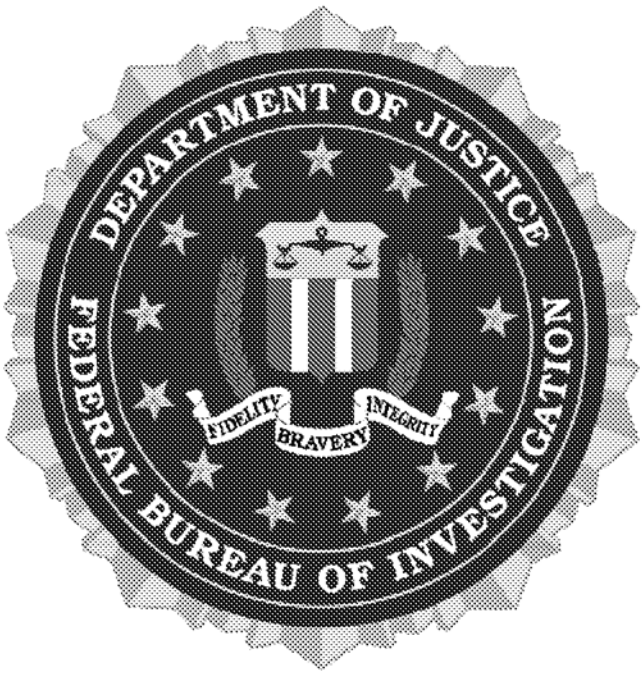
(U) FEDERAL BUREAU OF INVESTIGATION TECHNICAL SURVEILLANCE COUNTERMEASURES CLASSIFICATION GUIDE (TSCM CG)

(U) Science & Technology Branch

(U) December 1, 2011



CLASSIFIED BY: ~~EAD-STB, FBI~~
REASON: ~~1.4(c)(e)(g)~~
DECLASSIFY ON: ~~20361201~~



(U) FOREWORD

(U//~~FOUO~~) The Federal Bureau of Investigation (FBI) Technical Surveillance Countermeasures Classification Guide (TSCM CG) provides guidance concerning the classification and level of protection afforded to FBI-originated national security information. The TSCM CG is not intended to provide specific guidance concerning the handling, safeguarding, transport, declassification and downgrading, destruction, or administration of classified material, whether in paper or electronic form. Specific guidance concerning these topics is available in Executive Order (EO) 13526, "Classified National Security Information;" Department of Justice (DOJ) Security Program Operating Manual (SPOM); FBI Security Policy Manual (SPM); FBI Automatic Declassification Guide; FBI Foreign Dissemination Manual (FDM); Information Security Oversight Office (ISOO) Directive Number 1 (32 CFR Parts 2001 and 2003); and other documents referenced herein.

(U//~~FOUO~~) The duration of classification, classification markings, and other requirements of EO 13526, are to be applied to information classified pursuant to this guide, in accordance with the SPM and other approved FBI policies and procedures. I hereby approve the issuance of this classification guide and the classification determinations designated herein, as an authorized Original Classification Authority

(U//~~FOUO~~) The TSCM CG shall be considered the **only** authority on the subject matters it addresses for derivative classifiers within the FBI. This version, 1.0, is effective immediately, and supersedes the TSCM Classification Guidance, Dated 04/19/2002.

Louis E. Grever
Original Classification Authority
Executive Assistant Director
Science & Technology Branch

(U) TSCM CG 20111201

(U) Technical Surveillance Countermeasures Classification Guide

(U) December 01, 2011

(U) Federal Bureau of Investigation
(U) Science &Technology Branch
(U) Operational Technology Division
(U) Washington, D.C. 20535

THIS TABLE IS UNCLASSIFIED			
Date	Description	Editor	Version Number
09/17/2010	Initial draft		1.0
10/22/2010	Updated with NSB Classification SMEs' input		1.0
10/26/2010	Updated with corrected TSCM classifications		1.0
10/11/2011	Updated with changes from SecD		1.0
11/03/2011	Updated with changes from SecD		1.0
11/15/2011	Updated with changes from SecD and NSB		1.0

b6

Reviewed by:

Name	Signature / Date
AD Amy Hess	12/28/11
Acting DAD	12/15/11
Acting SC	12/15/11
UC	12/13/11
SSA	12/02/2011

(U) TECHNICAL SURVEILLANCE COUNTERMEASURES

(U) TABLE OF CONTENTS

1 (U) GENERAL

1.1 (U) PURPOSE

(U) The Technical Surveillance Countermeasures Classification Guide (TSCM CG), identifies specific topics of information associated with Technical Surveillance Countermeasures that meet the standards and criteria for classification and protection in accordance with Executive Order 13526, "Classified National Security Information," and its implementing directives. Specifically, this guide includes classification decisions regarding how to treat information and products produced by FBI employees and contractors in support of the Technical Surveillance Countermeasures program.

(S//NF)

b1
b3

(U)The TSCM CG also provides topics of information that do not meet the standards and criteria for classification under E.O. 13526, but are nonetheless sensitive and require protection against unauthorized disclosure. Such sensitive but unclassified information shall be categorized as "FOR OFFICIAL USE ONLY" (FOUO) or "LAW ENFORCEMENT SENSITIVE" (LES) per the FOUO and LES criteria listed in the Intelligence Policy Manual and will be marked as applicable to reflect that status.

1.2 (U) AUTHORITY

(U) This TSCM CG is approved by Louis E. Grever, Executive Assistant Director, Science & Technology Branch (STB), Federal Bureau of Investigation, a delegated Original Classification Authority (OCA) with the authority to classify information up to the TOP SECRET level. It is issued under the authority of E.O. 13526 and in accordance with Information Security Oversight Office (ISOO) Directive No. 1 (32 CFR, Parts 2001 and 2003), "Classified National Security Information; Final Rule"; and the Department of Justice Security Program Operating Manual.

(U) This Classification Guide constitutes EAD, STB original classification authority and may be cited as the basis for derivative classification of the information contained herein.

(U//~~FOUO~~) This TSCM CG supersedes the FBI Technical Surveillance Countermeasures (TSCM) Classification Guidance, dated April 19, 2002.

1.3 (U) SCOPE AND APPLICABILITY

(U) This document provides classification guidance for information associated with the FBI's Technical Surveillance Countermeasures program pursuant to E.O. 12333. The TSCM CG shall be cited as the basis for classification and sanitization of information and materials under FBI cognizance and control related to FBI TSCM programs. Classification will comply with the National TSCM Classification Standards identified in the Procedural Guides issued by the SPB. Changes in classification guidance required for operational necessity will be made in a timely fashion upon notification and concurrence of the approving authority and will be disseminated to original recipients of this guide. The provisions of this classification guide are applicable to all FBI employees, detailees, assignees, and contractors who, in the course of his or her responsibilities, collects or creates information by means of analysis and has the responsibility to determine whether the information is classified.

(U) This TSCM CG has been de-conflicted with the FBI's primary national security information classification guide, the "FBI National Security Information Security Classification (NSISC) Guide," Revision 1.1, dated June 15, 2009, and other FBI classification guides. Where any guides cover similar material, the classification decisions recorded in the guides have been verified as consistent. When this guide applies to the same information as the NSISC Guide, the correlating NSISC Guide citation number is shown in the Classification Matrix of this guide.

(U) In the case of a conflict between this TSCM CG and another FBI classification guide, the information involved shall be protected at the highest level required by any of the "conflicting" classification guides. Report any conflicts to both units listed as the Office of Primary Responsibility in Section 1.4 of this guide. Security Division's Strategy, Policy, and Information Security Unit will coordinate de-confliction of guides with the guides' respective original classification authorities.

