INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

August 31, 2007

INSPECTOR GENERAL INSTRUCTION 5200.1

INFORMATION SECURITY PROGRAM

FOREWORD

This Instruction prescribes policy and assigns responsibility to facilitate the effective and uniform application of the Department of Defense Information Security Program within the Department of Defense Office of Inspector General. The Instruction supplements Department of Defense 5200.1-R, *Information Security Program*, January 1997.

The office of primary responsibility for this Instruction is the Office of Security. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

Stephen D. Wilson
Assistant Inspector General for
Administration and Management

26 Appendices

TABLE OF CONTENTS

Paragraph **Page**

CHAPTER 1. GENERAL

CHAPTER 2. CLASSIFICATION MANAGEMENT SECTION 1 - CLASSIFICATION AND ORIGINAL CLASSIFICATION AUTHORITY

CHAPTER 2 SECTION 2 - MARKINGS

CHAPTER 2
SECTION 3 - CLASSIFICATION PROHIBITIONS AND LIMITATIONS

CHAPTER 2
SECTION 4 - CLASSIFICATION GUIDES

CHAPTER 2
SECTION 5 - DECLASSIFICATION AND DOWNGRADING

CHAPTER 3. SAFEGUARDING
SECTION 1 - SAFEKEEPING AND STORAGE

CHAPTER 3
SECTION 2 - CUSTODIAL PRECAUTIONS

CHAPTER 4. CLASSIFIED DOCUMENT CONTROL
SECTION 1 – ACCESS

CHAPTER 4
SECTION 2 - DISSEMINATION

CHAPTER 4
SECTION 3 - ACCOUNTABILITY AND CONTROL

CHAPTER 4
SECTION 4 - REPRODUCTION

CHAPTER 5. TRANSMISSION
SECTION 1 - METHODS OF TRANSMISSION OR TRANSPORTATION

CHAPTER 5
SECTION 2 - PREPARATION OF MATERIAL FOR TRANSMISSION, SHIPMENT OR CONVEYANCE

CHAPTER 5
SECTION 3 - RESTRICTIONS, PROCEDURES, AND AUTHORIZATION CONCERNING ESCORT OR HAND CARRYING OF CLASSIFIED INFORMATION

CHAPTER 6. DISPOSAL AND DESTRUCTION

CHAPTER 7. SECURITY EDUCATION

CHAPTER 8. COMPROMISE OF CLASSIFIED INFORMATION

CHAPTER 9. PROTECTING UNCLASSIFIED INFORMATION

CHAPTER 10. INFORMATION SYSTEMS

CHAPTER 11. NORTH ATLANTIC TREATY ORGANIZATION CLASSIFIED INFORMATION

CHAPTER 12. PROGRAM MANAGEMENT

CHAPTER 13. BUILDING ENTRANCE POLICY/BADGES/ PROPERTY PASSES/ESCORTING

APPENDICES

CHAPTER 1
GENERAL

A. Purpose. This Instruction prescribes policy and assigns responsibility to facilitate the effective and uniform application of the Department of Defense (DoD) Information Security Program within the DoD Office of Inspector General (OIG). The Instruction supplements DoD 5200.1-R, *Information Security Program*, January 1997.

B. References. See Appendix A.

C. Cancellation. This Instruction supersedes IGDM 5200.1, *Information Security Program Manual*, June 3, 2003.

D. Applicability. This Instruction applies to the Office of Inspector General, the Deputy Inspectors General, the Assistant Inspectors General who report to the Inspector General, the General Counsel, and the Director, Equal Employment Opportunity, hereafter referred to collectively as the OIG Components; and all field offices.

E. Definitions. See Appendix B.

F. Acronyms. See Appendix C.

G. Authority. This Instruction is published in accordance with (IAW) references (a) and (b), and DoD Administrative Instruction No. 26, *Information Security Supplement to DoD 5200.1-R*, April 1, 1987.

H. Policy

1. Each individual who possesses or who has knowledge of such information regardless of how it was obtained shall protect classified information.

2. Compliance with the provisions of this Instruction is mandatory. Violators are subject to administrative or judicial sanctions, or both.

3. Additional policy regarding information security is prescribed throughout pertinent chapters of this Instruction.

I. Responsibilities. All OIG managers are responsible for the effective application of information security policies and procedures within their organization. They shall ensure that individuals who have access to classified information are appropriately cleared, are aware of their security responsibilities, and are indoctrinated and proficient in the security policy and procedures that apply to them in the performance of their duties. Additional responsibilities for security managers and individuals are listed elsewhere in this Instruction.

J. Procedures. Procedures for implementing security guidelines are provided in reference (b) and this Instruction.

K. Executive Order Overview. Reference (a) prescribes a uniform system for managing the protection of national security information. Highlights of the Executive Order (E.O.) are:

1. Discourages unnecessary classification by instructing classifiers to keep information unclassified when in doubt and directs classifiers to choose the lower level of classification when in doubt about which level is appropriate.

2. Limits the duration of classification of most newly classified information to 10 years, subject to limited exceptions.

3. Mandates automatic declassification of information that is 25 years old, unless it falls within one of the narrow exemption categories, such as revealing the identity of a human source.

4. Establishes an Interagency Security Classification Appeals Panel (ISCAP) to hear appeals of agency decisions on mandatory declassification review requests or challenges to classification and to review an agency head's determination to exempt 25-year-old information from automatic declassification.

5. Authorizes agency officials to determine whether the public interest in disclosure outweighs the national security interest in maintaining classification when deciding whether to declassify information that otherwise continues to meet the standards for classification.

6. Implements a number of management improvements to better safeguard classified information and reduce the overall costs of protecting such information.

7. Stresses a general commitment to openness as a part of the classification management process.

8. Requires classifiers to identify why information is classified.

9. Eliminates the presumption that any category of information is automatically classified.

10. Specifies sanctions for over-classification.

11. Requires the establishment of a Government-wide declassification database.

12. Establishes an Information Security Policy Advisory Council of non-Government experts to recommend subject areas for systematic declassification review and to advise on classification system policies.

13. Limits the establishment and requires annual revalidation of Special Access Programs (SAPs) and increases both internal and external oversight of these programs.

14. Requires accounting and reporting of costs associated with security classification program.

15. Mandates training and accountability of Original Classification Authorities (OCAs).

16. Calls for challenges of improper classification decisions and establishes processing procedures to ensure non-retribution.

17. Requires personal commitment of Component Heads and senior management to the effective implementation of the system.

18. Requires that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of:

a. OCAs.

b. Security managers or security specialists.

c. All other personnel whose duties significantly involve the creation or handling of classified information.

L. <u>Delegation of Authority</u>. The Assistant Inspector General for Administration and Management (AIG-A&M) has delegated to the Chief, Office of Security, the responsibility for implementation and compliance with DoD regulations and for the establishment and administration of the Information Security Program. The Office of Security shall apprise the AIG-A&M of the security posture of the OIG and the status of ongoing investigations into security infractions and violations.

CHAPTER 2
CLASSIFICATION MANAGEMENT
SECTION 1 - CLASSIFICATION AND ORIGINAL CLASSIFICATION AUTHORITY

A. Background. Reference (a) prescribes a uniform system for classifying, safeguarding, and declassifying national security information assigned to keep the American people informed on the activities of Government. The E.O. also protects information critical to our nation's security. Implementing guidance on the provisions of reference (a) is contained in the Information Security Oversight Office (ISOO) directives. Reference (b) implements reference (a).

B. Authority. Each delegation of original classification authority shall be in writing and shall specify the title of the position held by the recipient. Under the authority delegated in reference (a), the Inspector General (IG) may exercise and delegate to the person designated to act in his or her absence the authority to originally classify national security information as Top Secret, Secret, and Confidential. The IG has designated the AIG-A&M as the Senior Official for Information Security. Each delegation of original classification authority shall be recorded and such authority shall not be redelegated.

C. Delegated Responsibility. The IG has been delegated Top Secret Original Classification Authority for this agency. Requests for additional delegation of original Top Secret classification authority, with appropriate justification, shall be submitted through proper channels for approval by the Secretary of Defense. Similarly, requests for additional original Secret and Confidential classification authority shall be submitted to the Office of the Assistant Secretary of Defense (Networks and Information Integration) (OASD (NII)) for approval.

D. Senior Official for Information Security. The AIG-A&M is responsible for actively overseeing the OIG information security program, including a security education program, to ensure effective implementation of reference (a). These responsibilities include establishing and monitoring policies and procedures to prevent over or under-classification of national security information and protecting classified information from unauthorized disclosure. The senior official for information security shall recommend the following to the IG:

1. Proposals for reclassification IAW reference (a).

2. Implementation plans that protect classified information and prevent unauthorized disclosure.

3. Guidance concerning corrective or disciplinary action in unusually important cases involving unauthorized disclosure.

4. Reporting to the ISOO information and reports required under reference (a).

5. Systematic document review for early downgrading, declassification, and public availability.

6. Reduction of the amount of classified material and the number of persons authorized to classify.

7. Establishment and implementation of a system for processing, tracking, and recording formal classification challenges made by authorized holders.

8. Guidance on agency development and implementation of an automatic declassification plan.

9. Training for all original and derivative classification authorities in classification, as provided in reference (a) and its implementing directives.

E. Classification Categories

1. To qualify for classification, information shall meet two tests. First, it must fall under one of the specified classification criteria listed below. (See reference (a)). Second, an official with original classification authority shall determine whether the unauthorized disclosure of the information, either by itself or in the context of other information, could reasonably be expected to cause damage to the national security.

2. Information may not be considered for classification unless it concerns: (Extracts from reference (a)).

a. Sec 1.4 a., Military plans, weapons systems or operations;

b. Sec 1.4 b., Foreign government information;

c. Sec 1.4 c., Intelligence activities, sources, methods, or cryptology;

d. Sec 1.4 d., Foreign relations or foreign activities of the United States (U.S.), including confidential sources;

e. Sec 1.4 e., Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

f. Sec 1.4 f., U.S. programs for safeguarding nuclear materials or facilities;

g. Sec 1.4 g., Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security, includes defense against transnational terrorism; or

h. Sec 1.4 h., Weapons of mass destruction.

F. Classification Levels. Information may be classified at one of the following three levels:

1. 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.

2. 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.

3. 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.

4. Except as otherwise provided by statute, no other terms shall be used to identify U.S. classified information.

G. Classification Standards. Information may be originally classified under the terms of reference (a) only if all of the following conditions are met:

1. An original classification authority is classifying the information.

2. The information is owned by, produced by or for, or is under the control of the U.S. Government.

3. The information falls within one or more of the categories of information listed in reference (a).

4. The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

5. If there is significant doubt about the need to classify information, it shall not be classified. Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

H. Responsibilities of Classifiers. Classifiers are responsible for proper classification and protection of documents that they create. Information is classified in one of two ways, originally and derivatively. Only OCA may formally make original classification determinations. Individuals with a security clearance, who are required by their work to restate classified information from an already classified source document may classify derivatively at the level of their clearance. Classifiers shall determine which information is classified as SECRET or CONFIDENTIAL (depending on the classification authority delegated to that individual), how long it needs to be protected and properly mark that information.

CHAPTER 2
SECTION 2 - MARKINGS

A. Identifying and Marking Classified Information. A uniform security classification system requires that standard markings be applied to classified information. Except in extraordinary circumstances or as indicated in this Instruction and in references (a), (b), and (c), the marking of classified information created after October 16, 1995, shall not deviate from the following prescribed formats. If markings cannot be affixed to specific classified information, the originator shall provide holders or recipients of the information with written instructions for protecting the information. 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. The overall marking shall be conspicuous enough to alert anyone handling the document that it is classified. If the markings do not attract your attention, it is not conspicuous. Overall, classification markings shall be larger and **Bolder** than other text on the page.

B. Identification of Authorities. The face of each originally classified document shall bear the following:

1. Classification Authority. The name or personal identifier and position title of the original classifier shall appear on the "Classified By" line. For example:

Classified By: John Doe, Chief, Division 5

2. Agency and Office of Origin. If not otherwise evident, the agency and office of origin shall be identified and placed below the "Classified By" line. For example:

Classified By: John Doe, Chief, Division 5,
Department of Good Works, Office of Administration

3. Reason for Classification. The original classifier shall identify the reason(s) for the decision to classify. The classifier shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.5 plus the letter(s) that corresponds to that classification category in section 1.5 of reference (a). For example:

Reason: 1.5 (b), (c), & (g).

C. Overall Marking. The highest level of classified information contained in a document shall appear in a way that shall distinguish it clearly from the information text.

1. Conspicuously place the overall classification at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

2. For documents comprised of information classified at more than one level, the overall marking shall be the highest level. For example, if a document contains some information marked "SECRET" and other information marked "CONFIDENTIAL," the overall marking would be "SECRET."

D. Portion Marking. Each portion of a document, usually a paragraph, but including subjects, titles, graphics and the like, shall be marked to indicate its classification level by placing a parenthetical symbol immediately preceding or following the portion to which it applies.

1. To indicate the appropriate classification level, the symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used.

2. Waivers from the portion marking requirements for a specific category of information shall be forwarded through the Office of Security before submission to the ISOO for final approval. All requests shall include the reasons that the benefits of portion marking are outweighed by other factors. Statements citing administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver by the ISOO.

3. **"Declassify On" Line.** The X1 through X8 exemption categories formerly used to exempt information from 10-year declassification can no longer be used. One of four options may be applied based on the sensitivity of the information IAW ISOO Directive No. 1, section 2001.12 reference (y) :

a. A date or event less than 10 years, or if unable to identify such a date or event;

b. A date 10 years from the date of the document;

c. A date greater than 10 and less than 25 years from the date of the document; or

d. A date 25 years from the date of the document.

Note: When determining the duration of classification, the original classification authority should consider the four options listed above sequentially:

a. consider the least amount of time that information needs to be classified, that is, a time frame that is less than 10 years;

b. if unable to determine a date or event of less than 10 years, then 10 years;

c. between 10 years and up to 25 years based upon the sensitivity of the information as determined by the OCA; and

d. then finally, 25 years from the date of the decision.

Note: Agencies with classification guides shall need to update them as soon as possible. The Directive requires that they be updated at least once every five years. For those agencies with ISCAP approved declassification guides, individual items from those guides, in current use, may be incorporated into revised classification guides. See reference (y), sections 2001.15 and 2001.32.

4. Declassification Examples.

a. Document is dated October 10, 2004, and the information will no longer meet the standards for classification 15 days after Admiral West completes his trip:

Classified by: David Smith, Chief, Protective Services Division,
Department of Military Travel
Reason: 1.4(g)
Declassify on: 15 days after Admiral West completes travel to Europe.

b. Document is dated October 10, 2003, and the information will no longer meet the standards for classification in eight years:

Classified by: David Smith, Chief Division 5, Department of Good Works
Reason: 1.4(h)
Declassify on: October 10, 2011

c. Document is dated November 15, 2003, and the information will no longer meet the standards for classification in ten years:

Classified by: Gary Smith, Branch Chief, Operations, Department of Good Works
Reason: 1.4(g)
Declassify on: November 15, 2013

d. Document is dated December 12, 2003, and the information will no longer meet the standards for classification in 16 years:

Classified by: Ethel Jones, Director, Operations Division,
Department of Diplomatic Services
Reason: 1.4(b)
Declassify on: December 12, 2019

e. Document is dated January 20, 2004, and the information will no longer meet the standards for classification in 25 years:

Classified by: Mary West, Lead Engineer, F25 Division, Department of Weapons
Reason: 1.4(a)
Declassify on: January 20, 2029

Note: See reference (y), section 2001.21(a) (4).

E. Classification Extensions

1. An original classification authority may extend the duration of classification for successive periods not to exceed 10 years at a time. For information contained in records determined to be permanently valuable, multiple extensions shall not exceed 25 years from the date of origin of the information. The "Declassify On" line shall indicate the date the original declassification instructions changed. The revised instructions shall be conspicuously applied to the face of the document and shall include the identity of the person authorizing the extension or other revision. The office of origin shall make reasonable attempts to notify all holders of such information and classification guides shall be updated to reflect such revisions.

2. An example of an extended duration of classification made on October 16, 2005, and originally marked for declassification 10 years from the date of the decision, may appear as follows:

> Classified By: John Doe, Chief, Division 5, Department of Good Works,
> Office of Administration
> Reason: 1.5(g)
> Declassify On: October 16, 2005
> Classification extended until October 16, 2015 by: John Doe, Chief, Division 5

F. Marking Information Exempted From Automatic Declassification at 25 Years

1. When an OIG senior official exempts permanently valuable information from automatic declassification at 25 years, the "Declassify On" line shall be revised to include the symbol "25X" plus a brief reference to the pertinent exemption category(ies) or the number(s) that corresponds to that category(ies) of reference (a). Other than when the exemption pertains to the identity of a confidential source, or a human intelligence source, the revised "Declassify On" line shall also include the new date or event for declassification. These categories are extracted from reference (a):

a. 25X1: Reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the U.S.

b. 25X2: Reveal information that would assist in the development or use of weapons of mass destruction.

c. 25X3: Reveal information that would impair U.S. cryptologic systems or activities.

d. 25X4: Reveal information that would impair the application of state-of-the-art technology within a U.S. weapons system.

e. 25X5: Reveal actual U.S. military war plans that remain in effect.

f. 25X6: Reveal information that would seriously and demonstrably impair relations between the U.S. and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the U.S.

g. 25X7: Reveal information that would clearly and demonstrably impair the current ability of U.S. Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized.

h. 25X8: Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans.

i. 25X9: Violate a statute, treaty, or international agreement.

2. The pertinent portion of the marking might appear as follows:

a. Declassify On: 25X-State-of-the-art technology within U.S. weapons system.
October 1, 2010, or

b. Declassify On: 25X4
October 1, 2010

G. <u>Derivative Classification Markings</u>. Information classified derivatively based on source documents or classification guides shall bear all markings except as provided below. Information for these markings shall be carried forward from the source document or taken from instructions in the appropriate classification guide.

1. **"Derived From" Line.** "Classified By" line is replaced with a "Derived From" line. The "Reason" line, as reflected in the source document(s) or classification guide, is not required to be transferred to the derivative document. The derivative classifier shall concisely identify the source document or the classification guide on this line, including the agency and office of origin. For example:

a. Derived From: John Doe, Chief, Division 5, Department of Good Works,
Office of Administration
Memo dated October 20, 1995, or

b. Derived From: CG No.1, Department of Good Works,
dated October 20, 1995

2. **More Than One Source Document.** When a document is classified derivatively based on <u>more than one source document</u> or <u>classification guide</u>, the "Derived From" line shall appear as follows:

a. Derived From: Multiple Sources. The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document.

b. A document derivatively classified on the basis of a source document that is itself marked "Multiple Sources" shall cite the source documents on its "Derived From" line rather than the term "Multiple Sources." For example:

Derived From: Report entitled, "New Weapons,"
dated October 20, 1995,
Department of Good Works, Office of Administration

3. **Reason for Classification.** The reason for the original classification decision, as reflected in the source document(s) or classification guide, is not required to be transferred in a derivative classification action.

4. **Declassification Instructions**

a. The derivative classifier shall carry forward the "Declassify On" line from the source document to the derivative document, or the duration instructions from the classification guide. In those instances where (a) source document(s) contain(s) the declassification instruction "OADR" or "X1 through X8," the derivative classifier, unless otherwise instructed, shall note (1) the fact that the source document(s) was marked with either of these instructions; and (2) the date of origin of the most recent source document as appropriate to the circumstances.

Note: Source documents with the notation "Originating Agency's Determination Required" or "OADR" on the "Declassify On" line cannot be dated later than October 13, 1995, the effective date of E.O. 12958.

Note: Source documents with an X1 through X8 notation on the "Declassify On" line cannot be dated later than September 21, 2003, the day before the effective date of the marking requirements in the March 25, 2003, amendment to E.O. 12958.

b. Declassification Examples:

(1) The source document used for a derivative decision that is being made on October 10, 2003, has OADR on the "Declassify On" line. The date of the source document is October 5, 1993.

Derived from: Department of Good Works Report titled *IT Developments*,
dated October 5, 1993
Declassify on: Source marked OADR; Date of Source, October 5, 1993

(2) The source document used for a derivative decision that is being made on November 15, 2003, has "X4" on the "Declassify On" line. The date of the source document is December 2, 2000.

Derived from: Department of Weapons Memo dated 12/2/00, Subject: New LASER Gun
Declassify on: Source marked X4; Date of Source, December 2, 2000

(3) Three source documents are being used for a derivative decision that is being made on November 15, 2003.

(a) *Source document 1* is a memo dated October 5, 1992, with "OADR" on the "Declassify On" line;

(b) *Source document 2* is a report dated January 20, 2001, with X5 on the "Declassify On" line; and

(c) *Source document 3* is a classification guide dated December 5, 2002, with the item from the guide being used in the document citing a duration of October 10, 2008.

This is a "Multiple Sources" derivative decision. Of the three sources, source 2 has the longest duration for classification and should be cited on the "Declassify On" line of this document:

Derived from: Department of Weapons Report dated 1/20/01, Subject: New Computers
Declassify on: Source marked X5, Date of Source, January 20, 2001

(4) Three source documents are being used for a derivative decision that is being made on November 15, 2003.

(a) *Source document 1* is a memo dated October 5, 1992, with "OADR" on the "Declassify On" line;

(b) *Source document 2* is a report dated January 20, 2001, with X5 on the "Declassify On" line; and

(c) *Source document 3* is a letter dated December 5, 2002, with "X-Foreign relations" noted on the "Declassify On" line.

This is also a "Multiple Sources" derivative decision. Of the three sources, source document 3 has the longest duration for classification and should be cited on the "Declassify On" line of this document:

Derived from: Department of Weapons Report dated 1/20/01, Subject: New Computers
Declassify on: Source marked X-Foreign Relations; Date of Source, December 5, 2002

Note: See reference (y), section 2001.22.

5. Use of the "25X" Marking

a. The marking applied to information when it has been exempted from 25 year automatic declassification cannot be used unless the specific information has been approved through the ISCAP process. This is usually in the form of a declassification guide. When used, the "Declassify On" line would include the symbol "25X" plus a brief reference to that category(ies) in section 3.3(b) of the Order and a new date or event for declassification. The marking would appear as:

(1) Declassify on: 25X-State-of-the-art use of technology within a U.S. weapons system, October 1, 2040, or

(2) Declassify on: 25X4, October 10, 2040

b. The identity of a confidential human source or a human intelligence source is not subject to automatic declassification. The marking for the exemption of this specific information, which also must be approved through ISCAP, is Declassify on: 25X1-human.

c. "Information about the application of an intelligence source or method" is still subject to automatic declassification on a specific date or event that must be included on the "Declassify On" line.

d. Those agencies with ISCAP approved declassification guides may choose to include the exempted items of information with the new declassification dates or events from these guides in revised or updated versions of appropriate classification guides.

ORIGINALLY CLASSIFIED DOCUMENTS WILL NOT CONTAIN A "25X" MARKING ON THE "Declassify On" LINE.

ALL ORIGINALLY CLASSIFIED DOCUMENTS WILL CONTAIN EITHER A DATE OR EVENT LESS THAN 10 YEARS OR A DATE FROM 10 TO 25 YEARS ON THE "Declassify On" LINE.

Note: See reference (y), section 2001.21(e).

H. Overall Marking (Derivative). The derivative classifier shall carry forward the overall marking from the source document or the classification level instruction from the classification guide and mark the derivative document as provided above. When a document is classified derivatively based on more than one source document or classification guide, the overall marking shall reflect the highest level of classification of any its sources.

I. Portion Marking (Derivative). Each portion of a derivatively classified document shall be marked IAW its source and as indicated above.

J. Marking Prohibitions. Markings other than "Top Secret," "Secret," or "Confidential" shall not be used to identify information as classified national security information. No other term or phrase shall be used in conjunction with these markings, such as "Secret Sensitive" or "Agency Confidential," to identify classified national security information. The terms "Top Secret," "Secret," and "Confidential" may not be used to identify unclassified executive branch information. Classifiers shall refrain from the use of special markings when they merely restate or emphasize the principles and standards of reference (a). Any special markings used outside the scope of reference (a) shall receive prior approval from the Director, ISSO.

K. Transmittal Document. A transmittal document shall indicate on its face the highest classification level of any classified information attached or enclosed. The transmittal letter shall include the highest overall marking of the document and if the transmittal contains no classified information in the body of the letter, the following statement shall be centered at the bottom of the page.

UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE REMOVED

(OR, if classified information is contained in the body of the letter)

UPON REMOVAL OF ATTACHMENTS, THIS DOCUMENT IS (*CLASSIFICATION*)

L. Foreign Government Information. Documents that contain foreign government information (FGI) shall include either the marking "Foreign Government Information," "FGI" or a marking that otherwise indicates that the information is of foreign origin. If the fact that information is foreign government information must be concealed, the marking shall not be used and the document shall be marked as if it were wholly of U.S. origin.

M. Working Papers. A working paper is defined as documents or materials, regardless of the media, which are expected to be revised prior to the preparation of finished product for dissemination or retention. Working papers containing classified information shall be dated when created, marked with the highest classification of any information contained in them, protected at that level, and destroyed when no longer needed. When any of the following apply, working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level:

1. Released by the originator outside of the originating activity.

2. Retained more than 180 days from date of origin.

3. Filed permanently.

N. Bulky Material. Bulky material, equipment, and facilities, etc., shall be clearly identified in a manner that leaves no doubt about the classified status of the material, the level of protection required, and the duration of classification. Upon a finding that identification would itself reveal classified information, such identification is not required. Supporting documentation for such a finding shall be maintained in the appropriate security facility and in any applicable classification guide.

O. Unmarked Presidential Materials. Information contained in unmarked presidential or related materials preserved in a presidential library or other repository and which pertains to the national defense or foreign relations of the U.S. and has been maintained and protected as classified information under prior orders shall continue to be treated as classified information under reference (a), and is subject to its provisions regarding classification.

P. Distribution Controls. Each OIG Component shall maintain control over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need to know the information. All recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in document status occurs.

Q. Specific Marking on Documents. Reference (c) provides illustrated guidance on the application of original/derivative classification and associated markings to documents prepared by the DoD. The OIG personnel are encouraged to use this document as a general guide. Reference (b) should be referred to when using special intelligence markings.

R. Overall and Page Markings. At the time of original/derivative classification, the document shall be marked in capital letters (preferably in red ink) at the top and bottom of the title/first page with the overall classification of the document and at the top and bottom of each interior page with the highest classification of information on the page. Within a classified document, the top and bottom of each page that contains no classified information shall be marked "Unclassified" or "For Official Use Only (FOUO)," as appropriate (preferably in black ink).

S. File, Folder, or Group of Documents. When classified information is permanently filed (bound or unbound) in a folder, the folder shall be marked in capital letters (preferably in red ink) at the top and bottom (front and back) with the highest classification of information contained in the folder. When possible, the top front marking on the folder used for filing classified material shall be accomplished in a manner that allows the classification to remain visible once the folders have been filed.

T. Markings on Special Categories of Material. Standard Form (SF) 706, *Top Secret Label*, SF-707, *Secret Label*, and SF-708, *Confidential Label*, are color-coded adhesive labels that shall be used, whenever possible, when marking special categories of classified material (i.e., non-document material, such as typewriter ribbons and the like). The SF-709, *Classified*, SF-710,

Unclassified, and SF 711, *Data Descriptor Label*, also adhesive labels, shall be used in conjunction with SF-706, 707, and 708, whenever possible, when applying any necessary additional identifying data and/or safeguarding procedures (e.g., North Atlantic Treaty Organization (NATO)) to special categories of material. (See Appendix E.)

U. Miscellaneous Material. Unless immediately destroyed, classified carbons, rejected copy, typewriter ribbons, ribbons from word processors, printers, and the like shall be marked or labeled to indicate the level of classification and stored accordingly.

V. For Official Use Only. FOUO procedures for handling, marking, and processing information should be IAW references (b) and (d).

CHAPTER 2
SECTION 3 - CLASSIFICATION PROHIBITIONS AND LIMITATIONS

A. Classification Prohibitions

1. Information shall not be classified to:

a. Conceal violations of law, inefficiency, or administrative error.

b. Prevent embarrassment to a person, organization, or agency.

c. Restrain competition.

d. Prevent or delay the release of information that does not require protection in the interest of national security.

2. Basic scientific research information not clearly related to the national security may not be classified.

3. Information may not be reclassified after it has been declassified and released to the public under proper authority.

4. Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under references (e) and (f) or the mandatory review provisions of reference (a) only if such classification meets the requirements of reference (a) and is accomplished on a document-by-document basis with the personal participation or under the direction of the OIG or the official designated under reference (a). This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under reference (g).

5. Compilations of items of information, which are individually unclassified, may be classified if the compiled information reveals an additional association or relationship that:

a. Meets the standards for classification under reference (a) and is not otherwise revealed in the individual item of information.

b. As used in reference (a), “compilation” means an aggregation of pre-existing unclassified items of information.

B. Classification Challenges. Reference (a) encourages individuals to challenge classification decisions as a means for promoting proper and thoughtful classification actions. As a result of this, OIG procedures shall ensure that no retribution or other negative actions are taken against any individual initiating such a challenge. Those authorized holders wishing to

challenge the classification status of information should present such challenges to an OCA who has jurisdiction over the information. Such a formal challenge should be made in writing, but does not have to be specific other than to ask why the information is or is not classified, or is classified at a certain level.

C. Classification Challenge Tracking System. The Office of Security maintains a system for processing, tracking, and recording formal classification challenges made by authorized holders. The records of challenges shall be subject to the attention of the ISCAP, which is under the auspices of the ISOO. All classification challenges shall be kept separate from Freedom of Information Act (FOIA)/Privacy Act (PA) requests with a separate record keeping system established to process and record the challenges.

D. Classification Challenge Review Process. Classification challenges shall be reviewed by an OCA with jurisdiction over the challenged information. The OCA shall provide a written response to the challenger within 30 days. If the challenger is not satisfied with the response, an impartial official or panel shall review the challenger's request (supervisor of the OCA at the next highest level). If the challenge is not processed within 30 days, the OCA shall acknowledge the challenge in writing and provide the challenger with a date when the OCA shall respond. The acknowledgment shall include a statement that if no response is received within 90 days, the challenger has the right to forward the challenge to the ISCAP for a decision.

E. Reevaluation of Classification Because of Compromise. The Office of Security, in conjunction with the office of primary responsibility (OPR), shall prepare a written damage assessment and reevaluate information classified by the OIG that has been lost or possibly compromised. The OPR shall promptly notify all holders of the information of any countermeasures taken to negate or minimize the effect of any compromise.

CHAPTER 2
SECTION 4 - CLASSIFICATION GUIDES

A. Classification Guides. Originators of classification guides are encouraged to consult the users of guides for input when reviewing or updating guides. Users of classification guides are encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide. Classification guides shall be reviewed as circumstances require, but at least once every 5 years. Each guide shall be approved and in writing by an official who has program or supervisory responsibility over the information or is the senior agency official and is authorized to classify information originally at the highest level of classification prescribed in the guide. The OIG shall submit to the ISOO all declassification guides for final approval. Classification guides shall, at a minimum:

1. Identify the subject matter of the classification guide.

2. Identify the original classification authority by name or personal identifier and position.

3. Identify an agency point-of-contact with subject matter expertise.

4. Provide the date of issuance or date of last review.

5. State precisely the elements of information to be protected.

6. State which classification level applies to each element of information and, when useful, specify the elements of information that are unclassified.

7. State, when applicable, special handling caveats.

8. Prescribe declassification instructions or the exemption category from automatic declassification for each element of information. When reviewing or updating a guide, the duration of classification prescribed for each element of information shall continue to correspond to the date of the guide's first issuance. When citing the exemption category listed in reference (a), the guide shall also specify the applicable statute, treaty or international agreement.

9. State a concise reason for classification, which, at a minimum, cites the applicable classification categories in reference (a).

B. Dissemination of Classification Guides. Classification guides shall be disseminated as widely as necessary to ensure the proper and uniform derivative classification of information. All classification guides shall be submitted through the Office of Security for review and then forwarded to ISOO for final approval. The Office of Security shall maintain a database of all classification guides approved and issued by the OIG. The OCA(s) shall be responsible for obtaining approval of all classification guides before they are distributed.

CHAPTER 2
SECTION 5 - DECLASSIFICATION AND DOWNGRADING

A. Declassification and Downgrading. Information shall be declassified as soon as it no longer meets the standards for classification under reference (a). It is presumed that information that continues to meet the classification requirements under reference (a) requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases, the information may be declassified by the OCA. When such questions arise, they shall be referred to the FOIA/PA Office. The FOIA/PA Office shall contact the equity holder(s) and request a declassification review in response to a FOIA request. The equity holder(s) shall determine, as an exercise of discretion, whether public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. Reference (a) does not amplify or modify the substantive criteria or procedures for classification; or create any substantive procedural right subject to judicial review. If the ISOO determines that information is classified in violation of reference (a), that official may require the information to be declassified.

B. Automatic Declassification. Within 5 years from the date of reference (a), all classified information contained in records that are more than 25 years old, and have been determined to have permanent historical value under reference (g) shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall automatically be declassified no longer than 25 years from the date of its original classification, except for information that would:

1. Reveal the identity of a confidential human source, reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the U.S.

2. Reveal information that would assist in the development or use of weapons of mass destruction.

3. Reveal information that would impair U.S. cryptologic systems or activities.

4. Reveal information that would impair the application of state-of-the-art technology within a U.S. weapons system.

5. Reveal actual U.S. military war plans that remain in effect.

6. Reveal information that would seriously and demonstrably impair relations between the U.S. and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the U.S.

7. Reveal information that would clearly and demonstrably impair the current ability of U.S. Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized.

8. Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans.

9. Violate a statute, treaty, or international agreement.

C. Systematic Declassification. Systematic declassification pertains to all classified agency records determined under Federal law to have permanent historical value wherever they may be stored. These records may be located or stored in:

1. The National Archives (including regional archive branches)

2. Federal Records Centers

3. Presidential Libraries

4. Agency file rooms or repositories

5. Other agencies

6. Other approved repositories, including contractor facilities, libraries, etc.

D. Mandatory Declassification Review. The OIG shall declassify information that no longer meets the standards for classification under reference (a). A process has been established to provide a means to administratively appeal the denial of a mandatory review request and for notifying the requestor of the right to appeal a final agency decision to the ISCAP. Information requested under the FOIA/PA is released unless withholding is otherwise authorized or warranted under applicable law.

E. Processing Requests and Reviews. The OIG and personnel may refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classified under reference (a). When the FOIA/PA Office receives any request for documents in its custody that contains information originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of reference (a), the FOIA/PA Office refers copies of requests and the pertinent documents to the originating agency for processing. After consultation with the originating agency, the FOIA/PA Office may inform any requester of the referral unless such association is itself classified under reference (a).

CHAPTER 3 SAFEGUARDING
SECTION 1 - SAFEKEEPING AND STORAGE

A. General Policy. Classified information shall be secured under conditions adequate to prevent access by unauthorized persons. The Chief, Office of Security, should approve exceptions to these requirements. The DoD policy concerning the use of force for the protection of classified information is specified in reference (h). Weapons or sensitive items such as funds, jewels, precious metals, or drugs shall not be stored in the same container used to safeguard classified information. Security requirements for Sensitive Compartmented Information Facilities (SCIFs) are established by the Director of Central Intelligence Directives. Current holdings of classified material shall be reduced to the minimum required for mission accomplishment.

B. Standards for Storage Equipment. The General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, alarm systems and associated security devices suitable for the storage and protection of classified information. Reference (i) describes acquisition requirements for physical security equipment used within the DoD. The GSA-approved security containers shall have a label stating "GSA Approved Security Container" affixed to the front of the container usually on the control or the top drawer. If the label is missing or if the container's integrity is in question, the container shall be inspected by a GSA certified technician. If the container is found to meet specifications, a new label shall be attached. Inspections and recertification of containers information can be found on the GSA website http://www.nfc.fss.gsa.gov/security, or on the DoD Lock Program website http://locks.nfesc.navy.mil, or by calling GSA at (703) 305-7342, or the DoD Lock Program at (800) 290-7607.

C. Storage of Classified Information. Classified information is to be guarded or stored in a locked security container, vault, room, or area, as follows:

1. Top Secret

a. A GSA approved security container or modular vault, in a vault; or in the U.S., in a secure room if under U.S. Government control. Other rooms that were approved for the storage of Top Secret in the U.S. may continue to be used. When located in areas not under U.S. Government control, the storage container, vault, or secure room shall be protected by an intrusion detection system or guarded when unoccupied. U.S. Government control means access to the classified material is controlled by an appropriately cleared U.S. Government civilian, military, or contractor employee. An Intrusion Detection System (IDS) used for this purpose shall meet the requirements of reference (b). Security forces shall respond to the alarmed location within 15 minutes from the time of notification.

b. New purchase of combination locks for GSA approved security containers, vault doors, and secure rooms shall conform to Federal Specification FF-L-2740. Existing non-FF-L-2740 mechanical combination locks will not be repaired. If the locks should fail, they will be replaced with locks meeting FF-Ll-2740.

c. Storage requirements for Top Secret Sensitive Compartmented Information (SCI) are proscribed in other Director of Central Intelligence Directives.

2. Secret and Confidential. Secret and Confidential information shall be stored in the manner prescribed for Top Secret. It can be stored in an approved GSA security container or vault without supplemental controls or in secure rooms that were approved for the storage of Secret and Confidential material by the DoD Components before October 1, 1995.

D. Replacement of Combination Locks. The mission and location of the activity, the classification level and sensitivity of the information, and the overall security posture of the activity determine the priority for replacement of existing combination locks. All system components and supplemental security measures, including electronic security systems (e.g., automated entry control subsystems and video assessment subsystems), and level of operations shall be evaluated by the Office of Security and coordinated with the Administration and Logistics Services Directorate (ALSD) when determining the priority for replacement of security equipment.

E. Storage of Bulky Material. Storage areas for bulky material containing classified information may have access openings secured by GSA-approved changeable combination padlocks (Federal Specification FF-P-110 series) or high security key-operated padlocks (Military Specification MIL-P-43607).

F. Key Accountability. The OIG Components shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are used. The level of protection provided by such keys shall be equivalent to that afforded the classified information being protected by the padlock. Reference (j) makes unauthorized possession of keys, key-blanks, key-ways, or locks adopted by any part of the DoD for use in the protection of conventional arms ammunition or explosives, special weapons and classified equipment, a criminal offense punishable by fine or imprisonment for up to 10 years, or both.

G. Procurement of New Storage Equipment. New security storage equipment shall be procured from those items listed on the GSA Federal Supply Schedule.

H. Numbering and Designating Storage Facilities. No external mark shall reveal the level of classified information authorized to be or actually stored in a given container or vault. Priorities for emergency evacuation and destruction shall not be marked or posted on the exterior of storage containers or vaults.

I. Combinations to Containers and Vaults. Combinations to security containers, vaults, and secure rooms shall be changed only by individuals having that responsibility and an appropriate security clearance. Combinations shall be changed:

1. When placed in use.

2. Whenever an individual knowing the combination no longer requires access.

3. When the combination has been subject to possible compromise.

4. Once a year for safes containing NATO classified information.

5. At least once every 2 years.

6. When taken out of service. Built-in combination locks shall then be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30.

a. Selecting Combinations. Combinations for each lock shall be unique to that lock and shall have no systematic relationship to other combinations used within a specific office. Combination numbers shall not be derived from numbers otherwise associated with the specific office or its personnel. The numbers within a combination shall be selected on a random basis without deliberate relationship to the other except to provide appropriate variance to operate the lock properly.

b. Classifying Combinations. The combination of a container, vault, or secure room used for the storage of classified information shall be assigned a security classification equal to the highest category of the classified information stored therein. Any written record of the combination shall be marked with the classification. Declassification of combinations occurs at the time they are changed.

c. Recording Storage Facility Data. A record shall be maintained for each vault or secure room door or container used for storage of classified information showing location of the door or container, and the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination. All security containers (safes), even if they are not in service, should have a SF-700, *Security Container Information*, completed. The SF-700 shall be used for this purpose (see Appendix F.)

(1) Part 1 of SF-700. When completed, the form shall be placed in an interior location in security cabinets and on vault or secure room doors. To the extent practical, Part 1 shall be on the inside face of the locking drawer of file cabinets, and on the inside surface of map and plan cabinet and vault doors.

(2) Parts 2 and 2A of SF-700. Parts 2 and 2A shall be marked conspicuously on the front of the form with the highest level of classification and any special access notice applicable to the information authorized for storage in the container and shall be stored in a security container other than the one in which they apply.

(3) Internal Security Containers. Internal security containers shall provide for prompt notification to the official responsible for the area if a container is found unsecured and unattended or shows evidence of unauthorized entry attempts or if the SF-700 is inaccessible or not available. Listings of persons having knowledge of the combination shall be continued as necessary on an attachment to Part 2. A minimum of two names shall be entered on the form.

(4) Safe Combinations. Safe combinations shall not be recorded on pieces of paper or other material with the following exception: persons having access to a number of combinations may, with the approval of their staff supervisor, record all combinations on an 8 1/2" x 11" page. This page shall be classified and marked with the highest classification of material stored in the security containers and filed in a master security container. The combination to the container in which the page is stored shall be memorized.

(5) Record of Entry. All SF-700s shall be listed in the Office of Security database.

J. Repair of Damaged Security Containers. Neutralization of lock-outs or repair of any damage that affects the integrity of a security container approved for storage of classified information shall be accomplished only by authorized persons who have been the subject of a trustworthiness determination as defined in reference (k) and are continuously escorted while so engaged. With the exception of frames bent through application of extraordinary stress, a GSA approved security container manufactured before October 1990 (identified by a silver GSA label with black lettering affixed to the exterior of the container) is considered to have been restored to its original state of security integrity as follows:

1. All damaged or altered parts, for example, the locking drawer, drawer head, or lock, are replaced.

2 Has been drilled immediately adjacent to or through the dial ring to neutralize a lock-out, a replacement lock meeting FF-L-2470A is used, and the drilled hole is repaired with a tapered, hardened tool-steel pin, or a steel dowel, drill bit or bearing with a diameter slightly larger than the hole and of such length that when driven into the hole there shall remain at each end of rod a shallow recess not less than 1/8" nor more than 3/16" deep to permit the acceptance of substantial welds, and the rod is welded both on the inside and outside surfaces. The outside of the drawer head shall then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface.

3. Unapproved modification or repair of security containers and vault doors is considered a violation of the container or integrity of the door and the GSA label shall be removed. Thereafter, they may not be used to protect classified information except as otherwise authorized in reference (b).

K. Moving/Turn-in of Safes. Safes being moved to another location should be locked before moving and escorted by appropriately cleared personnel. The cognizant Security Manager or personnel of the Office of Security shall inspect safes identified for turn-in to ensure no classified material remains therein. To prevent injury, OIG personnel shall ensure that all movement of safes is accomplished by the ALSD.

CHAPTER 3
SECTION 2 - CUSTODIAL PRECAUTIONS

A. Responsibilities of Custodians. All OIG employees are responsible for the safekeeping, handling, and storing of classified material in approved storage containers or facilities, when it is not in use or under the supervision of an authorized person. Before releasing classified information to another individual, the holder of the material shall ensure that person has the appropriate clearance and need to know for the information being released. The holder is defined as a person who has classified material in his or her possession, regardless of whether he or she has signed a receipt for the material. The OIG employee who releases the information or discloses the information verbally to another individual shall first ensure the individual is properly cleared and has the "need-to-know" for the information. *Employee badges do not constitute security clearance level or need-to-know*. Verification of clearance shall be made with the Office of Security.

B. Residential Storage Arrangements. The Chief, Office of Security, is the only approving authority to authorize removal of classified material from designated working areas in off-duty hours for work at home. The authorization shall be based on whether the residence has an approved GSA security container.

C. Care During Working Hours. Classified material removed from storage shall be kept under constant surveillance by persons authorized access and having a need to know thereto and, when not in use, protected from unauthorized view of its classified contents until returned to storage. Such protection shall be provided, as applicable, by the material's unclassified cover or by an appropriate cover sheet. Cover sheets shall be SF-703, 704, and 705 for, respectively, Top Secret, Secret, and Confidential documents (see Appendix G).

1. Cover sheets affixed to classified documents shall not be obscured by transmittal notes, routing sheets, etc.

2. Cover sheets shall remain with the document when the document is returned to the safe.

3. When documents are removed from classified storage files, a Optional Form 23, *Charge Out Record*, (or appropriate form), shall be completed and shall replace the document(s) when temporarily removed. When the documents are returned, the individual's name shall be lined out and the form stored for future use (see Appendix H). Sign-out sheets, automated tracking systems, and similar methods may be used.

4. Open containers including alarmed areas shall be identified by a standard issue red "OPEN" sign displayed on the front of the container. Locked and checked containers shall display the white reverse side of the sign "CLOSED." Containers with more than one built-in combination lock shall have the "OPEN-CLOSED" sign displayed on each drawer having a combination lock.

5. As a good security practice, the tops of security containers shall be kept free of all material except the SF-702, *Security Container Check Sheet* (see Appendix I).

6. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, computer and typewriter ribbons, and other items containing classified information shall be safeguarded according to the level of classified information they contain and shall be accordingly destroyed after they have served their purpose.

7. Destruction of personal computer printer or typewriter ribbons from which classified information can be obtained shall be accomplished in the manner prescribed for classified working papers of the same classification. After the upper and lower sections have been cycled through and overprinted five times in all ribbon, or impact, or typing positions, fabric ribbons may be treated as unclassified regardless of their previous classified use. Carbon and plastic ribbons and carbon paper that have been used in the production of classified information shall be destroyed in the manner prescribed for working papers of the same classification after initial use. However, any typewriter ribbon that uses technology that enables the ribbon to be struck several times in the same area before it moves to the next position may be treated as unclassified.

D. End-of-Day Security Checks. Each OIG Component that processes, handles, and stores classified information shall establish a system of security checks at the close of each working day to ensure that the area is secured. The SF-701, *Activity Security Checklist*, shall be used to record such checks. This form can be modified to suit the individual security (or safety) needs of the organization or particular office; i.e., entries for "STU-III CIK secured" "Common Access Card (CAC)" secured or "coffee pot turned off." The SF-702 shall be used to record the use of all vaults, secure rooms, and containers used for the storage of classified material (see Appendices I and J). Forms placed on safes, cabinets, or vaults containing security classified documents that record opening, closing, and routine checking of the security of the container, such as locking doors and windows, and activating alarms, (included are such forms as SF-701 and SF-702) shall be destroyed 3 months following the last entry on the form except for those forms that may be involved in an investigation.

1. After Hours and Weekend Activity. The SF-701 and 702 shall be annotated to reflect after-hours, weekend, and holiday activity.

2. Closing Containers. An authorized person shall record the date and time and initial the SF-702 in ink each time the container is opened or closed. When closing a container, the dial of the combination will be rotated at least four complete turns in the same direction and each drawer shall be physically checked before the SF-702 is initialed.

3. Checking Containers. At the end of each workday, or when a security container is closed other than during normal duty hours, a person other than the one closing the container shall check it, using the physical locking procedures described in the above paragraphs. The individual then shall record the time checked and initial the form. This checking procedure shall

apply for each workday whether or not the security container was opened. The date and the statement "Not Opened" shall precede the time and initials of the checker when the security container is not opened on a workday. A person other than the one locking the container shall make the check of the container. Individuals working alone after duty hours may contact a nearby OIG employee to check their container.

4. Desk Check. At the close of the workday, each occupant of a desk shall thoroughly check each drawer to determine that it does not contain any classified material.

5. Room Checks (Designated Security Checks). Supervisors shall designate a responsible individual for each workday to conduct a final security check of a working area using a SF-701. The security checker's designated area of responsibility may be a single room or a complex of rooms. The final security check shall verify all classified material is properly secured.

6. Personnel Working Late. The minimum and normal procedure, when personnel are working late on a duty day, requires the designated security checker (usually the last person to leave an area) to conduct the final security check in all areas that have been secured and to complete the SF-701 for those areas. The security checker shall then inform other personnel staying late that all areas are secured with the exception of the immediate area they are working in and that they are responsible for securing that area and completing the SF-701 when they finish their work.

E. Emergency Planning. Plans shall be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. Such plans shall establish detailed procedures and responsibilities for the protection of classified material to ensure that the material does not come into the possession of unauthorized persons. Emergency plans shall provide for the protection of classified material in a manner that shall minimize the risk of injury or loss of life to personnel. In the case of fire or natural disaster, the immediate placement of authorized personnel around the affected area, pre-instructed and trained to prevent the removal of classified material by unauthorized personnel, is an acceptable means of protecting classified material and reducing casualty risk. Such plans shall provide for emergency destruction to preclude capture of classified material. (OIG employees should refer to the Inspector General Instruction 6055.1-1, *Occupant Emergency and Evacuation Plan* and the Inspector General Plan 3020.26 *Continuity of Operations Plan (COOP),* for detailed information.)

1. In emergency situations, in which there is an imminent threat to life or in defense of the homeland, Military Department or other DoD Component Heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose.

b. Limit the number of individuals who receive it.

c. Transmit the classified information via approved Federal Government channels by the most secure and expeditious method according to reference (b), or other means deemed necessary when time is of the essence.

d. Provide instructions about what specific information is classified and how it should be safeguarded. Physical custody of classified information shall remain with an authorized Federal Government entity, in all but the most extraordinary circumstances.

e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement.

2. Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority shall notify the originating Agency of the information and the DUSD (CI&S) by providing the following information:

a. A description of the disclosed information;

b. To whom the information was disclosed;

c. How the information was disclosed and transmitted;

d. Reason for the emergency release;

e. How the information is being safeguarded; and

f. A description of the briefings provided and a copy of the nondisclosure agreements signed.

F. Telecommunications Conversations. Classified information shall not be discussed in telephone conversations except over approved secure communications circuits, that is, cryptographically protected circuits or protected distribution systems.

1. The Secure Telephone Unit-III (STU-III) and Secured Telephone Equipment (STE) are approved for classified discussions within the limitations displayed by the STU-III or STE. The need-to-know shall be established before discussing classified information.

2. Users of secure telephones shall assure that only personnel with appropriate clearance and need-to-know are within hearing range of their conversation.

3. Classified information shall not be discussed on unsecured, standard commercial telephones. The use of codes or attempt to talk around classified subjects is prohibited.

G. Removal of Classified Storage and Information Processing Equipment. Properly cleared personnel shall inspect classified storage containers and information processing equipment before removal from protected areas or unauthorized persons are allowed access to them. The inspection shall be accomplished to assure no classified information remains within the equipment. Some examples of equipment that shall be inspected are:

1. Reproduction or facsimile machines and other office equipment used to process classified information.

2. GSA-approved security containers, filing cabinets, or other storage containers used for safeguarding classified information.

3. Other items of equipment that may inadvertently contain classified information.

H. Classified Discussions, Meetings, and Conferences. The following procedures apply to hosting conferences, seminars or symposiums, exhibits, conventions, training courses, or other such gatherings during which classified information is disclosed, hereafter called a "meeting."

1. Before agreement to sponsorship, adequate security protective measures must exist or be provided far in advance of the meeting. The meetings shall be limited to appropriately cleared U.S. Government or U.S. Government contractor locations ensuring that adequate security procedures have been developed and shall be implemented to minimize risk to the classified information involved.

2. Once an OIG Component accepts sponsorship of a meeting, the OIG Component or its designated cleared contractor assumes overall security responsibility, ensuring that:

a. the invitations, etc., are unclassified;

b. all attendees have the appropriate level of clearances and the need to know has been certified;

c. access rosters are prepared, checked, and coordinated with the Office of Security; and,

d. the subject matter, location, etc., of the meeting is coordinated with the appropriate Security Manager.