(U//~~FOUO~~) The FBI's classification authority extends only to information originated by the FBI. Information produced and classified by another federal agency shall retain the classification and markings of the originating agency. In the event that the information is of a higher classification under FBI guidelines, the information shall be re-classified to provide the information the appropriate level of protection. The Challenge shall be conducted in accordance with the guidelines provided in Corporate Policy Directive 0305N.

(U) OFFICE OF PRIMARY RESPONSIBILITY

(U) The Office of Primary Responsibility for this TSCM CG is:

(U) Federal Bureau of Investigation
[redacted]
Quantico, VA 22135
Program Manager, TSCM [redacted]
[redacted] Unit Chief [redacted]

b6
b7E

(U) If the Office of Primary Responsibility cannot be reached, contact:

(U) Federal Bureau of Investigation
Strategy, Policy, and Information Security Unit
Mission Support Section, Security Division
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535
NSI Program Manager, SPISU 202-324-3000
SPISU Unit Chief 202-324-3000

2 (U) POLICY

2.1 (U) GENERAL

(C//NF [redacted]

b1
b3
b7E

(U) This TSCM CG is applicable to derivative classifiers (which includes all FBI employees, detailees, assignees, and contractors who, in the course of his or her responsibilities, collects or creates information by means of analysis and has the responsibility to determine whether information and/or products regarding Technical Surveillance Countermeasures information are classified). Derivative classification authorities shall use and cite this guide.

2.2 (U) REASON FOR CLASSIFICATION

(U) 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. 13526, and falling within one or more of the categories of information eligible for classification per Section 1.4 of E.O. 13526. The topics of information cited in this TSCM CG are classified pursuant to the reason(s) indicated in the "Reason" column of the classification matrix.

2.3 (U) CLASSIFICATION BY COMPILATION

(U) 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.

(U) 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. Careful consideration must be taken when determining the need for classification by compilation. When the determination is made that classification by compilation is necessary, the classifier must provide explicit instructions as to what elements of the compilation, when combined, constitute classified information and the precise association or relationship that warrants the classification. Information which is classified by compilation must be marked in accordance with the ISOO's *Marking Classified National Security Information* booklet, pages 29-30.

(U) Users of this TSCM CG should be aware of the possibility of classification by compilation when compiling unclassified information. If a compilation of otherwise unclassified information reveals information which requires protection as classified national security information according to the Classification Matrix of this TSCM CG, it must be marked in accordance with the ISOO's *Marking Classified National Security Information* booklet, pages 29-30.

(U) Likewise, the compilation of classified information will be classified, at a minimum, at the highest classification among 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. If a compilation of information classified at one level reveals information which requires protection at a higher classification level according to the Classification Matrix of this TSCM CG, it must be marked in accordance with the ISOO's *Marking Classified National Security Information* booklet, pages 29-30.

(U) Individuals who find instances of classification by compilation that are not covered in the Classification Matrix shall follow the guidance in Section 2.4 of this TSCM Guide.

2.4 (U) EXCEPTIONAL CIRCUMSTANCES

(U) Should a situation arise where a holder of information believes the information should be classified but it is not covered by this or any other classification guide; or a compilation of unclassified information should be classified but is not covered in a classification guide; or a compilation of classified information should be classified at a higher level than any of the individual information items but is not covered in a classification guide, the information will be handled and safeguarded in accordance with the highest level of classification the holder believes appropriate. In such instances, the information will be marked with the tentative level of classification and the notation *"Pending Classification Review."*

(U) The information will be transmitted, by a means approved for the level of classification, to [redacted] TSCM Program Manager, TOS, OTD, STB, as identified in Section 1.3 of this TSCM CG, to coordinate a classification determination with the appropriate original classification authority. If the information is commonly occurring information and is found to not be covered in this or any other FBI classification guide, the appropriate original classification authority will add the information to an appropriate classification guide. b7E

2.5 (U) CHALLENGES TO CLASSIFICATION

(U) If at any time classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this TSCM CG until such time as a formal decision by an appropriate authority is made (an appropriate authority is an OCA with jurisdiction over the information in question). Classification challenges should be addressed to SPISU (formerly SPCAU), MSS, SecD, as provided in FBI Corporate Policy Notice on Classification Challenges (CPN-0305N).