3. Notification is given to the appropriate Security Manager if loss or compromise occurs before, during, or after the meeting. The OIG Component also ensures that all participants are advised of their security responsibilities, and that classified presentations are appropriately marked and safeguarded for later compilation and distribution through secure channels.

4. Classified information to be presented shall be authorized for disclosure in advance by the U.S. Government department or agency having classified jurisdiction over the information involved. *Before showing or presenting the material, the briefer shall announce the overall classification level of the slides being presented. Slides shall not be shown unless the classification level is first disclosed by the presenter.*

5. If non-DoD members or foreign visitors are in attendance, OIG contractors shall obtain written approval from the Office of Security and Contracting Officer's Representative (COR) if they intend to disclose classified information.

6. Note-taking and electronic recordings such as cell phones, blackberries and PDA's shall not be permitted during classified presentations.

7. If foreign nationals are invited, a list of names, dates, and location of the sessions they will attend will be forwarded to the appropriate local security office following the basic procedures of foreign disclosure policy. The Office of Security shall:

a. Provide guidance and assistance to sponsoring OIG Components in developing and planning security measures for meetings.

b. Monitor meetings sponsored and conducted in the National Capital Region (NCR) by OIG Components to ensure compliance with established security measures.

c. Process requests from OIG Components concerning the attendance of foreign nationals at classified meetings and advise the requesting OIG Component of approval or disapproval of the request.

I. <u>Safeguarding United States Classified Information Located in Foreign Countries</u>. Except for classified information that has been authorized for release to a foreign government or international organization and is under the security control of such government or organization, the retention of U.S. classified material in foreign countries may be authorized only when that material is necessary to satisfy specific U.S. Government requirements. This includes classified material temporarily transferred into a foreign country through U.S. Government personnel authorized to escort or hand carry such material. Whether permanently or temporarily retained, the classified materials shall be stored under U.S. Government control, as follows:

1. At a U.S. military installation, or a location where the U.S. has extraterritorial status, such as an embassy or consulate.

2. At a U.S. Government activity located in a building used exclusively by U.S. Government tenants, if the building is under 24-hour control by U.S. Government personnel.

3. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants or under host-government control, provided the classified material is stored in security containers approved by the GSA and is placed under 24-hour control by U.S. Government personnel.

4. At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants, but which is under host-government control, provided the classified material is stored in GSA-approved security containers that are further secured in a locked room or area to which only U.S. personnel have access.

5. When the host government and U.S. personnel are collocated, U.S. classified material that has not been authorized for release to the host government shall be segregated from releasable classified material to facilitate physical control and prevent inadvertent compromise. The U.S. classified material that is releasable to the host country need not be subject to the 24 hour U.S. control requirement provided the host government exercises its own control measures over the pertinent areas or containers during non-duty hours.

6. Foreign nationals shall be escorted while in areas where nonreleasable U.S. classified material is handled or stored. When required by operational necessity, foreign nationals may be permitted, during duty hours, unescorted entry to such areas provided the nonreleasable information is properly stored or is under the direct personal supervision and control of cleared U.S. personnel who can prevent unauthorized access.

7. Under field conditions during military operations, the commander may prescribe the measures deemed appropriate to protect classified material.

J. <u>Non-Communications Security Classified Information Processing Equipment</u>. The OIG has a variety of non-Communications Security (COMSEC) approved equipment to process classified information. This includes copiers, computers, facsimile machines, printers, scanners, cameras, electronic typewriters, and other word processing systems, among others. Because much of this equipment has known security vulnerabilities, its use can cause unauthorized disclosure. Such vulnerabilities shall be reported to the Office of Security for handling.

1 Activities shall identify those features, parts, or functions of equipment used to process classified information that may retain all or part of the information. Activity security procedures shall prescribe safeguards to:

a. Prevent unauthorized access to that information.

b. Select equipment that performs the needed function and presents the lowest acceptable risk to the classified information the equipment processes.

c. Comply with guidance on security vulnerabilities issued by appropriate authority and shall report equipment problems and failures.

2. Reporting Equipment Problems and Vulnerabilities. The equipment that the OIG uses to safeguard, destroy, or process classified information can fail to function properly or otherwise perform in a way that threatens that information. When that occurs, responsible individuals within the using activities shall promptly:

a. Restore the protection to the information.

b. Report the incident to the Office of Security. Such reports shall:

(1) Describe the problem, equipment type, manufacturer, serial number, the number of equipment units involved, and any means found to overcome the problem.

(2) Problems or vulnerabilities with COMSEC equipment and controlled cryptographic items shall be reported as prescribed by the controlling COMSEC authorities reference (w). The COMSEC authority shall promptly coordinate these reports and corrective actions, along with the Director, Counterintelligence and Security Programs, OASD (NII), when the problems or vulnerabilities are common to all such equipment.

CHAPTER 4 CLASSIFIED DOCUMENT CONTROL
SECTION 1 - ACCESS

A. General Restrictions on Access

1. A person may have access to classified information provided that:

a. The Inspector General or designee has made a favorable determination of eligibility for access.

b. The person has signed an approved nondisclosure agreement.

c. The person has a need to know for the information.

2. Classified information shall remain under the control of the originating agency or its successor in function. The OIG shall not disclose information originally classified by another agency without its authorization. An official or employee leaving the OIG may not remove classified information from OIG control. Classified information may not be removed from any OIG official premises without proper authorization.

B. Policy

1. SF-312, *Classified Information Nondisclosure Agreement (NDA)* (previously SF-189). Any person who requires access to classified information shall be required to sign a nondisclosure agreement as a condition of access. Currently, SF-312 is the only form used to record newly executed agreements (see Appendix K).

2 Briefings. At the time an OIG member or employee is asked to sign a SF-312, the Security Manager or OIG Designated Personnel Representative shall ensure that a briefing is provided that addresses the purpose of the NDA, the intent and scope of its provisions, the consequences that shall result from the member's or employee's failure to sign the agreement, and the consequences that may result from the unauthorized disclosure of classified information, including possible administrative, civil or criminal sanctions. In addition to the NDA, personnel shall sign and read aloud the Security Attestation Statement. The SF-312 and Attestation Statement shall be maintained in the Office of Security file.

3. Implementation. Security Managers or Designated OIG Personnel Representatives shall ensure the briefing and the request to sign the SF-312 occur immediately before the employee is granted access to classified information. The signed SF-312 shall be forwarded to the Office of Security. The NDA remains valid for a 50 year retention period. The Office of Security shall retain previously signed copies of the SF-189 and SF-189-A, (the latter form applies only to cleared employees within industry) for 50 years. Any OIG employee may, at his or her discretion, elect to substitute a signed SF-312 for a previously signed SF-189.

4. Access by persons outside the Executive Branch. Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

5. Consistent with law, directives, and regulations, the Inspector General or designee shall establish uniform procedures to ensure that all automated information systems (AIS), including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

a. Prevent access by unauthorized persons.

b. Ensure the integrity of the information.

6. Responsibilities:

a. The Office of Security shall serve as the OIG focal point on all foreign disclosure matters.

b. The OIG Component Heads and field activities shall ensure that foreign visitors to their organizational elements are under escort at all times. The visitors shall only receive classified information if authorized on an oral and visual basis only.

c. All OIG briefing officers shall ensure that the information they provide to foreign visitors does not exceed that for which official approval has been granted.

d. Limited Access Authorization. Requests for limited access authorization to classified information by foreign nationals, foreign governments, and international organizations, under the provisions of reference (b) shall be addressed to the Office of Security. Requests shall include complete justification to support granting such access.

7. Visit Requests for Representatives of Foreign Governments. Requests by representatives of foreign governments visiting the OIG or any OIG field activity within the Continental United States (CONUS) shall be processed through the Department of State and Defense Intelligence Agency (DIA). The request shall then be forwarded to the Office of Security for appropriate action.

8. All OIG personnel shall be cognizant of the fact that:

a. Classified information, released in an oral or visual manner, shall relate only to the stated purpose of the visit and that no classified documents, tapes, recordings, or notes may be released unless such release has been approved.

b. Classified minutes of any meetings attended by the foreign visitor shall not be dispatched outside the OIG until proper processing of the minutes has been accomplished and the Office of Security has obtained approval for release.

c. Once a foreign visitor has been approved through the Department of State and DIA, no additions or deletions shall be made without a complete restatement of the purpose.

9. Visitor Verification of Clearance and Safeguarding Capability. The OIG policy requires that visitors shall provide advance notification of the pending visit in writing that establishes the visitor's security clearance and the purpose of the visit. An official other than the visitor who is in a position to verify the visitor's security clearance level shall sign requests. This is usually the visitor's security officer. Visit request letters shall include the full name of the individual, date and place of birth, social security number, rank or grade of visitor, security clearance of the visitor, employing activity of the visitor, date and duration of the proposed visit, the purpose of the visit in sufficient detail, and the names of persons to be contacted. Visit requests shall remain valid for not more than 1 year. The Joint Personnel Adjudication System (JPAS) may also be used to verify the personnel security clearance level for visitors requiring access to classified information. The Office of Security, upon receipt of visitor certification letters, shall consolidate all requests and provide the guard desk with an updated visitor certification roster. Visitors who appear on the list shall be granted a "no escort required badge." The Office of Security shall notify the office the person is visiting to provide confirmation of the level of access and safeguarding level of the visitor.

10. OIG Visit Requests. The Office of Security shall certify all requests for visits to other agencies and facilities requiring clearance verification. Requests shall be submitted immediately after the visit is confirmed, but no later than 1 week before departure, to ensure processing and receipt by the visiting activity. The sample visit request, Appendix L, provides details for preparing the request.

11. Processing the Visit Request. Each authorized user of the Automatic Security Administrative System (ASAS) may log in and generate a Visit Authorization Letter (VAL.) Once completed, go to Microsoft Outlook and send an E-mail notification to the Security Office or call. Provide the VAL number and, the Office of Security shall print it out, sign it, and fax it to the various destinations for the Field Offices. Headquarters personnel shall be notified when they may pick up the signed hard copy and make distribution as necessary.

CHAPTER 4
SECTION 2 - DISSEMINATION

A. Policy. Except as provided by statute or directives issued pursuant to reference (a), classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. The Inspector General or designee may waive this requirement for specific information originated within the OIG.

1. All OIG Components and field activities shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know.

2. Each OIG Component and field activity shall update, at least annually, the automatic, routine, or recurring distribution of classified information they distributed. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

B. Special Requirements for Release of Classified Intelligence Information to Department of Defense Contractors

1. The following information shall be provided to release classified intelligence information to a DoD contractor:

a. Name and address of the contractor for whom the intelligence information is intended. (The security classification for which the contractor's facility is accredited [facility clearance and storage capability] is required for physical release of the information to the contractor's custody.) This information shall be confirmed through the Office of Security.

b. Contract number, date services began, and contract duration. If extensions of the contract or follow-on contracts are anticipated, so state.

c. Name and address of the contracting activity.

d. Name and telephone number of an OIG point of contact for the contract.

e. Complete identification of the intelligence information for which release approval is required. Identify issuing agency, document subject, security classification, and all restrictive control markings and statements. In addition, include a statement as to whether the material is locally available to the requesting agency.

2. Authorization to Release. The authorization to release shall be based on the following criteria in that:

a. Determination has been made that the specific intelligence document is necessary to enable the contractor to perform. (If only portions of intelligence documents will satisfy the requirement, only the intelligence that is actually required for contract performance shall be considered for release.)

b. National Intelligence Estimates, Special National Intelligence Estimates, National Intelligence Analytical Memorandums, and Interagency Intelligence Memorandums are not released in their entirety to contractors. (Certain information contained therein may be released without identification as national intelligence.)

3 Special Requirements for Classified Intelligence. The Director, Central Intelligence Agency, has prescribed additional requirements and controls for classified intelligence in the possession of contractors. The contracting authority shall specifically include these requirements on the DD Form 254, *DoD Contract Security Classification Specification*. The contractor shall:

a. Maintain accountability for all classified intelligence information released to his or her custody, including confidential information.

b. Obtain the written permission of the releasing authority before reproducing classified intelligence information. If permission is granted, each copy shall be controlled in the same manner as the original.

c. Obtain prior approval of the releasing authority before destroying classified intelligence, including Confidential.

d. Restrict access to those individuals who possess the necessary security clearance and who are providing services under the contract. (Further dissemination to other contractors, subcontractors, other Government agencies, private individuals, or organizations are prohibited unless authorized in writing by the releasing authority.)

e. Ensure that classified intelligence information is not released to foreign nationals or immigrant aliens, whether or not they are consultants, U.S. contractors or employees of the contractor and regardless of the level of their security clearance, except with prior permission from the releasing authority.

f. Ensure that each employee having access to classified intelligence information is fully aware of the special security requirements for this material. The contractor shall also maintain records in a manner that shall provide, on demand, the names of individuals who have had access to this material.

g. Return of Classified Intelligence Information. Upon termination of the contract, or earlier when the purpose of the release has been served, the contracting officer shall require the contractor to return all classified intelligence information (furnished or generated) unless retention or destruction is authorized in writing by the releasing authority.

h. Authority for Release. Requests for authority to release classified intelligence information originated by the intelligence community, as defined in reference (l), shall be submitted to the Office of Security. Each request shall contain detailed justification for the release. Public release of SCI by contractors is not authorized.

C. Dissemination of Classified Information to Congress. Release of classified information to a congressional office shall be made in coordination with the Office of Communications and Congressional Liaison (OIG employees should refer to Inspector General Instruction 5545.1, *Participation in Congressional Activities*, for detailed information)

CHAPTER 4
SECTION 3 - ACCOUNTABILITY AND CONTROL

A. Collateral Top Secret Control Officer Program. Top Secret information, if disclosed, could cause exceptional, grave damage to the security of the U.S. A Top Secret Control Officer (TSCO) and at least one alternate shall be appointed by each OIG Component that prepares, receives, stores, or handles Top Secret material. The SD Form 507, *Top Secret Control Officer Designation Form*, (Appendix M), shall be completed and provided to the TSCO, who is responsible for issuing Top Secret control numbers and maintaining TS Form 02, *Top Secret Control Log*, (Appendix N). *Material received by OIG offices shall be logged in by the TSCO and then receipted to the OIG Component alternate TSCO for handling and safeguarding. All TSCOs and alternates shall possess a final Top Secret clearance.* Except in unusual circumstances, the TSCO should not be the person designated as the OIG Component's Security Manager. Top Secret material shall be taken to the TSCO or alternate for processing into the Top Secret account. For field activities, the office manager shall designate a TSCO and one alternate to accomplish matters affecting accountability and control of Top Secret material.

B. Accountability. A Top Secret Control Account (TSCA) is set up whenever Top Secret information is routinely originated, stored, received, or dispatched. The TSCAs, to include central points for receipting and dispatching Top Secret material, are limited to the minimum required for operational needs and functions of the office.

C. Top Secret Registers. The TSCO having accountability of Top Secret material shall prepare a IG Form 5200-1-8, *Top Secret Register Page* (Appendix O). Information received by or delivered to the Defense Courier Service (DEFCOS) shall be taken to the Top Secret Custodian for accountability. The DEFCOS receipts suffice for accountability purposes in these cases. The TSCO attaches a IG Form 5200-1-5, *Top Secret Access Record and Cover Sheet* (Appendix P), (or suitable form), to each Top Secret document. When completed, it shall identify all persons given access to the information and the date of the disclosure. The person possessing the material ensures the recording is done; however, the name of the person granted access need only appear once regardless of the number of times the individual has had access to the information. Recording access is not required for personnel permanently assigned to a TSCA, computer center, computer tape library, telecommunications facility, or printing and reproduction activity when duties involve processing large volumes of Top Secret material. This procedure is authorized only when entry to these areas is limited to assigned personnel identified on a roster. Such registers shall be retained for 5 years and shall, at a minimum, reflect the following:

1. Sufficient information to identify adequately the Top Secret document or material, to include the title or appropriate short title, date of the document, and identification of the originator.

2. The date the document was received.

3. Ensure each register page is assigned a consecutive number by including the calendar year and TSCA functional address symbol; for example, 99-IG-39. Alphabetical letters A, B, C, etc., are used when preparing continuation pages to the basic form. The register page number is also entered on the affected document to permit easier accomplishment of Top Secret inventories; however, care must be taken to not obliterate the permanently assigned originator control number.

4. Inactive Registers. This register reflects actions on documents no longer held in the office or agency. Documents that are transferred out of the office or agency, declassified, or destroyed shall be maintained for 5 years.

D. Inventory. The TSCO appointing authority, with action officers who use the information, annually review the volume and need for possessing the Top Secret material. The TSCO appointing authority certifies this review when endorsing the inventory report. An inventory shall be conducted upon change of the TSCO. The frequency between any type of inventory may not exceed 12 months. The TSCO appointing authority shall designate officials who understand Top Secret control procedures to conduct inventories. The number of inventory officials shall be based on the scope and volume of Top Secret material. The TSCO or alternate of the account undergoing the inventory may not participate; however, a succeeding TSCO may be appointed. Inventory shall determine if the TSCO is following proper procedures to ensure that that documents entered in the register are active and properly accounted for, and that all Top Secret material throughout the OIG served by the account is properly entered in the register. The inventory team shall perform the following procedures:

1. Count register pages to verify completeness of the register.

2. View all documents in the register. Account for all Top Secret documents stored in OIG Components and offices. Ensure each document has a receipt, or if the document was destroyed, a destruction certificate is on file.

3. Review the destruction process to verify correct procedures.

4. Review the inactive register, verify that documents listed are no longer the responsibility of the office being inspected; mark “audited” on the page, and have one team member initial and date the page. Entries so marked shall not be re-inspected on subsequent inspections.

5. Attempt to resolve any discrepancies noted during the inventory and treat as a possible security violation the inability to account for a document.

6. Submit a written report of the inventory to the Senior Information Officer (SIO), the Office of Security and forward one copy to the TSCO, who shall retain the report for 5 years.

E. Secret and Confidential Information. The OIG Components are not required to assign a control number to Secret or Confidential information materials. Each Component may implement this requirement as an additional security measure to provide ample accountability of

classified materials. If it has been determined that an accountability system (control numbers) will be utilized, prepare a IG Form 93, *Classified Control Log*, (Appendix O). Administrative procedures shall be established by each OIG Component for receiving and dispatching Secret and Confidential information and material via mail or courier. This applies to materials received from an outside source or from another OIG in a different geographical location. The control system for Secret and Confidential information shall meet the following minimum requirements:

1. Material received or dispatched outside any OIG Component shall show a record of receipt, SD Form 120, *OSD Receipt for Classified Material*, (Appendix S).

2. Records of receipts for Confidential and Secret material shall be retained for a minimum of 2 years.

3. The OIG Components shall develop procedures to protect incoming mail, bulk shipments, and items delivered by messenger until a determination is made whether classified information is contained therein. Screening points shall be established to limit access to classified information from personnel without an active security clearance.

F. Working Papers. Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be:

1. Dated when created.

2. Annotated with organization and office symbol of the originator.

3. Marked with the highest classification of any information contained therein.

4. Protected IAW the assigned classification.

5. Destroyed when no longer needed.

6. When any of the following conditions apply, working papers shall be protected and marked in the manner prescribed for a finished document of the same classification when:

a. Released by the originator outside the OIG Component or transmitted electrically through message center channels.

b. Retained more than 180 days from the date of origin; or

c. Filed permanently.

G. North Atlantic Treaty Organization and Joint Chiefs of Staff Documents. Active accountability records shall be maintained for North Atlantic Treaty Organization (NATO) and Joint Chiefs of Staff (JCS) documents.

H. Receipts. Receipts are required for Secret and Confidential material sent outside the geographical confines of an OIG Component or field activity.

I. Alternative or Compensatory Control Measures. The use of an unclassified nickname, obtained IAW the Chairman of the Joint Chiefs of Staff Manual CJCSM 3150.29B, together with a list of persons authorized access are designated as Alternative or Compensatory Control Measures (ACCM). ACCM may be used to assist in ensuring enforcement of strict need-to-know when other security measures are determined to be insufficient and where Special Access Program (SAP) controls are not warranted. Notify the Office of Security, Information Security Program Manager of your Component's use of ACCMs.

CHAPTER 4
SECTION 4 - REPRODUCTION

A. Restraint on Reproduction. Requests for reproduction of Confidential, Secret and special category material shall be used to document approval for reproduction and shall be submitted on IG Form 5200.1.1, *Authorization for Reproduction of Classified Material*, (Appendix Q). Top Secret material can only be reproduced by the Top Secret Custodian. Alternate TSCO's shall gain the approval of the TSCO before reproducing any Top Secret material.

B. Designation of Copiers. The OIG Components and field activities, in coordination with the Office of Security, shall designate copiers approved for reproduction of classified material. Ensure the equipment used for reproduction of classified information does not leave latent images in the equipment or on other material. The OIG Components and field activities where the copier is located shall ensure that the equipment is under constant surveillance by personnel responsible for enforcing the rules against unauthorized use or that the equipment is protected by safeguards approved by the Office of Security. Ensure the designated equipment has the proper classification markings via SF-707, which authorizes reproduction of secret materials and below. Coordination with the Office of Security is necessary for anything above Secret. Rules for reproduction of classified information shall be posted on or near the designated equipment. Run two blank sheets through copying machine at the conclusion of copying.

C. Facsimile Machine Controls. Some facsimile (fax) machines can be connected to the telephone system through a secure interface, such as the Secure Telephone Unit, Third Generation, (STU-III). These interfaces, accomplished IAW guidance issued by the National Security Agency (NSA), may be used for the transmission of classified faxes. The following controls are established for use of secure fax machines to transmit classified information:

1. The sender of a classified fax is responsible for verifying that the intended recipient/addressee has the appropriate security clearance and need-to-know. Further, the sender shall adhere to classification limitations displayed by the STU-III (or other equipment).

2 Transmission details shall be worked out by the sender before the actual transmission to ensure receipt of the classified fax by the intended recipient. In the case of transmitting Top Secret faxes, the sender shall ensure that the intended recipient is personally available to receive the fax. All Top Secret faxes received shall be taken to the TSCO for accountability.

3. Receipts for classified faxes shall be prepared by the sender and included with the transmission, executed by the recipient, and a signed copy faxed back to the sender.

4. The sender of a Top Secret fax is responsible for obtaining the consent of the originator of the Top Secret information to make a copy of the information that is inherent in the fax process.

5. Fax transmittal sheets shall be used for all fax transmissions. An Unclassified Facsimile Header Page is used for the transmission of unclassified material; a Secure Facsimile Header Page is used for the transmission of classified material and serves as the receipt.

6. When receiving a secure fax, account for all pages. The user of the fax machine shall ensure that no classified material is left in the fax machine and, that the STU-III Crypto Ignition Key (CIK) or Secure Terminal Equipment (STE) Fortezza Card is returned to secure storage.

CHAPTER 5 TRANSMISSION
SECTION 1 - METHODS OF TRANSMISSION OR TRANSPORTATION

A. Policy. Classified information may be transmitted or transported only as specified in this chapter. "Designated" as used in this chapter, means having been issued a DD Form 2501, *Courier Authorization*, (Appendix R). The procedures for completing the DD Form 2501 shall provide for accountability of the forms. The Office of Security shall issue all DD Forms 2501.

B. Top Secret Information. The Armed Forces Courier Service is now the Defense Courier Service (DEFCOS). For more guidance on using DEFCOS see reference (m). The Office of Security is the point of contact for issuing the courier service card. Transmission of Top Secret information shall be effected only by:

1. The DEFCOS.

2. Authorized DoD Component Courier Service.

3. If appropriate, the Department of State Courier System shall be used when transmitting any level of classified material or within foreign countries where the material might be subject to possible customs inspections or other examinations. The material shall be sent by an authorized means to the Chief, Diplomatic Mail and Pouch Branch, Department of State, Washington, DC 20520. The outer cover shall show the above address, and the inner cover shall show the address of the specific recipient.

4. Cleared and designated U.S. military personnel and government civilian employees by surface transportation.

5. Cleared and designated U.S. military personnel and government civilian employees on scheduled commercial passenger aircraft on flights outside the U.S., its territories, and Canada.

6 Cleared and designated DoD contractor employees within and between the U.S. and its territories provided that the transmission has been authorized in writing by the appropriate Cognizant Security Agency (CSA), and the designated employees have been briefed on their responsibilities as couriers and escorts for the protection for Top Secret material.

7. Cryptographic system authorized by the Director, NSA, or via a protected distribution system designed and installed to meet the standards included in the National COMSEC Instruction 4009. This applies to voice, data, message, and facsimile transmissions.

C. Secret and Confidential Information. Secret and Confidential information may be transmitted by:

1. U.S. Postal Service (USPS) Express Mail within and between the 50 States, the District of Columbia and the Commonwealth of Puerto Rico. The USPS Express Mail shall be used only when it is the most effective means to accomplish a mission within security, time, cost and

accountability constraints. To ensure direct delivery to the addressee, the "Waiver of Signature and Indemnity" block on the USPS Express Mail Label 11-B may not be executed under any circumstances. Secret USPS Express Mail shipments shall be processed through mail distribution centers or delivered directly to a USPS facility or representative. The use of external (street side) Express Mail collection boxes is prohibited.

2. GSA Contract Carrier. The GSA contract carrier(s) shall be used only when it is the most cost-effective way to meet program requirements, given time, security, and accountability restraints. The GSA contract carrier(s) may be used for the transmission of Secret and Confidential material only within CONUS. Secret material shall meet GSA contract carrier standard size and weight limitations. Under no circumstances should this mail be left unattended.

3. USPS Registered Mail Within and Between the U.S. and its Territories. USPS registered through the Army, Navy, or Air Force Postal Service activities outside the U.S. and its territories, provided that the information does not at any time pass out of U.S. control and does not pass through a foreign postal system or any foreign inspection.

4. Carriers authorized to transport Secret information by way of a Protective Security Service (PSS) under the DoD Industrial Security Program. This is only authorized within the U.S. boundaries. Routing for these shipments shall be obtained from the Military Traffic Management Command (MTMC).

5. Cleared and designated DoD contractor employees within and between the U.S. and its territories provided that the transmission has been authorized in writing by the appropriate contracting officer or his designated representative and the designated employees have been briefed on their responsibilities as couriers and escorts for the protection of Secret material.

6. Confidential information may be transmitted by means approved for the transmission of Secret information. The USPS registered mail shall be used for Confidential material to and from Fleet Post Office (FPO) and Army Post Office (APO) addresses located outside of the U.S. and its territories. USPS certified mail shall be used for Confidential material addressed to DoD contractors or non-DoD agencies. The USPS first class mail can also be used between DoD agency locations anywhere in the U.S. and its territories. If used, however, the outer wrapper shall be marked "POSTMASTER: Return Service Requested. Do Not Forward."

D. Accountable Mail. All custodians should ensure that accountable mail that is received as registered, certified from a GSA contract carrier (i.e., Federal Express), or unaccountable first class mail with the caveat "POSTMASTER: Address Correction Requested/Do Not Forward," is protected until its classification level is determined. All other first class mail, i.e., catalogs, vendor invoices, and personal mail that, using prudent judgment could not reasonably be expected to contain classified material is not required to be protected.

E. Transmission of Classified Material to Foreign Governments. To transmit classified material to a foreign government, obtain a signed receipt for all classified documentary information released. Show the complete unclassified title (or description of classified letter,

minutes of meeting, etc.) and the numerical identification (when used) of documents being released on the form. Use USPS registered mail to transfer Secret or Confidential material to an embassy, official agency, or designated representative of the recipient foreign government when they are located within the U.S.

CHAPTER 5
SECTION 2 - PREPARATION OF MATERIAL FOR TRANSMISSION, SHIPMENT, OR CONVEYANCE

A. Envelopes or Containers. Under no circumstances shall a SF-65, *U.S. Government Messenger Envelope* ("holey joe"), be used to transmit classified material. A GSA contract carrier envelope may be considered as the second envelope for purposes of double wrapping. When classified information is transmitted, it shall be enclosed in two opaque, sealed envelopes, wrappings or containers, durable enough to protect the material from accidental exposure or undetected deliberate compromise. Documents should be packaged so that classified text is not in direct contact with the inner envelope or container. When classified material is hand carried outside an activity, a locked briefcase may serve as the outer wrapper.

B. Addressing. Classified information shall be addressed to an official government activity or DoD contractor with a facility clearance and not to an individual. This is not intended, however, to prevent use of office codes or such phrases in the address as "Attention: Research Department," or similar aids in expediting internal routing.

1. The attention line of the address on the outer envelope shall appear as follows: "Attention: Security Office" (or "Officer") or "Document Control," as appropriate. When directing Secret or Confidential material to the attention of a particular member of an activity, the member's name may be indicated in an attention line on the inner envelope or container. The complete return address, including sender's office code, shall be placed on the inner and outer envelopes or containers. The outer envelope or container shall not bear a classification marking or any other unusual marks that might invite special attention to the fact that the contents are classified.

2. Classified material, under no circumstances, is to be mailed to the Senate or Congress. The Office of Communications and Congressional Liaison (OCCL) shall hand carry packages for congressional delivery.

C. Receipt System/SD Form 120

1. An SD Form 120 shall be used when transferring Top Secret, Secret, and Confidential information. The To, From, Classification, Date of Transfer, Description of Material Being Transferred, and number of copies blocks are mandatory items that shall be completed.

2. If the material is being mailed, the following procedures shall be followed:

   a. Separate the SD Form 120 before sealing the inner envelope.

   b. Keep the blue copy as the suspense for tracking the package.

c. Attach the pink and yellow copies directly onto the material (report) inside of the inner envelope (it is highly advisable to place a return address label on the back of the yellow copy).

d. Attach the white and green copies to the bottom left side of the outer envelope and record the receipt number on the envelope under the copies. The mailroom shall sign and remove the copies, keeping the green and providing the white copy to the courier.

3. When material is prepared for hand carrying to Congress, the following procedures shall be followed:

a. Keep the blue copy as the suspense for tracking the package.

b. Attach the green, pink, and yellow copies to the bottom left corner of the inner envelope (it is highly advisable to place a return address label on the back of the yellow copy.)

c. Attach the white copy to the bottom left corner of the outer envelope. The OCCL shall sign and remove the white copy, providing it to the courier.

4. When material is hand carried to locations other than the Congress, the following procedures shall be followed:

a. Keep the blue copy as the suspense for tracking the package.

b. Attach the remaining copies (white, green, pink, and yellow) to the outer envelope. The recipient shall retain the pink copy. The courier shall return the signed white, green, and yellow copies.

5. Receipts are also required for hand-to-hand transfer between OIG Components that are geographically separated. When an OIG Component receives a Secret document from outside the OIG, the recipient shall sign and date the receipt and return it to the sender as soon as possible. When the document is no longer needed, a record of disposition shall be kept for 2 years from the date of disposition (or destruction).

6. Receipt Forms. Any existing form may be used as a receipt for classified material if it adequately describes the material being transmitted. Developing new forms for this purpose is prohibited. Receipts shall include the following information:

a. To: Functional address and location

b. From: Functional address, location, and telephone number

c. Classification

d. Date of Transfer

e. Description of Material being transferred

f. Show the number of copies of each attachment and enclosure

g. Date material received

h. Signature of Recipient

7. Tracer Actions. When a signed receipt is not returned within 30 days in CONUS or 45 days outside of CONUS, tracer action should be taken immediately. This applies to all classified material, including that being transmitted by DEFCOS. A copy of the receipt should be reproduced and marked "TRACER--ORIGINAL NOT RECEIVED." If the recipient did not receive the classified information, notify the Office of Security.

8. Classified Information Released to Contractors. A SD Form 120 shall accompany all classified information released to contractors. The central office of record shall maintain one copy and another copy shall be forwarded to the appropriate contracting office for inclusion in the contract file.

CHAPTER 5
SECTION 3 - RESTRICTIONS, PROCEDURES, AND AUTHORIZATION CONCERNING ESCORT OR HAND CARRYING OF CLASSIFIED INFORMATION

A. General Restrictions. The OIG personnel are discouraged from hand carrying classified information on temporary duty (TDY), unless the information cannot be transmitted by other means. Hand carrying classified material is not authorized if other secure means of transmission are available. A DD Form 2501 is used to satisfy most policy requirements for written authorization to escort or hand carry classified material. The expiration date of the card shall not exceed 1 year from the date of issue. Personnel shall use an envelope, folder, or other closed container to prevent loss or observation of classified material hand carried outside of work areas. They should be provided with a written authorization when they are required to pass through an activity entry and exit inspection point to accomplish their classified information escort or hand carrying assignment.

B. Approval Process. The OIG personnel required to act as couriers of classified material shall submit a written Request for Approval to Escort or Hand Carry Classified Information Aboard Commercial Passenger Aircraft, (Appendix T), that shall be approved by their respective, designated approving authority. The DD Form 2501 shall be issued only to those personnel whose duties require routine hand carrying of classified material. The OIG personnel authorized infrequently to act as couriers for classified material shall be provided a Courier Pre-Departure Checklist, (Appendix U), in addition to the courier authorization letter issued prior to the trip. All couriers shall receive an initial briefing and shall be re-briefed annually on their responsibilities if the need for authorization remains valid. At a minimum, the courier briefing shall include information on the following:

1. Espionage and terrorist threats.

2. Proper receipting and control procedures.

3. Physical protection, wrapping, and storage procedures.

4. Procedures to be taken in an emergency.

C. Procedures for Hand Carrying Classified Information Aboard Commercial Passenger Aircraft. The OIG Component Heads, Program Managers, and Special Agents In Charge of OIG field activities are designated approval authorities for authorizing personnel to hand carry classified information aboard commercial passenger aircraft, to include international flights. These officials shall be referred to collectively as Designated Officials.

1. Local procedures established to justify TDY abroad shall require that the request for travel contain a written statement by the traveler that classified information will or will not (as applicable) be disclosed during the trip.

2. If the foreign disclosure of classified information is involved, an additional written statement shall advise that disclosure authorization has been obtained IAW reference (n). The statement also shall specify whether authorization has been obtained to carry classified material in compliance with reference (b).

3. If the traveler has been authorized to carry classified material, a copy of the written authorization shall accompany the justification for the TDY. Block 16 of DD Form 1610, *Request and Authorization for TDY Travel of DoD Personnel*, shall contain the following statements:

a. "Traveler is (or is not, as applicable) authorized to disclose classified information."

b. "Traveler is (or is not, as applicable) authorized to carry classified material."

c. "Traveler is aware of applicable export control, foreign disclosure, and security requirements."

d. In addition to the above, the name and telephone number of the Office of Security shall be entered in Item 16 of the DD Form 1610. The Chief, Office of Security, or Administrative Officer shall apply his or her signature, thus indicating that the traveler has complied with the above requirements.

4. International Flights. Travelers who are authorized to carry classified material on international flights shall have courier orders because DD Form 2501 is not valid for overseas travel. The traveler shall be informed of and acknowledge security responsibilities. This requirement, at a minimum, may be satisfied by a briefing or by requiring the traveler to read written instructions that contain the information listed below. The traveler shall be held liable and responsible for the material described in the courier certificate. Throughout the journey, the classified consignment must stay in the personal possession of the traveler, except when it is in authorized storage. The classified material is not to be discussed or disclosed in any public place. The classified material is not, under any circumstances, to be left unattended. During overnight stops, U.S. military facilities or embassies shall be used. Classified material may not be stored in hotel safes. The traveler shall not deviate from the authorized travel schedule. In cases of emergency, the traveler shall take measures to protect the classified material. The traveler's security manager shall provide appropriate guidance. The traveler is responsible for ensuring that personal travel documentation (passport, courier authorization, and medical documents, etc.) are complete, valid, and current.

5. Dealing with Customs, Police, and Immigration Officials. There is no assurance of immunity from search by the customs, police and/or immigration officials of the various countries whose borders the traveler will cross. Should such officials inquire as to the contents of the consignment, the traveler shall present the courier orders and ask to speak to the senior customs, police, and/or immigration official. This action should normally suffice to pass the material through unopened. If the senior customs, police, and/or immigration official demands to see the actual contents of the package, it may be opened in his or her presence, but should be done in an area out of sight of the general public. Precautions should be taken to show officials

only as much of the contents as will satisfy them that the package does not contain any other item. The traveler should ask the official to repack or assist in repackaging it immediately upon completion of the examination. The senior customs, police, and/or immigration official should be requested to provide evidence of the opening and inspection of the package by signing it when closed and by confirming on the shipping documents (if any) or courier certificate that the package has been opened. If the package has been opened under such circumstances as the foregoing, the addressee and the dispatching security manager shall be informed in writing. Classified material to be carried by a traveler shall be inventoried, a copy of the inventory shall be retained by the traveler's security office, and the traveler shall carry a copy. The material shall be double wrapped, marked, and sealed as specified in reference (b).

6. Travel Orders. Travel orders shall identify the traveler by name, title, and organization and include the traveler's passport or identification number. The orders shall describe the route to be taken by the traveler (the traveler's itinerary may be attached for this purpose); describe the package to be carried (size, weight, and configuration); and contain the name, title, and telephone number of the responsible OIG Component security manager who signed the orders. Upon completion of the trip, the traveler shall return all classified material, appropriately packaged, or produce a signed receipt for any material that is not returned.

D. Courier Authorization Procedures

1. General

a. As a courier, you are responsible for protecting and safeguarding the classified defense information entrusted to you from unauthorized disclosure and compromise. While it is unlikely that you as a courier will be assaulted and the material in your possession removed by force, it is possible that you could find yourself in a hostage situation or confronted with a terrorist incident. In light of this danger, you must be aware of the action required to fulfill your responsibility as a courier of classified information.

b. Because of the danger of unauthorized disclosure, hand carrying of classified material is discouraged and should be resorted to only when time constraints preclude transmission through authorized channels.

2. Preparation

a. Before departure, you must submit to your Security Manager a list of all classified information to be hand carried, a copy of your itinerary, and approved storage arrangements en route and at your destination. Upon arrival, go directly to the approved storage facility to deliver or store the material.

b. You must be in possession of a DD Form 2501, *Courier Authorization Card*, or possess a courier letter authorizing you as a courier for the highest level of classified material to be transported. When traveling by commercial airlines within CONUS, the U.S. territories and

Canada, a courier authorization letter shall be prepared and signed by the official signing your TDY orders. Block 16 of DD Form 1610, *Request and Authorization for TDY Travel of DoD Personnel*, shall contain the following statements for travel abroad:

(1) "Traveler is authorized to disclose classified information."

(2) "Traveler is authorized to carry classified material."

(3) "Traveler is aware of applicable export control, foreign disclosure and security requirements."

(4) The name and telephone number of the security manager shall be entered in Item 16 of the DD Form 1610; the security manager shall apply his or her signature, thus indicating that the traveler has complied with the above requirements.

(5) If foreign disclosure of classified information is involved, there shall be an additional written statement that disclosure authorization has been obtained IAW reference (n).

c. If traveling overseas, a memorandum to the appropriate approving authority through the Office of Security requesting a waiver from DoD regulations prohibiting hand carrying classified material aboard commercial shall be prepared.

d. The material shall be enclosed in two opaque wrappings in such a manner that the classified text does not directly contact the inner wrapping. The material used for wrapping must be of such strength and durability as to provide security protection while in transit, prevent items from breaking out of the container, and permit detection of all evidence of tampering. The wrapping must conceal all classified characteristics. When transported on commercial aircraft, each package shall bear the signature of the official who signed the courier authorization.

(1) The outer label of the package shall contain the correct address of an official U.S. Government activity or DoD contractor, with the proper facility clearance and safeguarding capabilities, and your return address. The outer wrapping shall not bear an individual's name, a classification, a listing of the contents divulging classified information, or any other unusual data or markings that might invite special attention to the fact that the contents are classified.

(2) The inner label of the package shall also bear the correct address and return address but can designate an individual. The inner wrapping shall be stamped with the highest classification level of classified material contained in the package; i.e., CONFIDENTIAL, SECRET, or TOP SECRET. The inner wrapping shall also be marked with special handling requirements. If the material is of a special nature, the statement, "TO BE OPENED ONLY BY" and the individual's name or title should be marked on the inner wrapping.

e. Classified information shall not be hand carried aboard commercial passenger aircraft unless there is neither time nor means available to move the information in the time required to accomplish objectives or contract requirements, including Requests for Quotation (RFQ) and/or Requests for Bid (RFB).

(1) When classified information is hand carried across international borders, prior arrangements should be made by you as the requester to ensure the information shall not be opened by customs, border, postal, or other inspectors, either U.S. or foreign.

(2) Ensure that the classified information carried contains no metal bindings and is contained in sealed envelopes.

(3) Ensure you have obtained the following documentation:

(a) An official ID card issued by a U.S. Government agency that carries photograph, descriptive data, and signature. (If the identification card does not contain date of birth, height, and weight, these items are included on the written authorization.)

(b) Original letters authorizing you to carry classified information. Reproduced copies are not acceptable. You must have a sufficient number of original signed letters to provide to each airline involved.

3. <u>En Route</u>

a. The classified package shall be placed in approved storage (a hotel safe is not approved storage) at all stops en route to the destination, unless the information is retained in your possession and under your constant surveillance at all times. Hand carrying classified information on trips that involve an overnight stopover is not permissible unless you have made advance arrangements for proper overnight storage at a U.S. Government installation or a cleared contractor facility.

b. Classified material shall not be read, studied, displayed, or used in any manner in public conveyances or places. When traveling on a public conveyance, keep the package in hand or in contact with your body so that you will immediately be aware if it moves or is removed. If you leave your seat temporarily while in a public or private conveyance, you must carry the package with you. A locked car or its trunk, hotel or room, transportation terminal locker, etc., are not approved classified security containers.

c. When you transport classified material via private, public, or Government conveyance, you cannot store it in any detachable storage compartment, such as automobile trailers, luggage racks, aircraft travel pods, or drop tanks.

4. <u>Arrival</u>

a. Upon arrival at your destination, you must go directly to the approved facility to deliver or store your material. If you deliver the material to someone, **be sure to get a signed package receipt**. It is your responsibility to verify that the recipient has the proper clearance

and to notify him or her of the highest level of classified material in the package before releasing it. Whether departing or returning to the Agency, **classified materials must not be stored at home.** If you return during non-duty hours with classified material, it must be stored in your office safe.

b. On TDY, if you must pass through customs upon your arrival, you usually will not be challenged if traveling with your official passport. If you are challenged, explain that you are an official U.S. courier, show the agent your courier authorization document and your orders, and point out the section that designates you as a courier. If this does not gain you entrance, ask to speak to the Senior Customs Official and repeat the above. If this fails, contact U.S. authorities for assistance (U.S. State Department officials). While telephoning for aid, **do not** leave your package in the hands of the Customs agents. Before resorting to calling local U.S. authorities, be sure of the exact requirements or wishes of the Customs agent's intended inspection. If he or she only wants to look at your package and it is properly wrapped, you may permit that. Under no circumstances shall the official be allowed visual access to the actual classified material.

5. Terrorism

a. Terrorism is defined as “the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Espionage is the act or practice of spying to obtain secret intelligence. Therefore, no person is immune and an employee’s position in a DoD agency makes him or her a possible target. Individual alertness, knowledge, and preparation for possible attempts are proven deterrents to such acts.

b. Everyone should be sensitive to possible surveillance. Avoiding predictable patterns and routines is one of the best individual means of protection against attacks.

c. If an employee suspects he or she is being followed, drive to the nearest safe location, such as a police station, fire station, or shopping center and ask for help.

d. When traveling overseas, do not travel in uniform if possible. Obtain any necessary foreign currency and/or traveler's checks before leaving, avoid corner “money changers” and displaying currency. Do not transport weapons or facsimiles of them, alcohol, other than legally allowed beverages, narcotic substances (if needed for health reasons, take a prescription for each drug), prohibited books and publications, fireworks or other explosives, or aerosol tear gas even though it may be legal in certain areas. Restrict knowledge of an itinerary to office and family. If a change in travel plans occurs, employees shall immediately notify his or her office and any office that might be expecting him or her.

e. If employees encounter trouble remain calm and attempt to withdraw without being noticed. If an employee is in the U.S., contact his or her security office. If abroad, contact the U.S. embassy or consulate. If no official U.S. representative is available, normally representatives from Australia, Canada, the United Kingdom or another friendly country will

help. Employees shall consult a consulate if they are a crime victim, if the authorities arrest them, or if they are injured or ill and hospitalized. Contact the local authorities if deemed necessary by the official consulate representatives. Finally, employees should notify the local security office.

CHAPTER 6
DISPOSAL AND DESTRUCTION

A. Policy. Classified documents and other material shall be retained only if they are required for effective operation of the organization or if law or regulation requires their retention. Documents that are no longer required shall be destroyed or disposed of IAW the provisions of the Federal Records Act and other OIG guidance. Destruction of classified documents shall be accomplished by means that eliminate risk of reconstruction of the classified information they contain.

B. Destruction of Material. The OIG has available two approved methods of destroying classified material. They are shredding and burning.

1. Shredders. Approved cross-cut shredders shall be used to destroy classified information. When shredding controlled documents, an IG Form 5200.1-10, *Classified Material Destruction Certificate*, (Appendix V), is required. Signatures are required from two staff members (shredder and witness) when shredding Top Secret material and one signature is required when shredding Secret and Confidential material. Approved shredders have a cross-cut of 1/2 x 1/32 or smaller and only shredders listed on the NSA Evaluated Product List for High Security Cross-Cut Shredders shall be used for the terminal destruction of classified paper-based material and documents. Any cross-cut shredders requiring replacement of the unit and/or rebuild of the shredder blades assembly shall be replaced by a cross-cut shredder on the latest NSA evaluated products list. This list may be obtained by calling the NSA National Information Assurance Service Center at 1-800-688-6115.

2. Burn Bags. Classified material shall be disposed of in red and white striped burn bags. Burn bags shall be marked to indicate the level of protection they require before destruction. Burn bags shall also be marked with a office code, room number, telephone number, and date. Burn bags are picked up at 400 Army Navy Drive on Tuesdays from 10:15 a.m. to 10:20 a.m. at the loading dock. Collection at Crystal Gateway North is on Tuesday from 9:35 a.m. to 9:45 a.m. at the loading dock. A DD Form 2843, *Classified Material Destruction Record*, (Appendix W), shall be filled out and a copy provided to the person picking up the burn bags. One copy of DD Form 2843 shall be retained by the OIG Component. The receipt is proof that the document has been burned and should be retained with classified document registers.

3. Destruction of FOUO and PA Information. As defined by DoD guidance, FOUO and PA information may be destroyed by "tearing each copy into pieces to preclude reconstruction or by shredding."

4. Other Material. Certain occasions may necessitate the destruction of classified or unclassified computer diskettes. This should be accomplished only when the diskette cannot be overwritten or if degaussing is impractical or unavailable. Computer diskettes should be disposed of in the following manner:

a. Classified diskettes shall be placed into burn bags marked “plastic.” The number of diskettes, at any given time, shall be kept to a minimum, and whole batches of diskettes shall not be dumped into a burn bag. This is because the coating on the diskettes produces toxic fumes when burned and can present a health hazard to the personnel operating the incinerators in which burn bags are destroyed.

b. Unclassified diskettes may be discarded with regular unclassified waste. That is, they may be placed into a regular office trashcan. The integrity of the diskette should be destroyed by cutting in half with scissors (for 5 1/4" diskettes) and bending in half or actually breaking (for 3 1/2" diskettes).

c. Classified media shall be disposed and destroyed IAW the procedures described in the following paragraphs.

(1) Destruction of Hard Drives. Destruction of classified OIG hard drives shall occur at the NSA physical destruction office, Fort Meade, Maryland. Procedures for sending classified hard drives to NSA are available from the Office of Security.

. (2) Destruction of Expendable Media. Expendable media (e.g., magnetic tapes and diskettes) classified up to and including Top Secret shall be placed in a burn bag and mixed with other classified waste. The burn bag shall be disposed with other classified waste. Plastic sleeves shall not be placed in the burn bag and the plastic disk shall be removed and cut in half before placing in the bag.

(3) Destruction of SCI Media. Destruction of SCI media shall occur IAW DIA policy. Contact the Special Security Officer (SSO) for additional information on the destruction of SCI information.

(4) Destruction of SAP Media. Destruction of SAP media shall occur IAW the SAP classification guidance. Contact the OSD-level SAP Central Office for additional guidance.

(5) Destruction of CD-ROMs. It is not required that unclassified CD-ROMs be “scratched” before they are sent to the destruction/recycling facility. The OIG Components wishing to destroy Sensitive But Unclassified (SBU) and FOUO CD-ROMs may still send them to the NSA CD-ROM destruction facility. Classified CD-ROMs shall be destroyed using the NSA approved destruction method of controlled incineration, which meets environmental standards. The NSA accepts not only classified CD-ROMs, but also SBU and FOUO CD-ROMs. Procedures for mailing classified CD-ROMs to NSA are available from the Office of Security.

C. <u>Annual Clean-Out Day</u>. The OIG has designated the month of December as the time when Components can select a date designated for their annual clean-out day. The number of cubic feet of classified material destroyed shall be calculated and reported to the Office of

Security for consolidation. (One cubic foot equals 2,500 pages; one safe drawer equals approximately 3 cubic feet or 7,500 pages.) Suspense date for reports to the security office is January 15 of each year. If the 15th falls on a weekend, the reports shall be due the next working day.

CHAPTER 7
SECURITY EDUCATION

A. Responsibility and Objectives. All OIG Components and field activities shall ensure that the requirements of this chapter are implemented within their respective OIG Components.

B. Scope and Principles. The scope of each security education program depends on the mission, functions of the activity, and the degree of involvement with classified material.

C. Security Education. The effectiveness of the OIG Security Program is proportional to the degree employees understand their responsibilities within the program. An integral part of the program is security education. To ensure that personnel become aware of their responsibilities, security education training is provided through the following briefings:

1. **Initial Briefings**

a. Personnel granted a security clearance are not permitted access to classified information until they are briefed on the requirements of safeguarding classified information and sign a NDA. The Human Capital Advisory Services (HCAS) Directorate shall conduct the briefings for employees located within the NCR. The manager of OIG field offices shall ensure the briefings are conducted and documented. The completed NDA shall be returned to the Office of Security for filing in the employee's Official Personnel Folder. Refusal to sign the agreement shall result in access denial and clearance revocation.

b. Supervisors shall personally brief new employees on their individual security responsibilities. The briefing shall be tailored to meet the employee's specific job requirements and shall be accomplished within 30 days of assignment.

c. The Office of Security shall conduct mandatory security indoctrination for incoming personnel assigned within the NCR. For personnel located outside the NCR, the office manager shall conduct the briefing.

2. **Refresher Briefings.** The Office of Security conducts annual refresher briefings for personnel in the NCR. The manager of OIG field offices shall conduct the briefings for field personnel and forward certificates of completion to the Office of Security. This training reacquaints the employee with the responsibilities for the various requirements for handling classified information and other elements of the Personnel Security Program. This is also conducted online at https://intra.dodig.mil/.

3. **Foreign Travel Briefings.** The OIG personnel are required to report all foreign travel to the Office of Security. Before traveling overseas, you must also receive a country-specific AOR threat briefing. The initial Level I awareness training is conducted in person at the Pentagon Library Conference Center the first Tuesday of the month from 12:00 p.m. 1:30 p.m.

Attendees shall receive a certificate upon completion. A copy of the certificate shall be given to the Office of Security to obtain credit. Annual Antiterrorism Level I Awareness training can be taken online at https://atlevel1.dtic.mil/at/. The access code word is **aware.**

4. **Termination Briefings**

a. Military personnel and civilian employees receive a termination briefing when:

(1) Assignment and/or employment are terminated.

(2) A contemplated absence from duty or employment shall last for 60 days or more.