2.6 (U) USE OF THIS GUIDE

(U) This TSCM CG is for the use of FBI personnel, contractors, assignees, and detailees performing derivative classification actions when addressing the elements of information covered by this TSCM CG.

(U) For the purpose of marking documents containing classified information covered by this TSCM CG, derivative classifiers will cite "FBI TSCM CG" at a minimum (including the date of this guide) on the "Derived From" line, and the declassification instruction as specified in this guide. For Example:

> *(U) Classified by: J12J34T56*
> [This should be your Unique Employee Identification Number]
> *(U) Derived From:* FBI TSCM CG, 20111201
> *(U) Declassify On: (Insert declassification instruction as cited for the particular type of information in the TSCM CG)*

(U) If classified information covered by this TSCM CG, as well as classified information from other classified sources, is included in the same document, the document will be marked as follows:

> *(U) Classified by: J12J34T56*
> *(U) Derived From: Multiple Sources*
> *(U) Declassify On: (Carry forward the single most restrictive declassification instruction from all source documents)*

(U) NOTE: If "Multiple Sources" are used for a derivatively classified document, a record of the sources used for classification will be maintained (at a minimum) with the file or record copy of the document. It is good practice to include the source listing either at the beginning of the document, near the classification authority block (the "Derived from/Declassify on" block), or at the end of the document with the words "Derived from:" and then a comprehensive list of only the sources from which the classifications were determined.

3 (U) MARKING

(U) All documents containing classified national security information will bear all required Intelligence Community classification markings, which include portion markings and a banner line on every page and the classification authority block described in Section 2.6 on the first page or front of the media.

(U) Detailed instructions for marking classified materials can be found in the ISOO booklet titled "Marking Classified National Security Information" dated December 2010. A link to this booklet (on the Secret Enclave) can be found in the "References" section of this TSCM CG. The booklet is also available on the unclassified network at: http://www.archives.gov/isoo.html.

> (U) NOTE: OADR, X1 through X8 and MR are commonly seen obsolete markings. If these markings appear on a source document, follow the instructions in the ISOO booklet (Marking Classified National Security Information December 2010) when marking a new document with information derived from the source document.

(U) Further marking guidance can be found on the SecD's web page located on the FBI's Secret Enclave.

3.1 (U) DISSEMINATION CONTROLS

(U) This TSCM CG indicates OCA decisions on the **reason** for classification (as detailed in E.O.13526, Section 1.4, a-h), **damage potential** of the information (which is the classification level – Unclassified, Confidential, Secret, or Top Secret) and **duration** of classification.

(U) Per ICD 710, Section G, requires all members of the Intelligence Community, including the FBI, to include one of the following foreign dissemination markings in all marking of classified documents and classified portions of documents:

> (U) NOFORN (NF) *Meaning:* Permission of the DIDO (Designated Intelligence Disclosure Officer) of the **originating organization** is required to release the information in any form to foreign governments, foreign nationals, foreign organizations, or non-US citizens.
>
> (U) REL TO USA, [Country List] (Where Country Listed is an ISO 3166 trigraph for a country or a tetragraph from the IC tetragraph table.) *Meaning:* **Any** recipient from **any** agency may release it to the country(ies) listed, but permission of the DIDO from the **originating organization** is required for release to other foreign governments, foreign nationals, foreign organizations, or non-US citizens.
>
> (U) RELIDO *Meaning:* **Any** DIDO from **any** agency may release the information to foreign governments, foreign nationals, foreign organizations, or non-US citizens **without** the permission of the originating agency.
>
> (U) REL TO USA, [Country List]/RELIDO *Meaning:* **Any** recipient from **any** agency may release it to the country(ies) listed and **any** DIDO from **any** agency may release the information to additional foreign governments, foreign nationals, foreign organizations, or non-US citizens **without** the permission of the originating agency without consulting with the originating agency.