(3) Access to classified and/or sensitive unclassified information is suspended.

b. When any of those reasons apply, employees assigned within the NCR shall report to the Office of Security to sign an IG Form 5200.2-1, *Security Termination Statement*, (Appendix X). The managers of OIG field offices shall ensure the briefings are conducted, documented, and ensure that the completed form is returned to the Office of Security.

c. If an employee refuses to execute a Security Termination Statement, an oral debriefing shall be given in the presence of a witness and documented on IG Form 5200.2-1. The briefer and witness shall sign beneath the statement attesting to the action and the completed form shall be forwarded to the Office of Security. The refusal to sign a Security Termination Statement shall be recorded in the Defense Central Index of Investigations (DCII) and the JPAS database.

CHAPTER 8
COMPROMISE OF CLASSIFIED INFORMATION

A. Policy. To determine the circumstances of occurrence, a preliminary inquiry is immediately initiated into incidents of compromise, possible compromise, possible loss of classified information, or an infraction of the safeguarding controls as established by this Instruction. A formal investigation shall be conducted into complex incidents or those of serious consequence. Initially, these incidents are referred to as information security incidents. In the course of the inquiry or investigation, the incident shall be categorized as:

1. Compromise. The disclosure of classified information to persons not authorized access thereto.

2. Possible Compromise. A security incident in which a reasonable presumption exists that an unauthorized person had or has access to classified information.

3. Inadvertent Access. A security incident in which a person who is the subject of a favorable personnel security investigation had access to classified material for which he or she was not technically authorized to have or did not have a need to know.

4. Security Deviation. An incident that involves the misuse or improper handling of classified material but does not fall in the category of compromise, possible compromise or inadvertent access.

B. Purpose of Inquiry or Investigation. The purpose of an inquiry or investigation is to determine:

1. Whether or not a security incident has occurred.

2. The source and reason for the security incident.

3. Appropriate measures or actions to minimize or negate the adverse effect of the security incident.

4. The seriousness of damage to U.S. interests. (An OCA's damage assessment determines the seriousness of damage. Damage assessments are conducted when there is a reasonable expectation of damage to national security. The content of the inquiry or investigation report establishes a need, as applicable, for the OCA to conduct a damage assessment.)

5. Identify vulnerabilities in the security program that could result in similar incidents in the future.

C. Debriefings in Cases of Unauthorized Access. In cases where a person has had unauthorized access to classified information, it may be advisable to discuss the situation with the individual to enhance the probability that he or she shall properly protect it. The OIG Component Head or responsible security officials shall decide whether such a discussion, commonly called a "debriefing" is held. This decision shall be based on the circumstances of the incident, what is known about the person or people involved, and the nature of the classified information. The following guidelines apply:

1. If the unauthorized access was by a person with the appropriate security clearance, but no need-to-know, a debriefing is usually unnecessary. A debriefing may be required if the individual is not aware that the information is classified and needs protection.

2. If the unauthorized access was by a Government employee or military member without the appropriate security clearance, a debriefing is appropriate. The person should be advised of the responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties that might follow if he or she fails to do so. The debriefing official should make sure the individual understands what classified information is, why its protection is important, and what to do should someone try to obtain the information. If the person who had unauthorized access is an employee of a contractor participating in the National Industrial Security Program, the same guidelines apply as for government employees.

D. Responsibility of Discoverer. If classified information appears in the public media, OIG personnel are cautioned not to make any statement or comment that would confirm the accuracy or verify the classified status of the information. If approached by a representative of the media who wishes to discuss information believed to be classified, individuals should neither confirm nor deny the accuracy of the information and should report the situation immediately to the appropriate security and public affairs authorities.

E. Appointment of Preliminary Inquiry Officer. Upon notification of a security incident, the Office of Security shall coordinate with the OIG Component Heads in appointing a Preliminary Inquiry Officer (PIO) in writing. The Office of Security shall be provided the name, office code, and telephone number of the PIO within 5 working days from the date of the requesting memorandum. The following individuals shall take action after a security incident is reported:

1. The **Appointing Official** shall:

a. Appoint a PIO to conduct an expeditious, thorough inquiry or investigation whenever a security incident occurs. (The person appointed to conduct the inquiry shall have an appropriate security clearance, shall have the ability and available resources to conduct an effective inquiry, and shall not have been involved, directly or indirectly, in the incident. Except in unusual circumstances, the activity Security Manager should not be appointed to conduct the inquiry.) Approve/disapprove extensions if the PIO cannot meet the set suspense date and provide a courtesy copy of the extension approval to the Office of Security.

b. Ensure any proposed disciplinary action is coordinated with the HCAS to determine whether the individual involved in the incident has any record of previous security violations. Any disciplinary action proposed against civilian employees is referred to the Workforce Relations Division. Proposed disciplinary action against military members shall be coordinated with the Director, HCAS; the AIG-A&M; and the Chief, Office of Security, and shall comply with the provisions of the Uniform Code of Military Justice. Proposed disciplinary action against contractor personnel shall be coordinated with the Industrial Security Program Manager, Office of Security.

2. The **PIO** shall:

a. Obtain a briefing from the Security Manager to receive initial facts and evidence surrounding the incident.

b. Consult with the Office of Security for technical guidance in conducting the inquiry.

c. Prepare and forward, within 15 working days, a report that shall include, at a minimum, the following sections:

(1) Authority. State when, where, and by whom the inquiry was conducted.

(2) Classification of Material. What specific classified information and/or material was involved? What was the level of classification?

(3) Personnel Interviewed. List all personnel who were interviewed. Include their rank or grade, full name, duty title or functional address, and security clearance level.

(4) Facts. When, where, and under what circumstances did the incident occur? Exactly what happened? (Arrange in chronological order.)

(5) Conclusions

(a) Brief summary of conclusions reached after a review of all pertinent information. Conclusions shall be supported by the facts, and the evidence obtained during the inquiry process shall support the facts.

(b) What was (were) the cause(s)? What persons, situations or conditions caused or contributed to the incident?

(c) Possibility of Compromise. Did compromise of classified information occur? If so, can damage to national security be expected? Every inquiry into compromise or possible compromise of classified information shall include a judgment about whether compromise occurred and about the potential damage to national security. One of the following alternatives shall be chosen:

1 Compromise of classified information did not occur.

2 Compromise of classified information may have occurred.

3 Compromise of classified information did occur, but there is no reasonable possibility of damage to the national security.

4 Compromise of classified information did occur and damage to national security may result.

5 Recommendation. Suggested corrective action to prevent future incidents.

F. Handling Instructions. The PIO shall mark each page "FOR OFFICIAL USE ONLY" unless the report contains classified material, then mark accordingly. Route the report through the Office of Security for a technical review and further processing.

CHAPTER 9
PROTECTING UNCLASSIFIED INFORMATION

A. General. In addition to classified information, there are certain types of unclassified information that require application of controls and protective measures for a variety of reasons. The protective measures specifically delineated in this chapter are the only protective measures authorized to be applied to such information. This chapter also addresses the use of distribution statements on both classified and unclassified technical documents as a means to facilitate control, distribution, and release of such documents.

B. For Official Use Only Information

1. Description. FOUO is a designation applied to unclassified information that may be exempt from mandatory release to the public under the FOIA. The FOIA specifies nine exemptions that may qualify certain information from release to the public, if, by its disclosure, a foreseeable harm would occur. They are:

a. Exemption 1. Information that is currently and properly classified.

b. Exemption 2. Information that pertains solely to the internal rules and practices of the agency. (This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)

c. Exemption 3. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute shall clearly state that the information shall not be disclosed.

d. Exemption 4. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness.

e. Exemption 5. Inter-agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions, and recommendations.

f. Exemption 6. Information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

g. Exemption 7. Records or information compiled for law enforcement purposes that:

(1) Could reasonably be expected to interfere with law enforcement proceedings;

(2) Would deprive a person of a right to a fair trial or impartial adjudication;

(3) Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others;

(4) Disclose the identity of a confidential source;

(5) Disclose investigative techniques and procedures; or

(6) Could reasonably be expected to endanger the life or physical safety of any individual.

h. Exemption 8. Certain records of agencies responsible for supervision of financial institutions.

i. Exemption 9. Geological and geophysical information concerning wells.

2. Application

a. Information that is currently and properly classified can be withheld from mandatory release under the first exemption category. FOUO is applied to information that is exempt under one of the other eight categories. So, by definition, information must be unclassified in order to be designated FOUO. If an item of information is declassified, it can be designated FOUO if it qualifies under one of those other categories. This means that:

(1) Information cannot be classified and FOUO at the same time. Therefore, classified documents containing FOUO information cannot bear an overall document marking of FOUO. However, portions or pages of a classified document, that contain only FOUO information shall be marked as FOUO.

(2) Information that is declassified may be designated FOUO, but only if it fits into one of the last eight exemption categories (categories 2 through 9).

b. The FOIA provides that, for information to be exempt from mandatory release, it must fit into one of the qualifying categories and there must be a legitimate Government purpose served by withholding it. Simply because information is marked FOUO does not mean it automatically qualifies for exemption. If a request for a record is received, the information shall be reviewed to see if it meets this dual test. On the other hand, the absence of the FOUO marking does not automatically mean the information shall be released. Some types of records, e.g., personnel records, are not normally marked FOUO, but may still qualify for withholding under the FOIA. All DoD unclassified information shall be reviewed before it is released to the public or to foreign governments and international organizations.

3. Markings

a. Marking information FOUO does not automatically qualify it for exemption. If a request for a record is received, the information shall be reviewed to determine if it actually qualifies for exemption, Information that has been determined to qualify for FOUO status shall be indicated by markings. Markings are to be applied at the time documents are created to promote proper protection of the information.

b. Unclassified documents and material containing FOUO information shall be marked as follows:

c. Documents shall be marked "FOR OFFICIAL USE ONLY" at the bottom of the front cover (if there is one), the title page, the first page, and the outside of the back cover (if there is one.)

d. Internal pages of the document that contain FOUO information shall be marked "FOR OFFICIAL USE ONLY" at the bottom.

e. Subjects, titles and each section, part, paragraph, and similar portion of an FOUO document shall be marked to show that they contain information requiring protection. The parenthetical notation "(FOUO)" shall be used to identify information as FOUO for this purpose. This notation shall be placed immediately before the text.

f. Material other than paper documents, e.g., slides, computer media, films, as well as information in electronic form to include e-mail, shall bear markings that alert the holder or viewer that the material contains FOUO information.

g. Classified documents and material containing FOUO information shall be marked as follows:

h. No additional special markings are required on the face of the document because it contains FOUO information.

i. If there are unclassified portions that contain FOUO information, the portion shall be marked "FOUO" in parentheses at the beginning of the portion. Since FOUO information is, by definition, unclassified, "FOUO" is an acceptable substitute for the normal "U."

j. Pages that contain FOUO information but no classified information shall be marked "FOR OFFICIAL USE ONLY" at the top and bottom.

k. Transmittal documents that have no classified material attached, but do have FOUO attachments shall be marked with a statement similar to this one: "FOR OFFICIAL USE ONLY ATTACHMENT."

l. Each part of electrically transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation "FOUO" before the beginning of the text.

4. Access to FOUO Information

a. No person may have access to information designated as FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized government purpose.

b. The final responsibility for determining whether an individual has a valid need for access to information designated as FOUO rests with the individual who has authorized possession, knowledge, or control of the information and not on the prospective recipient.

c. Information designated as FOUO may be disseminated within DoD Components and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the DoD, provided that dissemination is not further controlled by a Distribution Statement.

d. DoD holders of information designated as FOUO are authorized to convey such information to officials in other departments and agencies of the Executive and Judicial Branches to fulfill a government function, except to the extent prohibited by reference (f).

e. Release of FOUO information to Members of Congress is governed by reference (o).

f. Release of FOUO information to the General Accountability Office (GAO) is governed by reference (p).

5. Protection of FOUO Information

a. During working hours, reasonable steps shall be taken to minimize risk of access by unauthorized personnel. After working hours, FOUO information shall be stored in unlocked containers, desks or cabinets if government or government-contract building security is provided. If such building security is not provided, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, etc.

b. FOUO information and material may be transmitted via first class mail, parcel post or - for bulk shipments – via fourth-class mail. Electronic transmission of FOUO information, e.g., voice, data or facsimile, e-mail, should be by approved secure communications systems or systems using other protective measures such as Public Key Infrastructure (PKI), whenever practical.

c. FOUO information may only be posted to DoD Web sites consistent with security and access requirements specified in the Deputy Secretary of Defense Memorandum, *Web Site Administration*, December 1998.

d. Record copies of FOUO documents shall be disposed of IAW reference (g) and Component records management directives. Non-record FOUO documents may be destroyed by any of the means approved for the destruction of classified information, or by any other means that would make it difficult to recognize or reconstruct the information.

6. FOUO Information Containing Privacy Information. Additional guidance pertaining to the protection of FOUO information that contains information protected under the PA can be found in reference (q).

C. Sensitive Information

1. Description. Reference (r) established requirements for protection of certain information in Federal Government AISs. This information is referred to as "sensitive" information, defined in the act as: "Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under reference (f), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense of foreign policy."

2. Application. Two aspects of sensitive information deserve attention. First, the Act applies only to unclassified information that deserves protection. Second, unlike most other programs for protection of information, the Act is concerned with protecting the availability and integrity, as well as the confidentiality of information. Much of the information that fits the Act's definition of "sensitive" falls within one of the other protective categories delineated in this chapter.

3. Markings. Unclassified information that qualifies for protection under one of the protection categories delineated in this chapter shall, when placed on AIS systems, be marked IAW the marking prescribed for the particular protective category involved.

4. Access to Sensitive Information. If sensitive information falls within one of the other protective categories described in this Chapter, the specific limitations on access for the appropriate category shall be applied. If it does not, as a minimum, access to the information shall be limited to those persons that have been determined by a cognizant security authority to have a valid need for such access in connection with the accomplishment of a lawful and authorized government purpose.

5. Protection of Sensitive Information. Information on DoD AIS systems shall be protected consistent with the provisions of this chapter, reference (s), and related publications.

D. Other Authorized Designations

1. Sensitive But Unclassified and Limited Official Use Only

a. Description. Within the DoD, the criteria for allowing access to SBU information are the same as those used for FOUO information, except that information received from the Department of State marked SBU shall not be provided to any person who is not a U.S. citizen without the approval of the Department of State activity that originated the information.

b. Markings. The Department of State does not require that SBU information be specifically marked, but does require that holders be made aware of the need for controls. When SBU information is included in DoD documents, they shall be marked as if the information were FOUO. There is no requirement to re-mark existing material containing SBU information.

c. Access. Within the DoD, the criteria for allowing access to SBU information are the same as those used for FOUO information.

d. Protection of SBU Information. Within the DoD, SBU information shall be protected as required for FOUO information.

2. FOR OFFICIAL USE ONLY Law Enforcement Sensitive

a. Description. Law Enforcement Sensitive is a marking sometimes applied, in addition to the marking FOR OFFICIAL USE ONLY, by the Department of Justice and other activities in the law enforcement community. It is intended to denote that the information was compiled for law enforcement purposes and should be afforded appropriate security in order to protect certain legitimate government interests, including the protection of: enforcement proceedings; the right of a person to a fair trail or an impartial adjudication; grand jury information; personal privacy including records about individuals requiring protection under the PA; the identity of a confidential source, including a State, Local, or foreign agency or authority or any private institution which furnished information on a confidential basis; information furnished by a confidential source; proprietary information; techniques and procedures for law enforcement investigations or prosecutions; guidelines for law enforcement investigations when disclosure of such guideline could reasonably be expected to risk circumvention of the law, or jeopardize the life or physical safety of any individual, including the lives and safety of law enforcement personnel.

b. Markings

(1) In unclassified documents containing Law Enforcement Sensitive information, the words “Law Enforcement Sensitive” shall accompany the words “FOR OFFICIAL USE ONLY” at the top and bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one).

(2) In unclassified documents, each page containing FOR OFFICIAL USE ONLY Law Enforcement Sensitive information shall be marked “FOR OFFICIAL USE ONLY Law

Enforcement Sensitive" at the top and bottom. Classified documents containing such information shall be marked as required by reference (b) except that pages containing Law Enforcement Sensitive information but no classified information shall be marked "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" top and bottom.

(3) Portions of DoD classified or unclassified documents that contain FOR OFFICIAL USE ONLY Law Enforcement Sensitive information shall be marked "(FOUO_LES)" at the beginning of the portion. If a portion of a classified document contains both classified and FOR OFFICIAL USE ONLY Law Enforcement Sensitive information, the appropriate classification designation is sufficient to protect the information.

c. Access

(1) The criteria for allowing access to FOR OFFICIAL USE ONLY Law Enforcement Sensitive are the same as those used for FOUO information.

d. Protection

(1) Within the DoD, FOR OFFICIAL USE ONLY Law Enforcement Sensitive shall be protected as required for FOUO information.

3. LIMITED DISTRIBUTION Information

a. Description. LIMITED DISTRIBUTION is a caveat used by the National Geospatial-Intelligence Agency (NGA) to identify a select group of SBU imagery or geospatial information and data created or distributed by NGA or information, data, and products derived from such information. Reference (x) contains details of policies and procedures regarding use of the LIMITED DISTRIBUTION caveat.

b. Marking. Information or material designated as LIMITED DISTRIBUTION, or derived from such information or material shall, unless otherwise approved by the Director, NGA, be marked as follows:

LIMITED DISTRIBUTION Notation

UNCLASSIFIED/LIMITED DISTRIBUTION
Distribution authorized to DoD, IAW 10 U.S.C. §§ 130
and 455. Release authorized to U.S. DoD Contractors
IAW 48 C.F.R. §252.245-7000. Refer other requests to
Headquarters, NGA, ATTN: Release Officer, Stop D-136.
Destroy as "For Official Use Only." Removal of this
Caveat is prohibited.

c. Access

(1) Information bearing the LIMITED DISTRIBUTION caveat shall be disseminated by NGA to Military Departments or other DoD Components, and to authorized grantees for the conduct of official business.

(2) DoD civilian, military and contractor personnel of a recipient DoD Component, contractor or grantee may be granted access to information bearing the LIMITED DISTRIBUTION caveat provided they have been determined to have a valid need to know for such information in connection with the accomplishment of official business for the DoD. Recipients shall be made aware of the status of such information, and transmission shall be by means to preclude unauthorized disclosure or release. Further dissemination of information bearing the LIMITED DISTRIBUTION caveat by receiving contractors or grantees to another Military Department, other DoD Component, contractor or grantee, or dissemination by any recipient Component, contractor, or grantee to any person, agency or activity outside DoD, requires the express written approval of the Director, NGA.

(3) Information bearing the LIMITED DISTRIBUTION caveat, or derivative information, shall not be released, made accessible to or sold to foreign governments or international organizations, to include through Foreign Security Assistance transactions or arrangements, or transfer or loan of any weapon or weapon system that uses such information, or intended to be used in mission planning systems, or through the Foreign Military Sales process, without the express, written approval of the Director, NGA.

(4) All FOIA requests for information bearing the LIMITED DISTRIBUTION caveat or derived therefrom, shall be referred to NGA consistent with reference (x).

d. Protection

(1) Information bearing the LIMITED DISTRIBUTION caveat, or derivative information, shall not be stored on systems accessible by contractors, individuals who are not directly working on a DoD contract, or those who do not require access to such information in connection with the conduct of official DoD business.

(2) LIMITED DISTRIBUTION information or derivative information, may only be posted on DoD web sites consistent with security and access requirements specified in Deputy Secretary of Defense Memorandum, *Web Site Administration*, December 1998. Such information shall not be transmitted over the World Wide Web or over other publicly accessible and unsecured systems. Electronic transmission of such information, e.g. voice, data or facsimile, shall be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure.

(3) Store LIMITED DISTRIBUTION information in the same manner approved for FOUO.

(4) When no longer required, all LIMITED DISTRIBUTION information and copies, shall be returned to NGA or destroyed in a manner sufficient to prevent its reconstruction.

4. DoD Unclassified Controlled Nuclear Information

a. Description. DoD Unclassified Controlled Nuclear Information (UCNI) is unclassified information on security measures (including security plans, procedures, and equipment) for the physical protection of DoD Special Nuclear Material (SNM) equipment, or facilities. Information is designated DoD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities. Information may be designated DoD UCNI by the Heads of the DoD Components and individuals to whom they have delegated the authority.

b. Markings. Unclassified documents and material containing DoD UCNI shall be marked as follows:

(1) The face of the document and the outside of the back cover (if there is one) shall be marked "DoD Unclassified Controlled Nuclear Information."

(2) Portions of the document that contain DoD UCNI shall be marked with "(DoD UCNI)" at the beginning of the portion.

(3) Classified documents and material containing DoD UCNI shall be marked as follows:

(a) Pages with no classified information but containing DoD UCNI shall be marked "DoD Unclassified Controlled Nuclear Information" at the top and bottom.

(b) Portions of the document that contain DoD UCNI shall be marked with "DoD UCNI" at the beginning of the portion, in addition to the classification marking, where appropriate.

(c) Material other than paper documents (for example slides, computer media, films, etc.) shall bear markings that alter the holder or viewer that the material contains DoD UCNI.

(d) Documents and material containing DoD UCNI and transmitted outside the DoD shall bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information. A statement similar to this one should be used:

DEPARTMENT OF DEFENSE
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION
EXEMPT FROM MANDATORY DISCLOSURE
(5 U.S.C. 552(b)(3), as authorized by 10 U.S.C. 128)

c. Access to DoD UCNI. Access to DoD UCNI shall be granted only to persons who have a valid need-to-know for the information and are specifically eligible for access under the provisions of reference (t).

d. Protection of DoD UCNI

(1) During working hours, reasonable steps should be taken to minimize the risk of access by unauthorized personnel. After working hours, DoD UCNI may be stored in unlocked containers, desks or cabinets if government or government-contract building security is provided. If such building security is not provided, DoD UCNI shall be stored in locked buildings, rooms, desks, file cabinets, bookcases, or similar items.

(2) Record copies of DoD UCNI documents shall be disposed of IAW reference (g) and Component records management directives. Non-record DoD UCNI documents may be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

E. Distribution Statements on Technical Documents

1. General. Reference (u) requires distribution statements to be placed on technical documents, both classified and unclassified. These statements are intended to facilitate control, distribution, and release of these documents without the need to repeatedly refer questions to the originating activity. The originating office may, of course, make case-by-case exceptions to distribution limitations imposed by the statements.

2. Text of the Statements

a. Distribution Statement A. Approved for public release, distribution is unlimited.

b. Distribution Statement B. Distribution authorized to U.S. Government agencies only; (reason); (date). Other requests for this document shall be referred to (controlling DoD office).

c. Distribution Statement C. Distribution authorized to U.S. Government agencies and their contractors; (reason); (date). Other requests for this document shall be referred to (controlling DoD office).

d. Distribution Statement D. Distribution authorized to the DoD and U.S. DoD contractors only; (reason); (date). Other requests for this document shall be referred to (controlling DoD office).

e. Distribution Statement E. Distribution authorized to DoD Components only; (reason); (date). Other requests for this document shall be referred to (controlling DoD office).

f. Distribution Statement F. Further distribution only as directed by (controlling DoD office) or higher DoD authority; (date).

g. Distribution Statement X. Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data IAW DoD Directive 5230.25 (see reference (v)); (date). Controlling DoD office is (controlling DoD office).

CHAPTER 10
INFORMATION SYSTEMS

A. Background. Information systems (IS) security is a multifaceted discipline. Protecting information being processed, transmitted, and/or stored by IS requires software and hardware security features, in addition to more traditional security disciplines, such as physical security and personnel security. The IS security ensures the confidentiality, integrity, and availability of the information within the IS. The IS is often referred to as AIS and Information Technology.

B. General Requirements. Within the OIG the Chief Information Officer (CIO) is responsible for the direction, administration, and implementation of IS networks that process, store, reproduce, transmit, or otherwise handle classified or unclassified but sensitive information. When national security or unclassified but sensitive information is processed in an IS, the system shall be accredited by a Designated Approving Authority (DAA).

C. Certification and Accreditation Overview. Agency officials are required to certify systems that meet all applicable federal policies, regulations, and standards, and the results of system tests demonstrate that the Certification and Accreditation (C&A) process is proportional to the system size, mission criticality, data sensitivity, and security requirements.

D. Physical Security

1. Physical security of systems processing national security information shall be established and continuously maintained. The level of controls shall be commensurate with the highest classification level of the information handled by the IS and the environment in which the IS operates. Protective measures shall prevent or detect unauthorized access through system entry points and unauthorized modification of computer hardware. Mission critical systems shall have adequate security controls to prevent and/or detect unauthorized attempts to disclose, delay, modify, or destroy information handled by the IS.

2. Transmission of national security information shall be over secure communications lines.

E. Personnel Security. Personnel security clearances and access authorizations shall be commensurate with the mode of operation. Brief the users on their responsibility for AIS security and the information it contains.

F. Accountability, Marking, and Control of Information Systems Media. The IS media, such as tapes, diskettes, and optical and hard disks, are documents with properties requiring additional controls to compensate for their ability to retain information, their portability and the quantity of information stored on them. Accountability and control of media shall be consistent with the highest level of national security information ever recorded on the media until the information on the media, or the media itself, is declassified.

1. The IS media shall be marked and identified with appropriate SF Labels: SF-706, SF-707, SF-708, SF-709, SF-710, and SF 711 (Appendix E).

2. The AIS and the media remain classified at the highest level until they are declassified or destroyed.

G. Storage Media Review. The IS storage media shall be reviewed periodically for information that is no longer required or authorized for retention.

H. Violations and Compromises.

1. Violations and compromises of classified information via an IS shall be reported immediately to the Office of Security using the notification procedures outlined in Chapter 8 of this Instruction. The Office of Security shall notify the CIO.

2. The CIO shall ensure adequate procedures are instituted to facilitate compromise recovery for national security information to mitigate damage and identify information should the media or system be subject to loss or compromise. Sufficient system records, such as backup media and audit records, shall be maintained to reconstruct material.

CHAPTER 11
NORTH ATLANTIC TREATY ORGANIZATION CLASSIFIED INFORMATION

A. North Atlantic Treaty Organization Classified Information. The NATO information is information that has been generated by or for NATO, or member nation national information that has been released into the NATO security system. The protection of this information is controlled under the NATO security regulations, and access within NATO is determined by the holder, unless restrictions are specified by the originator at the time of release to NATO.

B. Requirements for Access to North Atlantic Treaty Organization Classified Information. All personnel requiring access to NATO classified information shall receive a security briefing by the Office of Security regarding the protection of NATO classified information and complete a statement acknowledging receipt of the briefing (reference (z)). These statements shall be retained by the security manager. (A sample NATO security briefing is found on the Central U.S. Registry (CUSR) websites.) The following web addresses provide access to the classified (http://classweb.hqdas.army.smil.mil/cusr/siprnet_A.asp) and unclassified (https://secureweb.hqda.pentagon.mil/cusr) websites. These sites provide access to NATO security documents, updates on the security of NATO information and a profile of the CUSR. The security briefing does not automatically permit the recipient to have access to NATO classified information. The recipient shall also possess the requisite personnel security clearance (PSC) and have a need to know NATO classified information. Need-to-know is determined by the official having possession or control of the NATO classified information. No individual is entitled solely because of rank, appointment, or security clearance to have access to NATO classified information. A PSC is not required for access to NATO RESTRICTED (NR) information. However, individuals shall be briefed on their responsibilities for the protection of NR information.

C. Marking and Safeguarding. The Office of Security, Information Security Program Manager is the focal point for specific safeguarding requirement for the control, accountability, distribution, and limited destruction of NATO documents. NATO security classifications and their significance are as follows:

1. COSMIC TOP SECRET (CTS) – unauthorized disclosure would result in exceptionally grave damage to NATO;

2. NATO SECRET (NS) – unauthorized disclosure would result in grave damage to NATO;

3. NATO CONFIDENTIAL (NC) – unauthorized disclosure would be damaging to NATO; and

4. NATO RESTRICTED (NR) – unauthorized disclosure would be detrimental to the interests or effectiveness of NATO. (Note: The U.S. does not have a level of classification equivalent to NR. Generally, the U.S. applies to NR the protective measures used nationally "For Official Use Only" (FOUO) information.)

5. ATOMAL – ATOMAL information can be either U.S. Restricted Data or Formerly Restricted Data that is classified pursuant to the Atomic Energy Act of 1954, as amended, or United Kingdom ATOMIC information that has been officially released to NATO. ATOMAL information is marked either COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

6. NATO UNCLASSIFIED (NU) is a marking applied to NATO information that does not have a security classification, but shall only be used for official purposes. NU information may also carry administrative or dissemination limitation markings.

7. The top and bottom of each page of a document shall be marked with the overall security classification of the document. Each portion of a document, including paragraphs, shall be assigned classification markings. NATO markings shall be removed from all information approved for release to the public.

8. The U.S. documents containing extracted NATO information shall be marked and handled as follows:

a. A U.S. classified document containing NATO classified information shall bear a U.S. classification marking that reflects the highest level of NATO or U. S. classified information contained therein. The statement "THIS DOCUMENT CONTAINS NATO (level of classification) INFORMATION" shall appear on the front of the document.

b. Each page of a U.S. document containing NATO information shall be marked with a U.S. classification that reflects the highest level of U.S. or NATO classified information found on the page. For example, if the page displays U.S. unclassified, U.S. "CONFIDENTIAL," and "NATO SECRET" information, the page shall be marked "SECRET."

c. When extracted NR information is included in an otherwise unclassified U.S. document, the front of the document shall be marked, THIS DOCUMENT CONTAINS NATO RESTRICTED INFORMATION – PROTECT AS "FOR OFFICIAL USE ONLY."

9. The NATO classified information shall be stored in a GSA approved security container, with supplemental controls as necessary. The NR shall be stored in a locked container that deters access by personnel not requiring the information for official NATO purposes.

10. Ensure that the combination to a GSA approved security container containing NATO documents is changed annually.

11. The combination of a container, vault, or open storage area used for the storage of NATO classified information shall be treated as information having a classification equal to the highest category of the classified information stored therein. Any written record of the combination shall be marked with the appropriate classification level.

12. Receipts are required for accountable NATO information, i.e., CTS, NS and special category information, e.g., ATOMAL. Receipts are not required for NC or NR information.

D. Disposal and Destruction. When NATO classified information is no longer needed, it shall be reviewed for downgrading, archival storage, declassification or destruction. It shall be destroyed in the same manner as U.S. classified information.

1. Destruction certificates and control records for CTS information shall be retained in a registry for a minimum of 10 years to assist in the event of an investigation.

2. The destruction of NS information shall be recorded and the record signed by an appropriately cleared destruction officer and witness.

3. Destruction certificates and control records for NS information shall be retained in the registry or office performing the destruction for a minimum of 5 years.

CHAPTER 12
PROGRAM MANAGEMENT

A. General Management. Supervisors at all OIG Component levels are responsible for effective program implementation and are accountable for the security performance of their employees.

B. Program Monitoring. The Office of Security is responsible for monitoring, inspecting, with or without prior announcement, or conducting staff assistance visits at locations involved in classified activities. Written documentation of inspections and staff assistance visits shall be maintained and available for review for a minimum of 2 years. Counterintelligence technical inspections shall be conducted or scheduled by the Office of Security on an "as needed" or recurring basis. The Office of Security shall:

1. Demonstrate personal commitment and commit senior management to the successful implementation of the program established under reference (a).

2. Promulgate implementing instructions.

3. Establish and maintain security education and training programs.

4. Establish and maintain an on-going self-inspection program, which shall include the periodic review and assessment of OIG classified products.

5. Establish procedures to prevent unnecessary access to classified information, including procedures that:

a. Require a need for access to classified information be established before initiating administrative clearance procedures.

b. Ensure the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs.

c. Develop special contingency plans to safeguard classified information used in or near hostile or potentially hostile areas.

d. Assure the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the employee's rating.

e. Account for the costs associated with the implementation of reference (a), which shall be reported to the Director of ISOO for publication.

f. Promptly assign OIG personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of reference (a) that pertains to classified information that originated in an OIG Component that no longer exists and for which there is no clear successor in function.

C. Field Program Management. The OIG field activities shall appoint, in writing, an official to serve as security manager for the activity. To ensure compliance with this Instruction, the official shall be responsible for the administration of an effective information security program emphasizing security education and training; assignment of proper classification, downgrading, and declassification; and overall information security oversight.

D. Appointing Authorities. Ensure officials appointed as Component security managers are authorized direct and ready access to the appointing official on matters concerning the Information Security Program. They shall provide sufficient resources of time, staff and funds to permit accomplishment of the security manager's responsibilities, to include meaningful oversight of the Information Security Program at all levels of the activity. (Appointing authorities include OIG Component Heads and Special Agents In Charge of the field activities.)

E. Appointed Security Managers. Serve as a focal point for the OIG Component for advice and assistance and distribution of OIG policy on classification, declassification, downgrading, and marking of national security information. They shall conduct and coordinate the following actions with the Office of Security:

1. Conduct annual self-inspections of their security programs.

2. Prepare a Standard Operating Procedure (SOP) for unique situations in their OIG Component that have not been addressed in this Instruction. (The SOP shall be submitted to the Office of Security for approval before implementation in the OIG Component.)

3. Ensure that indoctrination, refresher, threat, courier, foreign travel, and termination briefings are conducted. Maintain an official file copy of the orientation and annual briefings. Attendance verification can be obtained through the Office of Security.

4. Ensure a periodic document review program is conducted in the OIG Component annually to reduce unnecessary classified holdings. The program shall include downgrading, declassifying, destroying, or returning documents to originator.

5. Report all security incidents or violations to the Office of Security and serve as the point of contact on the status of ongoing preliminary inquiries and/or formal investigations.

6. Prepare and/or coordinate requests for badges and designation letters.

7. Coordinate DD Form 1610, *Request and Authorization for TDY Travel of DoD Personnel*, as necessary, acknowledging that travelers are authorized to hand carry classified material and have received a briefing before departure regarding applicable export control, foreign disclosure, and security requirements.

8. Maintain an account for all classified information stored, handled, and processed in their Components.

CHAPTER 13
BUILDING ENTRANCE POLICY/BADGES/PROPERTY PASSES/ESCORTING

A. Policy. Only authorized personnel with a valid DoD identification (ID) are allowed access into 400 Army Navy Drive. All other personnel shall sign in and be escorted. Café patrons shall be permitted to walk through the lobby to the café even though it is not the primary entrance for the café. Personnel working at off-site field activities shall ensure visitors are properly cleared and SOPs address visitor control, property removal, and deliveries. Visitors shall be controlled and escorted in OIG offices located in Crystal Gateway North.

1. Acceptable ID (Building Passes)

   a. White DoD Badge (DoD Employees)

   b. Pink DoD Badge (Contractors)

   c. Blue DoD Badge (Press/Foreign Nationals)

   d. Gray (Retired DoD Civilians)

   e. Tan Temporary (Press)

   f. DoD Civilian ID

   g. Military ID

2. X-ray and Metal Detector Screening. Individuals without an acceptable ID badge shall go through the metal detector screening. Packages in their possession shall also be screened through the x-ray machine. Packages too large for screening shall be physically checked.

3. Mail/FEDEX/UPS/RPS/Airborne Deliveries. Packages shall go through the x-ray machine for screening. To avoid problems with the lobby guards, delivery personnel should have a designated point of contact. Delivery personnel should at least know the office to where the package is to be delivered. Packages shall not be dropped off at the guard desk or held by the lobby guards.

4. Bulk Deliveries (Supplies and Equipment, etc.). Bulk deliveries that are expected and verified do not require screening. The escort shall be responsible for the shipment.

5. Removing Property. Property (including personal property) being removed from 400 Army Navy Drive no longer requires a valid Property Pass (Appendix Y). It is a good security practice to receive one when visiting other locations in case the Lobby guards check the serial number, bar code, and description of the item to verify that it corresponds to the information listed on the property pass. This way they may ensure it legitimately belongs to the subject involved.

6. Exceptions may be granted to waive visitor badge and X-ray screening on a case-by-case basis. Advance coordination shall be made with the Office of Security to have these requirements waived.

7. Before and After Hours Sign-In. For safety reasons, OIG personnel are required to sign-in before 6:00 a.m. and after 6:00 p.m. during weekdays. Additionally, personnel shall sign in and out during weekends and holidays.

8. Forgotten or Lost Badges. Employees who forget or lose their badge may be issued a temporary badge by the main lobby guards at 400 Army Navy Drive. A personnel roster of all DoD civilian employees is maintained at the front lobby desk. Military personnel may show a military ID to gain entry and to obtain a temporary badge. Temporary badges issued to the individual shall require an exchange ID or driver's license. The ID or driver license shall be returned to the individual when the temporary ID is returned to the main lobby guard desk. Lost or broken badges may be replaced by going directly to the Pentagon Building Pass Office. Expired badges shall be taken to the Office of Security for renewal.

B. Basic Rules for Escorting and General Escort Requirements. The escort shall accept responsibility for the uncleared individuals visiting OIG facilities. By doing so, the escort acknowledges his or her commitment to the escort assignment, is knowledgeable of escorting requirements and guidelines, and assumes control over the visitor at all time. The escort shall be familiar with the OIG Fire and Building Evacuation Plan and know what to do in case of an evacuation procedure. The escort shall observe all security rules and regulations and shall ensure uncleared individuals comply with OIG instructions and directions. The need-to-know rule applies to all persons at all times. The escort shall maintain visual contact with escorted personnel at all times and/or shall be in a position to control the movement and actions of uncleared persons. The escort shall remain with visitors at all times until he or she is turned over to another official or escort; or leaves the OIG facility. Escorts shall ensure that the uncleared person(s) wears his or her badge above the waist.

1. Non-OIG personnel, workers, contractors, maintenance personnel, and delivery personnel cannot perform escort responsibilities. Exceptions to this rule shall be addressed individually with the Office of Security.

2. Escorting Groups. When escorting a group, the limit ratio is one escort to not more than 5 uncleared persons, all within the line of sight.

3. Office Areas. When escorting individuals into an office area (or any processing area), the escort shall ensure that:

   a. Repositories are locked or drawers closed.

   b. No classified data is visible on a computer screen.

   c. No classified documents are unattended.

d. Persons using classified material are advised to shield such information.

e. No classified discussions are held in the presence of uncleared personnel.

f. Reproduction machines, telefax, secured telephones, and mail drops are free of visible classified data.

g. Be aware of the movement of classified materials through areas where uncleared visitors are present.

h. Needs to be aware of what items are placed in all toolboxes.

C. Escorting Persons with a Suspended Clearance or Restricted Access. The OIG employees whose clearances are suspended shall be escorted at all times. Escorts shall ensure that they are in full compliance with this Instruction.

D. Non-Receipt of Visit Certification Letter. Visitors occasionally arrive at OIG facilities without having had their security clearance passed by their security office. Although the escort may have personal knowledge that the visitor holds a clearance at another facility, or they tell you their clearance is held elsewhere, or they show you their facility badge, they shall still be treated as uncleared. A security badge can only grant access to areas in OIG facilities. An "employee badge" shall not be used to grant an individual access to classified information. The Office of Security can verify a DoD clearance through the JPAS.

E. Field Activity Managers and Components. The OIG Components and field activity managers are responsible for classified information security within their areas. Therefore, managers who request uncleared personnel be afforded access to their areas are certifying that appropriate security measures are in place, that uncleared personnel shall not be afforded access to classified matter and that escorts are properly briefed.

F. Challenges. Should any OIG employee observe an uncleared individual unescorted, it is the employee's responsibility to become an escort to that person. This may be accomplished by detaining the uncleared person while you call the Office of Security or front lobby guards to respond to your location or to escort the individual to the front lobby guard desk. Uncleared employees who observe an unescorted individual should report the situation to their escort who shall take appropriate action. ***The OIG personnel should never ignore the situation – each OIG employee is authorized and obligated to take immediate action.***

APPENDIX A
REFERENCES

a. Executive Order (E.O.) 12958, *Classified National Security Information,* April 17, 1995, effective October 14, 1995

b. DoD 5200.1-R, *Information Security Program Regulation*, January 1997

c. DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*, April 1997

d. DoD 5400.7-R, *DoD Freedom of Information Act Program*, September 1998 with Change 1, April 11, 2006

e. Title 5, United States Code, Section 552, as amended, *The Freedom of Information Act*

f. Title 5, United States Code, Section 552a, *The Privacy Act*

g. Title, 44, United States Code, Chapters 21, 31, and 33, *Federal Records Act and National Archives and Records Administration Act of 1984*

h. DoD Directive 5210.56, *Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties*, November 1, 2001, with Change 1, January 24, 2002

i. DoD Directive 3224.3, *Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support*, February 17, 1989

j. Title 18, United States Code, *Crimes and Criminal Procedure*

k. DoD 5200.2-R, *Personnel Security Program*, January 1987, with Changes 1, 2, 3, February 23, 1996

l. DoD C-5105.21-M-1, *Sensitive Compartmented Information (SCI) Administrative Security Manual*, March 1995*(U),* authorized by DoD Directive 5105.21, Defense Intelligence Agency, May 19, 1977

m. DoD Directive 5200.33, *Defense Courier Service (DCS),* June 24, 2002

n. DoD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations,* June 16, 1992

o. DoD Directive 5400.4, *Provisions of Information to Congress*, January 30, 1978

p. DoD Directive 7650.1, *General Accounting Office and Comptroller General Access to Records*, September 11, 1997

q. DoD 5400.11-R, *Department of Defense Privacy Program*, May 14, 2007

r. Title 15, United States Code, *Computer Security Act of 1987*

s. DoD Directive 8500.01E, *Information Assurance*, October 24, 2002

t. DoD Directive 5210.83, *Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI),*" November 15, 1991, with Change 1, November 16, 1994

u. DoD Directive 5230.24, *Distribution Statements on Technical Documents*, March 18, 1987

v. DoD Directive 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, November 16, 1984, with Change 1, August 18, 1995

w. DoD Directive C-5200.5, *Communications Security (COMSEC),* April 21, 1990

x. DoD Instruction 5030.59, *National Geospatial-Intelligence Agency (NGA) LIMITED DISTRIBUTION Geospatial Intelligence*, December 7, 2006

y. Federal Register, Part IV National Archives and Records Administration, Information Security Oversight Office (ISOO) Directive No. 1 September 22, 2003

z. DoD Directive 5100.55, *United States Security Authority for North Atlantic Treaty Organization Affairs*, February 27, 2006

APPENDIX B
DEFINITIONS

1. **Access**. The ability or opportunity to gain knowledge of classified information.

2. **Accreditation**. A formal declaration by the Designated Approving Authority (DAA) that the Information System (IS) is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an IS and is based on the certification process, as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

3. **Agency**. Any "Executive Agency," as defined in 5 United States Code (U.S.C.) 105, and any other entity within the executive branch that comes into the possession of classified information.

4. **Automated Information System (AIS) or Information System**. An assembly of computer hardware, software or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

5. **Automatic Declassification**. The declassification of information based solely upon:

a. The occurrence of a specific date or event as determined by Original Classification Authority (OCA); or

b. The expiration of a maximum period for duration of classification established under reference (a).

6. **Certification**. (Also called **Functional Compliance Certification**, **Security Certification, and Summary Certification**). The technical evaluation of an AIS's security features and other safeguards, made in support of the accreditation process, which established the extent that a particular AIS's design and implementation meets a set of specified security requirements.

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

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

9. **Classification Guide**. A documentary form of classification guidance issued by an OCA 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.

10. **Classified Contract**. Any contract that requires or will require access to classified information by the contractor or contractor employees in the performance of the contract. A contract may be classified although the contract documentation is not classified.

11. **Classified National Security Council (NSC) Information** (hereafter called NSC Information). Classified information contained in documents prepared by or for the NSC, its interagency groups and associated committees and groups. The term also includes deliberations of the NSC, its interagency groups and associated committees and groups.

12. **Classified National Security Information** (hereafter "classified information"). Information that has been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

13. **Cleared Contractor Facility**. A contractor facility in the U.S. that has been granted a facility security clearance IAW the National Industrial Security Program. The level of clearance granted to individual facilities varies.

14. **Confidential Source**. Any individual or organization that has provided, or that may reasonably be expected to provide, information to the U.S. on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

15. **Contact Officer**. An OIG official designated in writing to oversee and control the activities of foreign representatives accredited to or visiting OIG facilities.

16. **Damage to the National Security**. Harm to the national defense or foreign relations of the U.S. from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

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

18. **Declassification Authority**:

a. The official who authorizes the original classification, if that official is still serving in the same position.

b. The originator's current successor in function.

c. A supervisory official of either 1 or 2 above.

d. Officials delegated declassification authority in writing by the Inspector General of the DoD, or his or her designee.

19. **Declassification Guide**. Written instructions issued by a declassification authority that describe the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

20. **Derivative Classification**. The incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly created 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.

21. **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.

22. **Extended Visit**. Identical to a visit, except that approval is extended for recurring contacts over a longer time, normally not to exceed 1 year.

23. **File Series**. Documentary material, regardless of its physical form or characteristics, that is arranged IAW a filing system or maintained as a unit because it pertains to the same function or activity.

24. **For Official Use Only (FOUO)**. Information that has not been given a security classification under the criteria of an Executive Order, but that may be withheld from the public for one or more of the reasons cited in Freedom of Information Act Exemptions 2 through 9 shall be considered as being FOUO. FOUO is not authorized as a weak form of classification to protect U.S. National Security Interests.

25. **Foreign Disclosure**. The conveying of classified information to an authorized representative of a foreign government or international organization in a manner approved by this Instruction. It may be accomplished by providing documents or materials or by oral or visual means, including briefings, conferences, or other meetings.

26. **Foreign Government Information**:

a. Information provided to the U.S. Government 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.

b. Information produced by the U.S. 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.

c. Information received and treated as “Foreign Government Information” under the terms of a predecessor order.

27. **Foreign Nationals**. All persons who are not citizens, nationals, or immigrant aliens of the U.S.

28. **Foreign Representatives**. Foreign nationals as well as citizens or nationals of the U.S. or immigrant aliens who, in their individual capacity, or on behalf of a corporation (whether as a corporate officer or official, or as a corporate employee who personally is involved with the foreign entity), are acting as representatives, officials, agents, or employees of a foreign government, firm, corporation, international organization, or foreign national.

29. **Government Installation**. A U.S. Government facility where adequate measures for safeguarding classified information can be imposed.

30. **Government to Government**. The approved channel for the disclosure of classified information by an authorized U.S. Government agency or representative of a foreign government or international organization.

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

32. **Information System**. See ***Automated Information System***.

33. **Infraction**. Any knowing, willful, or negligent action contrary to the requirements of reference (a) or its implementing directives that does not comprise a "violation."

34. **Integrity**. The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, stored, or destroyed.

35. **International Organization**. A duly constituted international body, civilian or military or both, having responsibility for any aspect of mutual defense, which may have a requirement for access to U.S. classified information in carrying out its assigned responsibilities; e.g., the International Staff of the North Atlantic Treaty Organization (NATO), Australia-New Zealand-United States (ANZUS), Inter-American Defense Board (IADB), Canada-U.S. Regional Planning Group, the military staffs of Supreme Headquarters Allied Powers, Europe (SHAPE), and Supreme Allied Command, Atlantic (SACLANT).

36. **Limited Dissemination**. Restrictive controls for classified information established by an original classification authority to emphasize need-to-know protective measures available within the regular security system.

37. **Mandatory Declassification Review**. The review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of E.O. 12958.

38. **Meeting**. A conference, seminar, symposium, exhibit, convention, or gathering conducted by an OIG office, directorate, organizational element, a cleared contractor or an association, institute, or society, or employee whose membership includes DoD or contractor personnel, and during which DoD classified information or classified information of interest to the DoD is disclosed.

39. **Multiple Sources**. Two or more source documents, classification guides, or a combination of both.

40. **National Security**. The national defense or foreign relations of the U.S.

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

42. **Network**. A system of two or more computers that can exchange data or information.

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

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

45. **Originating Agency**. The agency responsible for the initial determination that particular information is classified.

46. **Safeguarding**. Measures and controls that are prescribed to protect classified information.

47. **Security Sponsor**. An official designated by the Inspector General of the DoD, or a designee, to be responsible for supervising all security aspects of classified meetings.

48. **Self-Inspection**. The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established reference (a) and its implementing directives.

49. **Senior Agency Official**. The official designated by the agency head under section 5.6(c) of E.O. 12958 to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

50. **Sensitive Information**. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest of the conduct of Federal programs, or the privacy to which individuals are entitled reference (f), but which has not been specifically authorized under criteria established by an E.O. or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

51. **Source Document**. An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

52. **Special Access Program (SAP)**. A program established for a specific class of classified information that imposes safeguarding and accesses requirements that exceed those normally required for information at the same classification level.

53. **Special Category (SPECAT)**. The term "SPECAT" is used only for electrically transmitted information identified with a specific project or subject having worldwide application and requiring security protection or handling not guaranteed by the primary security classification. Such messages shall be handled by, and disseminated to, only those personnel specifically authorized such access. The term "SPECAT" is inserted by the originator immediately following the message classification and preceding the special category designator; e.g., TOP SECRET (SPECAT SIOP-ESI).

54. **Special Handling**. Special handling is that procedure required for safeguarding information annotated with code words, nicknames, or caveats, which restricts the dissemination of such information to approved areas or personnel.

55. **Sponsor**. An OIG Component that has a principal interest in the subject matter of a meeting and that has accepted security sponsorship for the meeting.

56. **Systematic Declassification Review**. The review for declassification of classified information contained in records that have been determined by the Archivist of the U.S. ("Archivist") to have permanent historical value IAW reference (g).

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

58. **Unauthorized Disclosure**. A communication or physical transfer of classified information to an unauthorized recipient.

59. **Violation**:

a. Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.

b. Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E. O. 12958 or its implementing directives.

c. Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of E.O. 12958.