(U) Note that the foreign dissemination markings used in this guide are advisory, and may be modified for any particular document or information item by the cognizant FBI foreign dissemination authority. There are two types of FBI foreign dissemination authorities: DIDOs and Focal Point Officers (FPOs). DIDO authorities can authorize the dissemination of FBI information to any foreign government. A FPO is an action officer who is authorized to disseminate specific classified information to specific foreign governments as determined in writing by the EAD-NSB, i.e. FVEYS (the tetragraph FVEY means “Australia, Canada, Great Britain, New Zealand, and the United States.”), Counterterrorism IIRS only, specific pending case information, information originating from specific Area of Responsibilities, etc. For a full listing of current FBI foreign dissemination authorities and related foreign disclosure policy guidance, see the FBI’s Foreign Disclosure website [redacted] b7E

(U) As stated in Corporate Policy Directive 0062D and the FBI Foreign Dissemination Manual (FDM), FBI employees shall not disseminate classified information to foreign governments, unless an FBI DIDO/FPO has documented

his/her approval as part of his/her official duty. Documents containing multiple portions with different foreign dissemination markings shall be marked overall (in the banner line) with the most protective marking, per guidance in the Intelligence Community Classification and Control Markings Implementation Manual.

(U) Common dissemination controls, as well as the procedures for applying them, are covered in the Intelligence Community Classification and Control Markings Implementation Manual:

(U) PROPRIETARY INFORMATION (PROPIN)

(U) ORIGINATOR CONTROLLED (ORCON) (Users should follow procedures outlined in the 2011 EC regarding proper use of ORCON when applying this marking to FBI information.)

(U) Other dissemination and control markings do exist and guidance on their use can be found in the Intelligence Community Classification and Control Markings Implementation Manual. Such a designation may be removed by the official who made the original designation, by the successor in function to such an official, by an official in the chain of supervision of the official who made the original decision, or his/her successor in function.

4 (U) DECLASSIFICATION

(U) Classified information may only be declassified by an original classification authority or declassification authority with jurisdiction over the information or by a declassification authority. To obtain declassification of information which has been classified according to this classification guide, consult the Office of Primary Responsibility listed in Section 1.3 of this Classification Guide. The Office of Primary Responsibility will coordinate declassification with the OCA with jurisdiction over the information contained herein (EAD, STB).

5 (U) CLASSIFIED HANDLING AND PROCESSING

(U) Classified information shall be handled and safeguarded in accordance with E.O. 13526, its implementing directives, the Department of Justice Security Program Operating Manual, and FBI Security Policy. Classified information will not be processed on any automated IT equipment unless the equipment has been specifically accredited and approved for the applicable level of classified processing. Consult division/field office security officials for instructions on local handling and processing procedures.

(U) Any questions about sharing TSCM information with US or foreign partners should be directed to the Office of Primary Responsibility, listed in Section 1.3 of this Classification Guide. Such guidance must be provided consistent with the FDM.

6 (U) REPRODUCTION AND DISSEMINATION

(U) This TSCM CG may be reproduced and disseminated within the FBI as needed. However, to ensure receipt of updates, revisions, and classification changes, whenever the guide is disseminated beyond an initial addressee, the Office of Primary Responsibility identified in Section 1.3 of this Classification Guide must be notified.