APPENDIX C
ACRONYMS

ACCM	Alternative Compensatory Control Measures
AIG-A&M	Assistant Inspector General for Administration and Management
AIS	Automated Information Systems
ALSD	Administration and Logistics Services Directorate
APO	Army Post Office
ASAS	Automatic Security Administrative System
C	Confidential
C&A	Certification and Accreditation
CAC	Common Access Card
CIK	Crypto Ignition Key
CIO	Chief Information Officer
CJCSM	Chairman of the Joint Chiefs of Staff Manual
COMSEC	Communications Security
CONUS	Continental United States
COOP	Continuity of Operations Plan
COR	Contracting Officer's Representative)
CSA	Cognizant Security Agency
CTS	Cosmic Top Secret
CTSA	Cosmic Top Secret Atomal
CUSR	Central U.S. Registry
DAA	Designated Approving Authority
DCII	Defense Central Index of Investigations
DEFCOS	Defense Courier Service
DIA	Defense Intelligence Agency
DoD UCNI	Department of Defense Unclassified Controlled Nuclear Information
DoD	Department of Defense
FGI	Foreign Government Information
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FOUO_LES	For Office Use Only Law Enforcement Sensitive
FPO	Fleet Post Office
GAO	General Accountability Office
GSA	General Service Administration
IDS	Intrusion Detection System
IG	Inspector General
IS	Information Systems
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
IT	Information Technology
JCS	Joint Chiefs of Staff
JPAS	Joint Personnel Adjudication System
MTMC	Military Traffic Management Command

NATO	North Atlantic Treaty Organization
NC	North Atlantic Treaty Organization Confidential
NCA	North Atlantic Treaty Organization Confidential Atomal
NCR	National Capital Region
NDA	Nondisclosure Agreement
NGA	National Geospatial-Intelligence Agency
NR	North Atlantic Treaty Organization Restricted
NS	North Atlantic Treaty Organization Secret
NSA	National Security Agency
NSA	North Atlantic Treaty Organization Secret Atomal
NU	North Atlantic Treaty Organization Unclassified
OASD(NII)	Office of the Assistant Secretary of Defense (Networks and Information Integration)
OCAs	Original Classification Authorities
OCCL	Office of Communications and Congressional Liaison
OIG	Office of Inspector General
OPR	Office of Primary Responsibility
PA	Privacy Act
PDA	Personal Digital Assistant
PIO	Preliminary Inquiry Officer
PKI	Public Key Infrastructure
PSC	Personnel Security Clearance
PSS	Protective Security Service
RFB	Requests for Bid
RFQ	Requests for Quotation
S	Secret
SAPs	Special Access Programs
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIFs	Sensitive Compartmented Information Facilities
SF	Standard Form
SIO	Senior Information Officer
SNM	Special Nuclear Material
SOP	Standard Operating Procedure
SSO	Special Security Officer
STE	Secured Telephone Equipment
STU-III	Secure Telephone Unit-III
TDY	Temporary Duty
TS	Top Secret
TSCA	Top Secret Control Account
TSCO	Top Secret Control Officer
U	Unclassified
USPS	United States Postal Service
VAL	Visit Authorization Letter

APPENDIX D
OIG INFORMATION SECURITY SELF-INSPECTION CHECKLIST

ALL PURPOSE CHECKLIST		PAGE 1 OF 6 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA OIG/ Information Security Self-Inspection Checklist		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	PROGRAM MANAGEMENT			
1.	Has the head of each activity in the Component appointed a security manager to oversee the implementation and oversight of the provisions of DoD 5200.1-R? (DoD 5200.1-R, C1.2.2.3)			
2.	Does the Component Head develop and implement, through the security manager, security instructions necessary for program implementation? (DoD 5200.1-R, C1.2.3.2)			
3.	Does the security manager host staff assistance visit with PFPA/SSD?			
4.	Has the security manager attended the required security manager's training sponsored by PFPA-SSD? Note: Training and education shall be provided before, concurrent with, or not later than six months following appointment? (DoD 5200.1-R, C9.3.1)			
5.	Does the security manager attend the PFPA/SSD Security Manager's meeting, hosted by PFPA-SSD?			
6.	Does the security manager oversee the conduct of security inspections (self-inspection)? (DoD 5200.1-R, C1.7)			
	• Is the Component Head informed of the results of such inspection?			
7.	Does the security manager establish, implement and maintain an effective security education program as required by DoD 5200.1-R, Chapter 9, to include initial orientation and continuing/refresher training for assigned members? (DoD 5200.1-R, C1.2.3.3, C9.4.1 and C9.4.2)			
	• Do security managers document all security-related training? (DoD 5200.1-R, C9.6)			
8.	Are procedures established to prevent unauthorized access to classified information? (DoD 5200.1-R, C1.2.3.5))			
	• Note: Examples include implementing visitor controls, restricting combinations to cleared members, establishing end-of-day security checks, etc)			
9.	**Are members familiar with the procedures for safeguarding classified information in case of fire, natural disaster or civil disturbances? (DoD 5200.1-R, C6.3.4)**			
10.	**Are procedures established for ensuring that all persons handling classified material are properly cleared and have a need-to-know? (DoD 5200.1-R, C1.1.2.5, C1.1.2.5.1, C1.1.2.5.2 and C1.1.2.5.3)**			
11.	**Does the security manager maintain a continuity handbook? (DoD 5200.1-R, C1.2.3)**			
	DOCUMENT MARKINGS			
1.	Are derivatively classified documents properly marked when information is extracted from a classified source, to include the:			
	• Overall classification (DoD 5200.1-R, C5.2.1))			
	• The Agency, Office or Origin, and Date (DoD 5200.1-R, C5.2.2)			
	• A "Derived From :" line (DoD 5200.1-R, C5.2.3.2)			

ALL PURPOSE CHECKLIST		PAGE 2 OF 6 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA OIG/ Information Security Self-Inspection Checklist		**OPR**	**DATE**	
NO.	**ITEM** ***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)***	YES	NO	N/A
	• Identification of the "sources" of classification (DoD 5200.1-R, C5.2.3.3)			
	• Declassification Instructions (DoD 5200.1-R, C5.2.5))			
	DOCUMENT MARKINGS (CONTINUED)			
	• Downgrading instructions, if required (DoD 5200.1-R, C5.2.6)			
	• Page Markings (DoD 5200.1-R, C5.1.3.1.5)			
2.	Are "subjects" or "titles" of classified documents marked with the appropriate symbol (TS), (S), (C), or (U) following and to the right of the title or subject? (DOD 5200.1-R, C5.2.7.1.2)			
3.	Is each section, part, paragraph, or similar portion of a classified document marked to show the highest level of classification of information it contains, or that it is unclassified? Portion of text shall be marked with the appropriate abbreviations (TS, S, C, or U). (DoD 5200.1-R, C5.2.7.1.1)			
4.	Are portions within documents containing Restricted Data and Formerly Restricted Data marked with the abbreviation "RD" or "FRD" (e.g. S-RD or TS-FRD)? (DoD 5200.1-R, C5.2.7.1.1.1)			
5.	Are portions within documents containing foreign government or North Atlantic Treaty Organization (NATO) information marked with the foreign classification or N for NATO with the appropriate level (e.g. UK-S or N-TS)? (DoD 5200.1-R, C5.2.7.1.1.2)			
6.	Is the abbreviation "FOUO" used to designate unclassified portions that contain information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA)? (DoD 5200.1-R, C5.2.7.1.1.3)			
7.	Are charts, graphs, photographs, illustrations, figures, and similar items within classified documents marked to show their classification? (DoD 5200.1-R, C5.2.7.1.3)			
8.	Are the markings placed within the chart, graph, photograph, illustration, figure, etc. or next to the item? (DoD 5200.1-R, C5.2.7.1.3.2)			
9.	Is the highest classification level placed on the top and bottom of each page containing classified information or marked "unclassified"?			
	• Do the markings stand out from the balance of the information on the page (must be readily visible)? (DoD 5200.1-R, C5.2.8.1)			
10.	**Are TRANSMITTAL documents properly marked to include either its highest classification or a notation "Unclassified when separated from classified enclosures"? (DOD 5200.1-R, C5.3.2))**			
11.	For ELECTRONICALLY transmitted documents:			
	• Is the FIRST item in the text the overall classification? (DoD 5200.1-R, C5.3.5.1)			
	• Is the overall and page marking applied conspicuously to each page? (DoD 5200.1-R, C5.3.5.2)			
	• Does the LAST line include a "Classified by:" or "Derived From:" line and declassification and downgrading instructions? (DoD 5200.1-R, C5.3.5.3)			

ALL PURPOSE CHECKLIST		PAGE 3 OF 6 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA OIG/ Information Security Self-Inspection Checklist		**OPR**	**DATE**	
NO.	**ITEM** ***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)***	YES	NO	N/A
12.	Are Files, Folders, and Groups of documents clearly marked on the outside of the file or folder (attaching a classified document cover sheet to the front of the folder or holder will satisfy this requirement)? (DoD 5200.1-R, C5.3.7)			
13.	Are removable storage media (e.g. magnetic tape reels, disk packs, diskettes, CD-ROMS, removable hard disks, disk cartridges, tape cassettes, etc.) marked with the appropriate Standard Form label (SF-706/707/708/709/710)? (DoD 5200.1-R, C5.4.8)			
	SAFEGUARDING AND STORAGE			
1.	Is classified information removed from storage kept under constant surveillance of authorized persons? (DoD 5200.1-R, C6.3.2.1)			
2.	Are cover sheets placed on all documents removed from storage? (DoD 5200.1-R, Ch 6, para C6.3.2.1)			
3.	Are end-of-day security checks established for areas that process or store classified information to ensure the area is secure at the close of each working day? (DoD 5200.1-R, C6.3.3.3)			
4.	Is the SF-701, Activity Security Checklist, used to record end-of-day checks? (DoD 5200.1-R, C6.3.3)			
5.	Is the SF-702, Security Container Check Sheet, used to record the closing of each vault, secure room, or container used for storage of classified material? (DoD 5200.1-R, C6.3.3)			
6.	Is the SF-700, Security Container Information, properly completed and posted inside the LOCKING drawer of the security container, or inside the door of vault and similar facilities? (DoD 5200.1-R, C6.3.3)			
7.	Are storage containers (safes) that may have been used to store classified information inspected by properly cleared personnel before removal from protected areas or before unauthorized persons are allowed access to them? (DoD 5200.1-R, C6.3.6)			
8.	Are combinations to security containers changed at the required intervals? (DoD 5200.1-R, C6.4.6.2.1)			
9.	If written records of the combination are maintained, are they marked and protected at the highest classification of the material stored therein? (DoD 5200.1-R, C6.4.6.2.3)			
	• Is the combination stored in a security container other than the one for which it is being used?			
10.	Are entrances to secure rooms or areas under visual control at all times during duty hours to prevent unauthorized access or equipped with electric, mechanical or electromechanical access control devices to limit access during duty hours? (DoD 5200.1-R, C6.4.6.3)			
11.	Does each vault or container bear an external marking for identification purpose? NOTE: The level of classification stored therein must NOT be marked on the outside of the container(s). (DoD 5200.1-R, C6.4.6.1)			
12.	Is Top Secret material stored only in a GSA approved security container having one of the following supplemental controls: (DoD 5200.1-R, C6.4.3.1.1))			
	• Continuous (24 hour) protection by cleared guard or duty personnel			
	• Cleared guard or duty personnel inspect the security container every two hours			

ALL PURPOSE CHECKLIST		PAGE 4 OF 6 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA OIG/ Information Security Self-Inspection Checklist		**OPR**	**DATE**	
NO.	**ITEM** ***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)***	YES	NO	N/A
	• An Intrusion Detection System (Alarm System) meeting requirements of Appendix G			
	• Combination lock meeting Federal Specification FF-L-2740 (XO-7) with Security-In-Depth			
13.	Is Secret material stored in a GSA approved security container (safe) without supplemental controls or in the same manner as Top Secret? NOTE: Approved containers will have a certification label on the container itself) (DoD 5200.1-R, C6.4.3.2)			
14.	Is Confidential material stored in a GSA approved security container? (DoD 5200.1-R, C6.4.3.3)			
15.	Are security container repairs (e.g. drilled because of a forgotten combination) done in accordance with DoD 5200.1-R, C6.4.7)?			
16.	Is Information Processing Equipment (IPE) e.g. copiers, facsimile machines, AIS equipment and peripherals, electronic typewriters and word processing systems) used for processing classified information protected from unauthorized access? (D0D 5200.1-R, C6.3.10)			
17.	Do appropriately cleared and technically knowledgeable personnel inspect the IPE before the equipment is removed from the protected areas? (DoD 5200.1-R, C6.3.10.3)			
18.	**Are GSA approved field safes and special purpose one and two drawer lightweight security containers securely fastened to the structure or under sufficient surveillance to prevent their theft? (DoD 5200.1-R, C6.4.3.4.2)**			
	REPRODUCTION OF CLASSIFIED MATERIAL			
1.	Are procedures established to limit the reproduction of classified material? (DoD 5200.1-R, C6.5.1)			
2.	Are personnel, who reproduce classified, aware of the risks involved with the specific reproduction equipment and the appropriate countermeasures they are required to take? (DoD 5200.1-R, C6.5.3.3)			
3.	Are waste products generated during reproduction properly protected and disposed of? (DoD 5200.1-R, C6.5.3.6)			
4.	**Is reproduction equipment specifically designated for the reproduction of classified material? (DoD 5200.1-R, C6.5.3)**			
5.	**Are RULES POSTED on or near the designated equipment authorized for the reproduction of classified? (DoD 5200.1-R, C6.5.3)**			
6.	**Are NOTICES prohibiting reproduction of classified POSTED on equipment used only for the reproduction of unclassified material? (DoD 5200.1-R, C6.5.3)**			
	DISPOSITION AND DESTRUCTION OF CLASSIFIED MATERIAL			
1.	Has each activity with classified holdings set aside at least one "Clean-Out" day each year when specific attention and effort is focused on disposition of unneeded classified material? (DoD 5200.1-R, C6.7.1.2)			

ALL PURPOSE CHECKLIST		PAGE 5 OF 6 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA OIG/ Information Security Self-Inspection Checklist		**OPR**	**DATE**	
NO.	**ITEM** ***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)***	YES	NO	N/A
2.	Is classified materials properly destroyed by approved methods? (DoD 5200.1-R, C6.7.2.1)			
	TRANSMISSION AND TRANSPORTATION OF CLASSIFIED INFORMATION			
1.	Whenever classified information is transmitted outside of the activity is it enclosed in two opaque sealed envelopes or similar wrappings or containers durable enough to properly protect the material from accidental exposure and facilitate detection of tampering? (DoD 5200.1-R, C7.2.1.1)			
	• NOTE: When classified material is hand-carried outside an activity, a locked briefcase may serve as the outer wrapper.			
2.	Is the outer wrapper addressed to an official government activity or to a DoD contractor with a facility clearance and appropriate storage capability with a complete return address of the sender? (DoD 5200.1-R, C7.2.2.1)			
3.	Is the inner wrapper or container marked with the following information: sender's and receiving activity's address and highest classification level of the contents (including , where appropriate, any special markings)			
	• NOTE: The inner envelope may have an "attention line" with a persons name? (DoD 5200.1-R, Ch 7.2.2.2)			
4.	Are procedures established to limit the hand carrying of classified information to only when other means of transmission or transportation can not be used? (DoD 5200.1-R, Ch 7, para 7.3.1.1)			
5.	Are hand-carrying officials briefed on and have they acknowledged their responsibilities for protecting classified information? (DoD 5200.1-R, C7.3.1.2)			
6.	Are courier officials provided a written statement authorizing such hand carrying transmission? (DoD 5200.1-R, C7.3.1.2)			
	• Does the activity list all classified carried or escorted by traveling personnel? (DoD 5200.1-R, C7.3.1.2.8.3)			
	• Does the activity keep this list until all material reaches the recipients activity? (DoD 5200.1-R, C7.3.1.2.8.3)			
7.	Is the DD Form 2501, Courier Authorization card, controlled to preclude unauthorized use? (DoD 5200.1-R, C7.3.2.2.3)			
8.	When "Confidential" classified information is sent U.S. Postal Service "First Class" mail between DoD Components within the United States, is the outer envelope or wrapper endorsed "POSTMASTER: RETUREN SERVICE REQUESTED"? (DoD 5200.1-R, C7.1.4.4)			
9.	Do recipients of First Class mail bearing the "Postmaster" notice protect it as Confidential material?			

ALL PURPOSE CHECKLIST		PAGE 6 OF 6 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA OIG/ Information Security Self-Inspection Checklist		**OPR**	**DATE**	
NO.	**ITEM** ***(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)***	YES	NO	N/A
	SECURITY EDUCATION			
1.	Has the Head of each activity in the Component established a Security Education program? (DoD 5200.1-R, C9.1.1)			
2.	Does this training program include an "Initial Orientation" for all assigned personnel who are cleared for access to classified information? (DoD 5200.1-R, C9.2.1)			
3.	Does this orientation include the: (DoD 5200.1-R, C9.2.1.1-C9.2.2)			
	• Roles and responsibilities of assigned members and key personnel?			
	• Elements of Safeguarding classified information?			
	• Elements of Classifying and Declassifying Information?			
4.	Are training programs established for members who: (DoD 5200.1-R, C9.3.5)			
	• Will be traveling to foreign countries?			
	• Will be escorting, handcarrying, or serving as a courier for classified material?			
	• Will use automated information systems to store, process, or transmit classified?			
5.	Is Refresher training provided at least annually to assigned members? (DoD 5200.1-R, C9.4.2)			
6.	Is Refresher training tailored to the mission needs and address policies, principles and procedures covered in initial training? (DoD 5200.1-R, C9.4.2)			
7.	Does Refresher training address concerns identified during Component Self-Inspections? (DoD 5200.1-R, C9.4.2)			
8.	Are procedures established to ensure cleared employees who leave the organization or whose clearance is terminated receives a termination briefing? (DoD 5200.1-R, C9.5.1)			
9.	Are records maintained to show the names of members who participated in "Initial" and "Refresher" training? (DoD 5200.1-R, C9.6)			
10.	Do training programs for "Uncleared" members include:			
	• The nature and importance of classified information?			
	• Actions to take if they discover classified information unprotected?			
	• The need to report suspected contact with a foreign intelligence collector?			
	SECURITY INCIDENTS AND VIOLATIONS TO INCLUDE COMPROMISES			
1.	Are assigned members aware of their responsibilities to report security violations concerning classified information? (DoD 5200.1-R, C10.1.2.2)			
2.	Do security managers report security incidents & violations to-PFPA/SSD/SS? (AI 26)			
3.	Is an inquiry and/or investigation promptly conducted to ascertain the facts surrounding a reported incident? (DoD 5200.1-R, C10.1.2.6 and AI 26)			

APPENDIX E
CLASSIFIED LABELS
SF-706, TOP SECRET; SF-707, SECRET; SF-708, CONFIDENTIAL; SF-709, CLASSIFIED; SF-710, UNCLASSIFIED; AND SF-711, DATA DESCRIPTOR

APPENDIX F
SF-700, SECURITY CONTAINER INFORMATION

SECURITY CONTAINER INFORMATION

INSTRUCTIONS

1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.
4. DETACH PART 2A AND INSERT IN ENVELOPE.
5. SEE PRIVACY ACT STATEMENT ON REVERSE.

1. AREA OR POST (If required)	2. BUILDING (If required)	3. ROOM NO.
4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		

10. Immediately notify one of the following persons, if this container is found open and unattended.

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

1. ATTACH TO INSIDE OF CONTAINER 700-101 NSN 7540-01-214-5372 **STANDARD FORM 700** (8-85) Prescribed by GSA/ISOO 32 CFR 2003

SECURITY CONTAINER INFORMATION

INSTRUCTIONS

1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.
4. DETACH PART 2A AND INSERT IN ENVELOPE.
5. SEE PRIVACY ACT STATEMENT ON REVERSE.

1. AREA OR POST (If required)	2. BUILDING (If required)	3. ROOM NO.
4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		

10. Persons listed below have knowledge of this container combination.

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

2. 700-101 NSN 7540-01-214-5372 **STANDARD FORM 700** (8-85) Prescribed by GSA/ISOO 32 CFR 2003

WARNING

WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CONTAINER NUMBER

COMBINATION

_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____

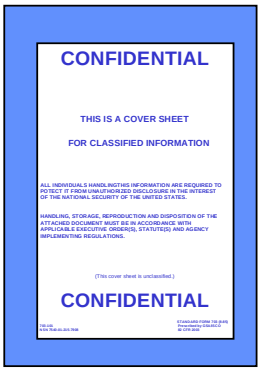
WARNING

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

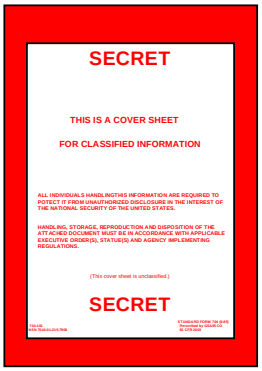
UNCLASSIFIED UPON CHANGE OF COMBINATION.

2A INSERT IN ENVELOPE **SF 700** (8-85) Prescribed by GSA/ISOO 32 CFR 2003

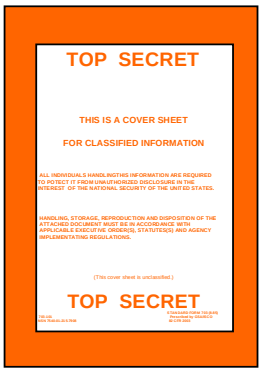
APPENDIX G
CLASSIFIED COVER SHEETS
SF-703, TOP SECRET; SF-704, SECRET; AND SF-705, CONFIDENTIAL



SF 705



SF 704



SF 703

APPENDIX H
OF-23, CHARGE OUT RECORD

OUT

IDENTIFICATION OF RECORD (NUMBER, TITLE AND/OR SUBJECT, DATE OF FILE OR DOCUMENT	CHARGED TO (PERSON & OFFICE)	DATE CHARGED OUT

OPTIONAL FORM 23
FEB 1962
GSA Circular No. 259

CHARGOUT RECORD
5023-101

OUT

DATE CHARGED OUT	CHARGED TO (PERSON & OFFICE)	IDENTIFICATION OF RECORD (NUMBER, TITLE AND/OR SUBJECT, DATE OF FILE OR DOCUMENT

APPENDIX I
SF-702, SECURITY CONTAINER CHECK SHEET

SECURITY CONTAINER CHECK SHEET

TO (if required) | **THRU** (if required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIO AND OPERATING INSTRUCTIONS.

MONTH/YEAR

D A T E	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

—FOLD HERE—REVERSE FOLD FOR FULL USE OF BOTH SIDES—FOLD HERE—

702-101
NSN 7540-01-213-7900

SECURITY CONTAINER CHECK SHEET

FROM | ROOM NO. | BUILDING | CONTAINER NO.

CERTIFICATION

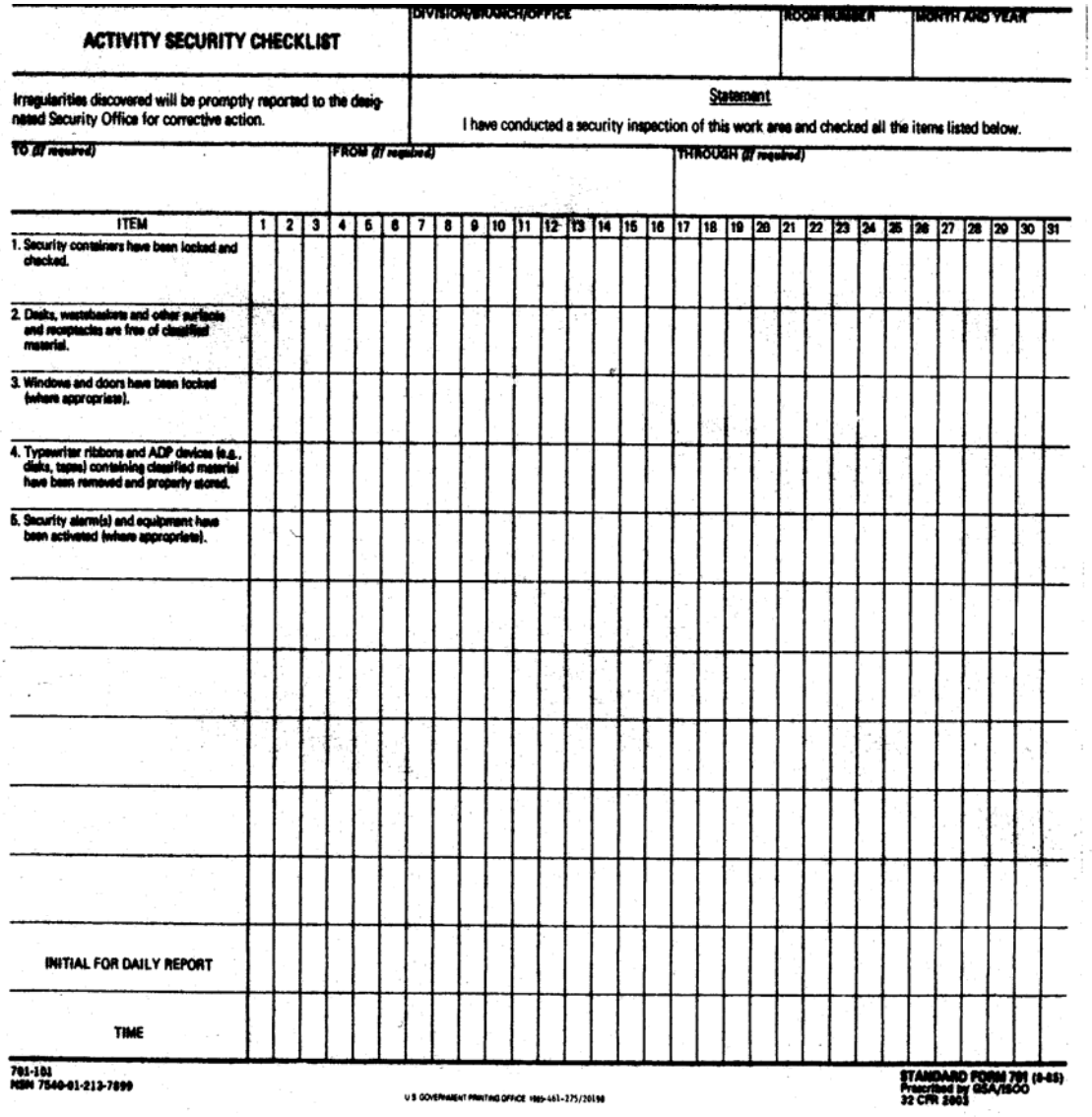
I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

D A T E	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

APPENDIX J
SF-701, ACTIVITY SECURITY CHECKLIST



ACTIVITY SECURITY CHECKLIST	DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR
Irregularities discovered will be promptly reported to the designated Security Office for corrective action.	Statement I have conducted a security inspection of this work area and checked all the items listed below.		
TO (If required)	FROM (If required)	THROUGH (If required)	

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Windows and doors have been locked (where appropriate).																															
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.																															
5. Security alarm(s) and equipment have been activated (where appropriate).																															
INITIAL FOR DAILY REPORT																															
TIME																															

7B1-101
NSN 7540-01-213-7899

U S GOVERNMENT PRINTING OFFICE 1985-461-275/20198

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

APPENDIX K
SF-312, CLASSIFIED INFORMATION NON-DISCLOSURE AGREEMENT

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such inform ation in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and *952, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.

312-102

STANDARD FORM 312 (REV. 1-91)
Prescribed by GSA/ISOO
32 CFR 2003, E.O. 12356

APPENDIX L
VISIT REQUEST LETTER
(Prepare on OIG Letterhead)

(Date)

CIFA
251 18th Street, Suite 1200
Arlington, Virginia 22202

SUBJECT: Visit Request

This certifies the security clearances of the following named individuals, some of whom will visit the facilities listed below.

VISITORS NAME, SSN & D/POB	ACCESS INFORMATION	OIG OFFICE
DOODY, Howdy NMI	Secret 09/26/2002	Audit
222-33-4444	NACLC/08/22/2002	
11/29/51, Anywhere, OH		

All of the above individuals are U.S. citizens.

Facilities to be visited: CIFA

Person to be contacted: Tiny Tim (703) 604-XXXX, FAX (703) 604-1XXX

Period of visit: 02 Jan 08 to 31 Dec 08 (Not to exceed 1 year)

Purpose of visit: OPSEC Brainstorming session

OIG Contact: Oprah Winfrey, (703) 602-0X0X

OIG Security: Joe Snuffy, (703) 604-X0X0

John L. Henry
Chief, Office of Security

"Privacy Act Information" In compliance with the Privacy Act of 1974, this information is Personal Data and must be protected from public disclosure

APPENDIX M
SD FORM 507, TOP SECRET CONTROL OFFICER DESIGNATION FORM

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

TOP SECRET CONTROL OFFICER DESIGNATION FORM

REFERENCES

A. DoD 5200.1-R, "Information Security Program Regulation."

B. PSD ADMINISTRATIVE INSTRUCTION 26, "OSD Information Security Supplement to DoD 5200.1-R."

C. DoD 5200.1-PH, "A Guide to Marking Classified Documents."

By signature below, officials designating Top Secret Control Officers (TSCOs) and alternates, as well as TSCOs accept responsibility for compliance with accountability and control procedures for Top Secret materials as required by references identified above, excerpts of which are cited on the reverse of this form.

The following personnel are designated as Top Secret Control Officers for the Office of _____:

PRIMARY TSCO

NAME *(Last, First, MI)*	PAY GRADE
SIGNATURE	DATE *(YYMMDD)*

ALTERNATE TSCOs

[1] NAME *(Last, First, MI)*	PAY GRADE
SIGNATURE	DATE *(YYMMDD)*
[2] NAME *(Last, First, MI)*	PAY GRADE
SIGNATURE	DATE *(YYMMDD)*
NAME OF DESIGNATING OFFICIAL *(Last, First, MI)*	TITLE OF DESIGNATING OFFICIAL
SIGNATURE	DATE *(YYMMDD)*

NOTE: The original of this form shall be provided to OSD Component Security Managers; copies shall be provided to designated TSCOs and The Director, Physical Security Division, SM&SD, WHS.

SD Form 507, MAR 83

APPENDIX N
TS FORM 02, TOP SECRET CONTROL LOG

TOP SECRET CONTROL LOG

(Please print all information)

CONTROL	NAME	OFFICE	DATE OUT	DATE RETURNED	COMMENT

TSForm 02, May 12, 2000

APPENDIX O
IG FORM 5200.1-8, TOP SECRET REGISTER PAGE

TOP SECRET REGISTER PAGE
(DO NOT enter classified information on this form)

I. DESCRIPTION OF DOCUMENT

1. INDICATE: ORIGINATOR, TYPE OF INFORMATION (Letter, message, plan, vredo-tape, disk, etc.) DATE OF INFORMATION, UNCLASSIFIED SUBJECT TITLE, ORIGINATOR CONTROL NUMBER, COPY NUMBER(S), AND DATE RECEIVED. ALSO USE THESE DATA ELEMENTS FOR DESCRIBING ANY ATTACHMENTS THAT WOULD REQUIRE A RECEIPT IF TRANSMITTED SEPARATELY

II. RECORD OF DOCUMENT CHANGES

2. CHANGE NO..	3. COPY NO.	4. DATE	5. CLASSIFICATION	6. ORIGINATOR	7. ORIGINATOR CONTROL NO.	8. COPY NO. OF BASIC DOCUMENT POSTED TO

III. DISPOSITION OF DOCUMENT

SECTION 1

9.COPY NO.	10. TO	11. DATE	12. TYPE OF ACTION	13. SIGNATURE(S)	
	A.	A.	A. ACCOUNTABILITY TRANSFERRED	A.	
	B.	B.	B. ACTION, REVIEW, OR COORDINATION	B.	
		C.	C. DOCUMENT RETURNED	C.	
		D.	D. DOCUMENT DESTROYED OR	D.	
		E.	E. COMMITTED TO CENTRAL DESTRUCTION FACILITY	E.	
		F.	F. OTHER (Specify)	F.	
		G.	G. AUDITED	G.	

SECTION 2

9.COPY NO.	10. TO	11. DATE	12. TYPE OF ACTION	13. SIGNATURE(S)	
	A.	A.	A. ACCOUNTABILITY TRANSFERRED	A.	
	B.	B.	B. ACTION, REVIEW, OR COORDINATION	B.	
		C.	C. DOCUMENT RETURNED	C.	
		D.	D. DOCUMENT DESTROYED OR	D.	
		E.	E. COMMITTED TO CENTRAL DESTRUCTION FACILITY	E.	
		F.	F. OTHER (Specify)	F.	
		G.	G. AUDITED	G.	

14. REGISTER PAGE NO.	15. RECONTROLLED TO REGISTER PAGE NO.	16. RECONTROLLED TO REGISTER PAGE NO.

IG Form 5200.1-8, October 8, 1987

APPENDIX P
IG FORM 5200.1-5, TOP SECRET ACCESS RECORD AND COVER SHEET

TOP SECRET ACCESS RECORD AND COVER SHEET

The following personnel have been given access to or disclosure of information in the attached document on the date shown. DO NOT enter classified information on this form. Only record initial access to or disclosure of the information.

NAME AND GRADE	FUNCTIONAL ADDRESS SYMBOL	DATE

ORIGINATOR OF TOP SECRET DOCUMENT	ORIGINATOR CONTROL NUMBER	REMARKS
REGISTER PAGE NUMBER	DATE ACCOUNTABILITY TERMINATED	

IG FORM 5200.1-5, October 1987

APPENDIX Q
IG FORM 5200.1-1, AUTHORIZATION FOR REPRODUCTION OF CLASSIFIED MATERIAL

AUTHORIZATION FOR REPRODUCTION OF CLASSIFIED MATERIAL

REQUESTOR: (Name and Office Symbol)	CLASSIFICATION	NUMBER OF PAGES OF ORIGINAL DOCUMENT	DATE OF REQUEST

UNCLASSIFIED DESCRIPTION OF MATERIAL (Subject, date, originator)	NO. OF COPIES: (requested)	NO. OF COPIES: (reproduced)
	NAME OF PERSON REPRODUCING COPIES	

DISTRIBUTION OF MATERIAL:

The person shown above is authorized to reproduce the classified material described. The person reproducing the copies will physically Account For All Copies.

SIGNATURE OF AUTHORIZING OFFICIAL:	DATE

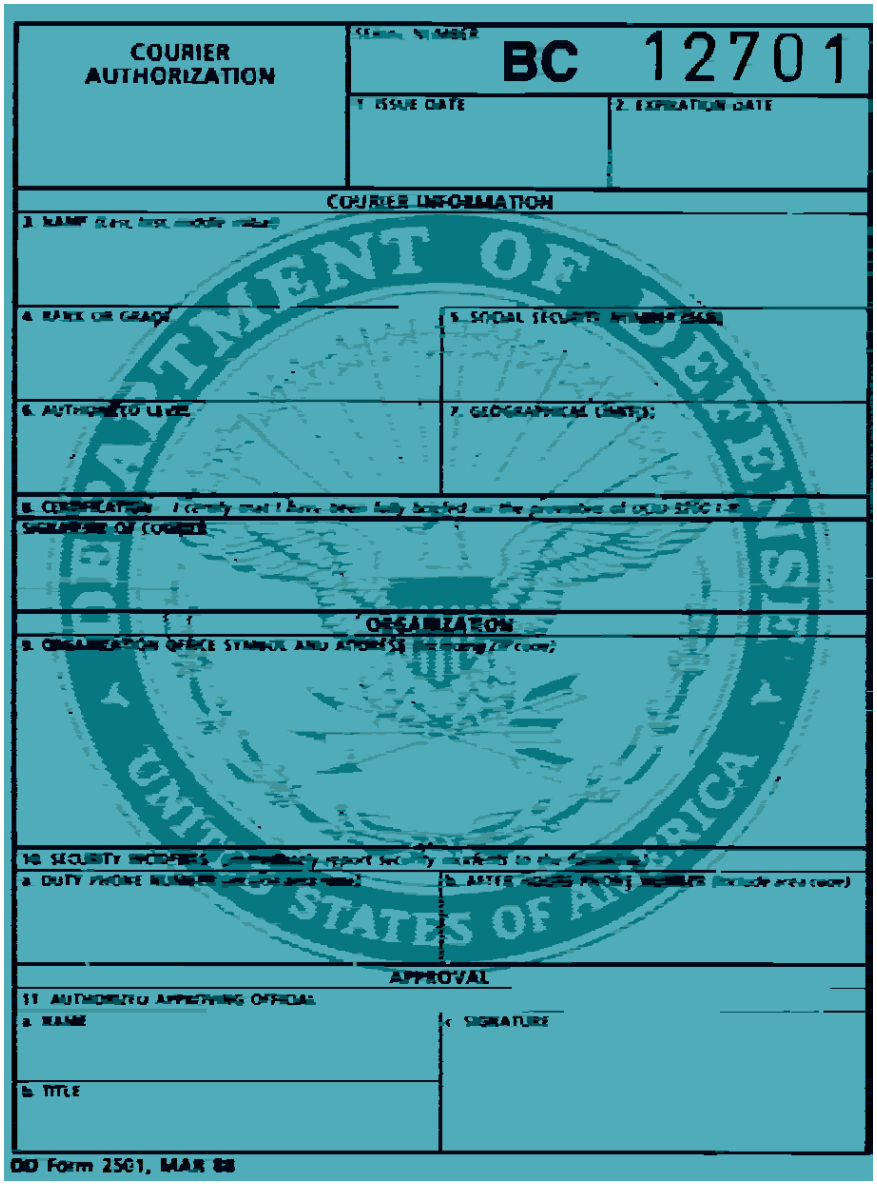
SIGNATURE OF SECURITY OFFICER	DATE

IG FORM 5200.1-1 October 1999 PREVIOUS EDITION OBSOLETE

Instructions:

1. **The distribution of the reproduced copies MUST be annotated in the DISTRIBUTION OF MATERIAL box before approval.**
2. **A copy of this form MUST be retained with the original document.**
3. **The original copy of this form is given to the Reprographic Facility Personnel after reproduction of the material.**

APPENDIX R
DD FORM 2501, COURIER AUTHORIZATION



COURIER AUTHORIZATION

BC 12701

1. ISSUE DATE

2. EXPIRATION DATE

COURIER INFORMATION

3. NAME (Last, first, middle initial)

4. RANK OR GRADE

5. SOCIAL SECURITY NUMBER (SSN)

6. AUTHORIZED USER

7. GEOGRAPHICAL LIMIT(S)

8. CERTIFICATION I certify that I have been fully briefed on the provisions of DOD 5200.1-R

SIGNATURE OF COURIER

ORGANIZATION

9. ORGANIZATION OFFICE SYMBOL AND ADDRESS (Including ZIP Code)

10. SECURITY INCIDENTS (Immediately report security incidents to the Commander)

a. DUTY PHONE NUMBER (Include area code)

b. AFTER HOURS PHONE NUMBER (Include area code)

APPROVAL

11. AUTHORIZED APPROVING OFFICIAL

a. NAME

c. SIGNATURE

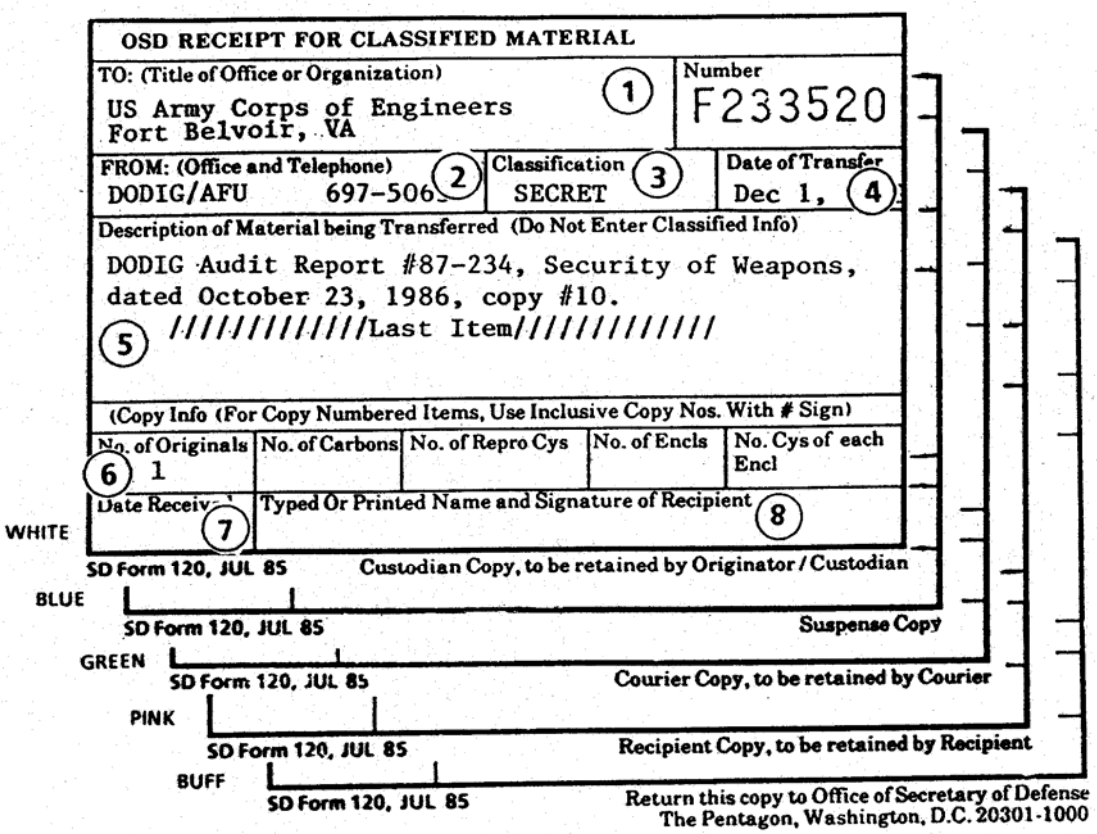
b. TITLE

DD Form 2501, MAR 88

APPENDIX S
SD FORM 120, OSD RECEIPT FOR CLASSIFIED MATERIAL

How to Prepare SD Form 120

1. Functional address and location.
2. Functional address, location, and telephone number.
3. Classification level of classified documents.
4. Date the material is transmitted from the sending office.
5. Completely describe each classified attachment. When a subject or title is classified, use the unclassified short title. If the document is a message, use the identification elements.
6. Show the number of copies of each attachment and enclosure.
7. Date material received.
8. Self-explanatory.



APPENDIX T
DESIGNATION OF CLASSIFIED DOCUMENT CARRIER MEMORANDUM

(Prepare on OIG Letterhead)

(Date)

MEMORANDUM FOR AIRPORT SECURITY SCREENING STATION REPRESENTATIVE,
AIR CARRIER REPRESENTATIVE, AIR CREW MEMBER(S)

SUBJECT: Designation of Classified Document Carrier

The following named individuals are designated as couriers for transporting classified material from **Washington DC/DCA and Miami International.** The sealed package measures **approximately 12 x 15 inches** c**ourier bag**.

The designated courier shall present, upon request, a Military or Government identification card or picture ID.

The package shall remain in the courier's possession at all times. While the package may be screened, we request that it remain sealed and not be opened for visual inspection. The individuals listed below will travel as follows:

Name	**SSN**	**Courier Card #**
Joe Blow Jr.	*111-22-3456*	*AA 12630*

Travel/Flight Itinerary

Date/Time Dep.	**Carrier/Flt#**	**Dep Location**	**Arr Location**	**Date/Time Arr.**
7 Aug/1456	*AA/749*	*Wash DC/DCA*	*Miami Intl*	*7 Aug/1730*
9 Aug/0654	*AA/684*	*Miami Intl*	*Wash DC/DCA*	*9 Aug/0915*

The classified material shall be secured at final destination, **Washington DC.** If the courier/traveler officially deviates from travel itinerary, he or she is responsible for ensuring the package is safeguarded in accordance with DOD 5200.1-R, *DoD Information Security Program Manual*. The Office of Inspector General, Office of Security may be contacted for assistance.

During business hours, questions relating to this matter should be directed to: **XXXXX, Information Security Program Manager**, **703-604-9717.** This courier authorization supplements the individual's current courier card and expires upon courier's completion of this specific travel**.**

XXX XXXXXX
Information Security Program Manager

APPENDIX U
COURIER PRE-DEPARTURE CHECKLIST

COURIER PRE-DEPARTURE CHECKLIST

1. Do you have appropriate authorization? (Courier Authorization Letter or DD Form 2501, *Courier Authorization Card*)

2. Is the Courier Authorization Letter or DD Form 2501 dated?

3. Did you receive a courier briefing? If so, is there documentation to show this?

4. Does Block 16 of DD Form 1610, *Request and Authorization for TDY Travel of DoD Personnel*, contain the following statements (for TDY abroad)?

   a. Traveler (is or is not) authorized to disclose classified information.

   b. Traveler (is or is not) authorized to carry classified material.

   c. Traveler is aware of applicable export control, foreign disclosure, and security requirements. (This statement is to be used if either or both 4a and 4b above indicate that classified information is involved.)

   d. Has the Chief, Office of Security, or Component security manager applied his or her signature to Block 16 of DD Form 1610, thus indicating that the traveler has complied with the above requirements?

   e. Have travel orders identified the traveler by name, title, and organization, and include the traveler's passport or identification number? Do they describe the route to be taken by the traveler? (The traveler's itinerary may be attached for this purpose.)

5. Does the inner envelope:

   a. Have a full destination and return address?

   b. Have appropriate classification markings and additional warning notices?

   c. Have sufficient wrapping to provide security protection, prevent contents from breaking out, and provide for the detection of tampering?

6. Does the outer envelope:

   a. Have a full destination and return address?

   b. Have a classification marking and additional warning notices? ***(This is prohibited, please correct immediately!)***

   c. Have sufficient wrapping to provide security protection, prevent contents from breaking out, and provide for the detection of tampering?

7. Have prior arrangements with a military installation or cleared contractor facility been made to allow for proper storage during overnight stops?

APPENDIX V
IG FORM 5200.1-10, CLASSIFIED MATERIAL DESTRUCTION CERTIFICATE

CLASSIFIED MATERIAL DESTRUCTION CERTIFICATE			
TO:	FROM: (Office or Agency)		
DESCRIPTION OF MATERIAL	**DATE OF DOCUMENT**	**COPY NO. (If Any)**	**NUMBER OF COPIES**
The material listed above has been (destroyed) (committed to the central destruction facility) according to IGDM 5200.1/DoD 5200.1-R.		DATE	
Signature of Destruction/Commited to Destruction Official (Type or Print name)	Signature of Witnessing Official (Type or Print Name)		

IG Form 5200.1-10, October 1987

APPENDIX W
DD FORM 2843, CLASSIFIED MATERIAL DESTRUCTION RECORD

FOR OFFICIAL USE ONLY

CLASSIFIED MATERIAL DESTRUCTION RECORD		
1. DATE *(YYYYMMDD)*	2. MILITARY DEPARTMENT OR AGENCY NAME	
3. OFFICE SYMBOL OR COMPONENT NAME		4. TELEPHONE NUMBER *(Include Area Code)*
5. NUMBER OF BAGS (NOTE: There is a ten (10) pound weight limit per bag.)		
a. NUMBER OF UNCLASSIFIED BAGS		
b. NUMBER OF CONFIDENTIAL BAGS		
c. NUMBER OF SECRET BAGS		
d. NUMBER OF TOP SECRET BAGS		
e. NUMBER OF SCI BAGS		
f. TOTAL NUMBER OF BAGS		0
g. REMARKS		
6. NAME OF DELIVERY PERSON(S) *(Delivery person be cleared at the same level of, or higher than the material delivered.)*		
7. RECEIVED BY *(To be completed by incinerator plant personnel/driver)*		
DEPARTMENT OF DEFENSE CLASSIFIED WASTE FACILITY 425 OLD JEFFERSON DAVIS HIGHWAY ARLINGTON, VA 22202	TELEPHONE: (703) 695-1828 or (703) 695-2265	

DD FORM 2843, SEP 2001

FOR OFFICIAL USE ONLY

Reset

APPENDIX X
IG FORM 5200.2-1, SECURITY TERMINATION STATEMENT

DEPARTMENT OF DEFENSE
OFFICE OF THE INSPECTOR GENERAL

SECURITY TERMINATION STATEMENT

I am aware that my authorization for access to classified information with the Office of the Inspector General, DoD is hereby terminated in view of my pending termination of employment and/or assignment, administrative withdrawal of my security clearance, or any absence from duty for 60 days or more. I am aware of my continuing responsibility for safeguarding the classified information.
I HEREBY CERTIFY THAT:

1. I have read the provisions of the Espionage Act, Title 18, U.S. Code, Section 793 and 794, and other criminal statutes and understand the implications thereof.

I understand that one who unlawfully divulges information affecting the national defense is subject to severe criminal penalties and that the making of a false statement herein may be punished as a felony under Title 18, U.S. Code, Section 1001.

2. I have surrendered all material and documents containing classified information in my possession.

3. I shall not hereafter communicate or transmit classified information orally or in writing to any unauthorized person or agency.

4. I shall report without delay to the Federal Bureau of Investigation, to an appropriate military authority, or the OIG, DoD, Security Office, any attempt by any unauthorized person to solicit classified information.

5. I understand that my refusal to execute a Security Termination Statement will result in a verbal debriefing and such refusal will be reported to the Director, Defense Investigative Services, for subsequent recording in the Defense Central Index of Investigations.

REFUSAL TO SIGN - ORAL DEBRIEFING

"Oral briefing conducted:
Individual refused to sign."

_____
Debriefer Signature (Date)

_____
Typed/Printed Name

_____
Witness Signature (Date)

_____
Typed/Printed Name

_____
Signature (Date)

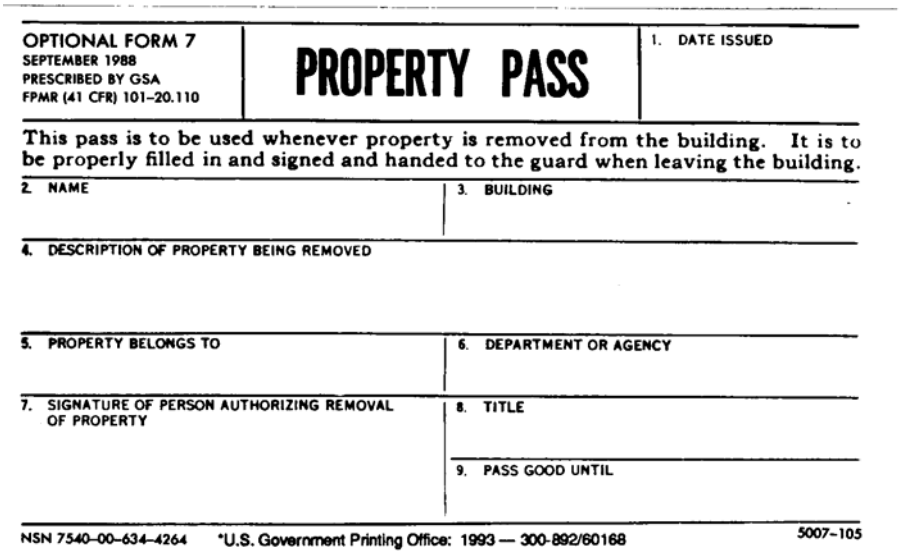
_____
Typed/Printed Name

_____
Debriefer Signature (Date)

_____
Typed/Printed Name

IG Form 5200.2-1, October 1987 (EG)

APPENDIX Y
OF-7, PROPERTY PASS



OPTIONAL FORM 7
SEPTEMBER 1988
PRESCRIBED BY GSA
FPMR (41 CFR) 101–20.110

PROPERTY PASS

1. DATE ISSUED

This pass is to be used whenever property is removed from the building. It is to be properly filled in and signed and handed to the guard when leaving the building.

2. NAME

3. BUILDING

4. DESCRIPTION OF PROPERTY BEING REMOVED

5. PROPERTY BELONGS TO

6. DEPARTMENT OR AGENCY

7. SIGNATURE OF PERSON AUTHORIZING REMOVAL OF PROPERTY

8. TITLE

9. PASS GOOD UNTIL

NSN 7540-00-634-4264 *U.S. Government Printing Office: 1993 — 300-892/60168 5007-105

APPENDIX Z

BRIEFING/REBRIEFING/DEBRIEFING CERTIFICATE

SECTION A - GENERAL

1. NAME: _____

2. DUTY POSITION: _____ 3. PHONE NUMBER: _____

4. ORGANIZATION: _____ 5. ADDRESS: _____

SECTION B - BRIEFING

6. I certify that I have (read) (been briefed) and fully understand the procedures for handling (COSMIC) (ATOMAL) (NATO SECRET) (NATO CONFIDENTIAL) material and am aware of my responsibility for safeguarding such information and that I am liable to prosecution under Sections 793 and 794 of Title 18, U.S.C., if either by intent or negligence I allow it to pass into unauthorized hands.

7. SIGNATURE OF INDIVIDUAL: _____ DATE: _____

8. SIGNATURE OF BRIEFER: _____ DATE: _____

SECTION C - ATOMAL REBRIEFING

9. I certify that I have been rebriefed and fully understand the procedures for handling ATOMAL material and am aware of my responsibility to safeguard such information.

SIGNATURE AND DATE SIGNATURE AND DATE

_____

_____

_____

_____

_____

SECTION D - DEBRIEFING

10. I have been debriefed for (COSMIC) (ATOMAL) (NATO SECRET) (NATO CONFIDENTIAL) and I understand that I must not disclose any classified information which I have obtained in my assignment to this organization or in connection therewith. I also understand that I must not make any such classified information available to the public or to any person not lawfully entitled to that information. I further understand that any unauthorized disclosure of such classified information, whether public or private, intentional or unintentional, will subject me to prosecution under applicable laws.

SIGNATURE OF INDIVIDUAL: _____ DATE: _____

SIGNATURE OF CONTROL OFFICER: _____ DATE: _____