(U) Coordinate dissemination to government agencies outside of the FBI through the Office of Primary Responsibility identified in Section 1.3 of this Classification Guide. When disseminating to other government agencies, ensure the information disseminated contains instructions on how that government agency must handle and protect the information, including instructions on further dissemination. Guidance on format of information to be released may be obtained from the TSCM Program Manager or the [redacted] Unit Chief. b7E

7 (U) RELEASE OF INFORMATION

7.1 (U) PUBLIC RELEASE

(U) The fact that this TSCM CG indicates that some information may be unclassified does not imply that the information is automatically releasable to the public. Requests for public release of information will be addressed in accordance with Federal statutes, rules, and regulations which provide for access to this material.

(U) Portions of this TSCM CG are designated "FOR OFFICIAL USE ONLY" and will not be released to the public. Requests for copies of this guide by non-government officials will be addressed in accordance with the Freedom of Information Act (FOIA). The procedures for filing FOIA and Privacy Act requests with the FBI can be found on the unclassified network at http://foia.fbi.gov.

8 (U) EFFECTIVE DATE AND IMPLEMENTATION

(U) This Classification Guide is effective immediately upon OCA approval and publication.

(U) TECHNICAL SURVEILLANCE COUNTERMEASURES CLASSIFICATION GUIDE

(U) APPENDIX A : CLASSIFICATION MATRIX

(U) November 18, 2011

(U) APPENDIX B: DEFINITIONS

(U) *Classification* means the act or process by which information is determined to be classified information, and the determination of whether the information is Confidential, Secret, or Top Secret pursuant to E.O 13526.

(U) *Classification guidance* means any instruction or source that prescribes the classification of specific information.

(U) *Classification guide* means 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.

(U) *Classified national security information* or *classified information* means information that has been determined pursuant to Executive Order 13526, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

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

> (U) Sec. 1.3 of Executive Order 13526 states that information may be classified at one of the following three levels (damage potential):
>
> (U) *Top Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
>
> (U) *Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
>
> (U) *Confidential* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(U) *Declassification* means the authorized change in the status of information from classified information to unclassified information.

(U) *Derivative classification* means 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 classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(U) *Document* means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(U) *For Official Use Only* is a caveat which can be used with unclassified FBI information if the information meets one of the eight FBI criteria for using FOUO:

(a) (U) internal personnel rules and practices

(b) (U) information specifically exempted from disclosure by a statute

(c) (U) trade secrets or other commercial or financial information obtained from a person under circumstances that make it privileged or confidential

(d) (U) privileged interagency or intra-agency memoranda or letters

(e) (U) personnel and medical files and similar files whose disclosure would constitute a clearly unwarranted invasion of personal privacy

(f) (U) information contained in or related to examination, operating, or condition reports, prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions

(g) (U) reports that disclose security vulnerabilities not related to national security

(h) (U) geological and geophysical information and data, including maps concerning wells

(U) *Information* means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which 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.

(U) *Multiple sources* mean two or more source documents, classification guides, or a combination of both.

(U) *National security* means the national defense or foreign relations of the United States, including measures to counter international terrorism.

(U) *Original classification* means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

(U) *Original classification authority* means an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance.

(U) *Sensitive Compartmented Information (SCI)* means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

(U) *Source document* means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(U) *Technical Surveillance Countermeasures (TSCM)* is typically referred to as a sweep or inspection process. TSCM consists of complex technical examinations of areas requiring protection from hostile technical surveillance operations. The main objective is to protect FBI spaces worldwide from clandestine penetrations, and ensure the integrity of FBI controlled spaces in connection with National Security matters. TSCM inspections are classified procedures executed under strict operational and administrative guidelines.

(U) APPENDIX C: REFERENCES

(U) 32 CFR Parts 2001 and 2003 The Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA), published this Directive as a final rule and pursuant to Executive Order 13526, relating to classified national security information. The Executive Order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. It also establishes a monitoring system to enhance its effectiveness. This Directive sets forth guidance to agencies on original and derivative classification, downgrading, declassification, and safeguarding of classified national security information.

(U) Executive Order 13526: Classified National Security Information, prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.

(U) ISOO Marking Booklet – Marking Classified National Security Information, December 2010, Executive Order 13526, and ISOO Implementing Directive No. 1 prescribe a uniform security classification system. This system requires that standard markings be applied to classified information. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of classified information created after September 22, 2003, shall not deviate from the prescribed formats. Markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification. Since a booklet of this size cannot illustrate every conceivable situation, please refer to ISOO Implementing Directive No. 1 and FBI-specific marking policy. Consult your security manager if you have any questions. (Note: As of publication of this guide, the Marking Booklet had not been updated to reflect the changes required by EO13526.)

(U) Intelligence Community Classification and Control Markings Implementation Manual The Implementation Manual is a companion document developed to provide amplifying and explanatory guidance on the syntax and use of the markings contained in the CAPCO Register. While not the policy basis for individual agencies' use of any particular marking, the Implementation Manual cites the applicable authority and sponsor for each marking. Some of the Dissemination Controls and Non-Intelligence Community Dissemination Control Markings are restricted to use by certain agencies. They are included to provide guidance on handling documents that bear them. Their inclusion in the Manual does not authorize other Agencies to use these markings. Non-US Classification and Joint Classification Markings are restricted to the respective countries or international organizations.

(U) Department of Justice Security Program Operating Manual This manual prescribes requirements and procedures for the classification, safeguarding and declassification of classified National Security Information (NSI) within the Department of Justice (DOJ). The manual also prescribes requirements and safeguards necessary for Sensitive Compartmented Information (SCI) and other Special Access Programs (SAPs).

(U) FBI Security Policy Manual Establishes a consolidated manual containing security policy for the protection of FBI people, information, operations, equipment, and facilities. This manual is broad in scope providing security policies and procedures for the protection, use, and dissemination of classified information and material, including sensitive compartmented information (SCI); personnel security; physical and technical security requirements; transmission requirements; industrial and acquisition security; force protection; security compliance; information assurance and systems security; and communication security.

(U) FBI Original Classification Authority Listing Lists all current FBI Original Classification Authorities, as appointed by the Attorney General, Department of Justice.

(U) FBI Intelligence Policy Manual The intelligence policy of the FBI is based on statutes, Executive Orders and Presidential Directives, Attorney General Guidelines and Department of Justice Orders, Director of Central Intelligence Directives, and the March 4, 2003 Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing. The policies in this Manual apply to the dissemination of intelligence **products,** as distinct from both raw data and information disseminated in other forms, such as operational leads, threat warnings, and law enforcement leads.

(U) FBI Foreign Dissemination Manual This manual establishes FBI policy regarding the sharing of classified information with foreign governments and supersedes existing FBI policy regarding the sharing of classified information with such governments. It is FBI policy to share classified information with foreign governments only when doing so advances an identifiable U.S. national interest.

(U) FBI Foreign Dissemination Web Page This links to the National Security Branch's foreign dissemination web page.

(U) FBI National Security Information Security Classification Guide This classification guide (hereinafter NSISC Guide) identifies categories of information that are frequently obtained in the course of national security investigations and intelligence analysis and provides guidance on whether information in these

categories should be designated UNCLASSIFIED (U), CONFIDENTIAL (C), SECRET (S), or TOP SECRET (TS). It also provides guidance regarding the declassification instructions for such information and the markings to indicate foreign releasability.

(U) FBI Security Division Information Security Team – National Security Information web page This link provides a central location for most resources which may be required when making classification and marking decisions.

(U) Intelligence Community Directive (ICD) 710 This Directive establishes the Intelligence Community (IC) classification and control markings system as a critical element of IC procedures for protecting intelligence and information (hereinafter referred to as "information"), and sources and methods while ensuring that information is available without delay or unnecessary restrictions . The classification and control markings system enables information sharing and includes all markings added to classified and unclassified information to communicate one or more of the following: classification, compartmentation, dissemination controls, disclosure or release authorizations, and other warnings.