



U.S. DEPARTMENT OF
ENERGY

Office of Health,
Safety and Security

Classified Matter Protection and Control Policy Resource & Information Tool (CPRIT)



*Classified Matter Protection and Control
Policy Resource & Information Tool (CPRIT)*

July 2009

Purpose

The DOE M 470.4-4A, *Information Security Manual* states, “All information security programs, practices, and procedures developed within DOE must be consistent with and incorporate the requirements of this Manual along with all of the national requirements (Atomic Energy Act, Executive Orders, Code of Federal Regulations, United States Code, National Industrial Security Operations Manual, etc.). All these national information security requirements must be reviewed and incorporated because requirements have not been repeated in this Manual.”

Because DOE M 470.4-4A does not duplicate national policy requirements, this document, the Classified Matter Protection and Control Policy Resource and Information Tool (CPRIT), was developed to assist the user in finding those national policy directives that relate to Classified Matter Protection and Control (CMPC) and assist in local implementation.

Contents

Purpose.....	iii
How to Use This Tool.....	1
Responsibilities for Classified Matter Protection and Control	3
Deviations to Classified Matter Protection and Control	5
Definitions Within Classified Matter Protection and Control.....	6
Section A—Classified Matter Protection and Control	7
Chapter I. Protection and Control Planning	7
Classified Matter Protection and Control Program Implementation, Strategies and Planning.....	8
Disclosure and Release of Classified Matter	10
Classified Matter Protection and Control Training.....	12
Chapter II. Classified Matter Protection and Control Requirements.....	13
Classified Matter Protection and Control General Requirements.....	14
Classified Matter in Use.....	17
Marking Classified Matter	19
Control Systems and Accountability for Classified Matter	21
Reproduction of Classified Matter	23
Receiving and Transmitting Classified Matter	24
Destruction of Classified Matter	26
Classified Foreign Government Information	27
Chapter III. Storage Requirements for Classified Matter.....	29
Storage of Classified Matter	30
Appendix A Forms Usage in Classified Matter Protection and Control Programs	A.1
Appendix B Examples of Forms Usage in Classified Matter Protection and Control Programs.....	B.1

Tables

1	References for Additional Requirements for CMPC	4
2	References for Additional Requirements for Deviations to CMPC.....	5
3	References for Additional Requirements for Definitions Within CMPC	6
4	References for Additional Requirements for CMPC Program Implementation, Strategies and Planning	9
5	References for Additional Requirements for Closure and Release of Classified Matter.....	11
6	References for Additional Requirements for CMPC Training	12
7	References for Additional Requirements for CMPC	15
8	References for Additional Requirements for Classified Matter in Use	18
9	References for Additional Requirements for Marking Classified Matter.....	20
10	References for Additional Requirements for Control Systems and Accountability for Classified Matter.....	22
11	References for Additional Requirements for the Reproduction of Classified Matter.....	23
12	References for Additional Requirements for Receiving and Transmitting Classified Matter	25
13	References for Additional Requirements for the Destruction of Classified Matter.....	26
14	References for Additional Requirements for Classifying Foreign Government Information.....	27
15	References for Additional Requirements for Storing Classified Information	31

How to Use This Tool

This tool may be used in conjunction with DOE M 470.4-4A when developing local CMPC programs. **No requirements are established in this document and its use or application is discretionary.** The references and other resources found within address the major elements of a CMPC program. However, given the diversity of options on implementing a CMPC program, these resources are not comprehensive.

The sequence of topics included in this tool corresponds with those in DOE M 470.4-4A through Section A, CMPC. National policy references that relate to each CMPC topic are listed under the respective section. When specific paragraphs apply, they are listed along with the title or language of the referenced section. In some cases, entire sections or chapters are applicable. U.S. Department of Energy (DOE) directives listed in DOE M 470.4-4A have generally not been included, as employees and contractors should already be familiar with them. There may be differences in terminology from one referenced directive to another, and it may be necessary to use more than one source directive to determine the requirements for a given topic.

The objectives stated in each section are not intended to modify DOE or national directive requirements. The objectives are simple statements provided as concepts that should be kept in mind when discerning the meaning and applicability of various requirements.

Key words are provided as an additional resource to search for requirements related to particular topics. The entire set of key words is not comprehensive, nor is each one necessary for each user of this document.

Some, but not all, of the topics include additional helpful information. For example, if different terminology is used by different directives when they address the same concept, a brief explanation may be provided to clarify how the terms are inter-related. Again, this information does not establish or modify any requirement; it should only be used if done so consistent with applicable requirements.

The suggested references are source documents, section/chapters and associated titles for use in locating additional requirements related to the topic.

Appendix A contains copies of forms commonly used in CMPC.

Classified information exists in many forms. Written documents, verbal communication, the shape of a weapon part, electronic data or digital data are examples. The life cycle of classified information, which exists as or is contained within physical forms, undergoes the following activities:

Protection in Use

- Origination
- Classification Review
- Marking
- Control Systems and Accountability
- Reproduction
- Receipt and Transmission
- Destruction

Storage

Cyber security is a separate security discipline that is not directly addressed in this document because it is governed by other DOE and national directives.

Responsibilities for Classified Matter Protection and Control

Objective

Establish the individuals and offices with authorities and responsibilities to ensure U.S. Department of Energy (DOE) classified information and classified matter are protected from theft, unauthorized disclosure, loss, or compromise, whether in use or in storage.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to responsibilities for CMPC: DOE Cognizant Security Authority; DOE CSA; Cognizant Security Authority; CSA; ACREM Custodian; Alternate ACREM Custodian; Custodian; Administrator of the National Nuclear Security Administration; departmental element; contracting officer; contractor; heads of field elements; headquarters departmental elements; Deputy Administrator for Naval Reactors; deputy administrator; CMPC point of contact; point of contact; Associate Administrator for Defense Nuclear Security; DOE line management; line management; National Disclosure Policy Committee; Deputy Administrator, Defense Nuclear Nonproliferation; General Counsel, the Office of Health, Safety and Security; receiving government; personnel with security clearances; individual; responsible; responsibilities.

General Responsibility Information

DOE Directives

The current DOE classified matter protection and control (CMPC) policy is primarily found in the following directives:

- DOE M 470.4-1 Change 1, Chg. 1, *Safeguards and Security Program Planning and Management*. This manual establishes overall responsibilities within the Safeguards and Security program, to include deviations from Safeguard and Security policies.
- DOE M 470.4-4A, *Information Security*. This manual provides specific responsibilities for individuals required to protect classified information throughout the CMPC cycle.
- DOE Order 5610.2, *Control of Weapon Data*, 8/1/1980. This order sets the access policy and marking requirements for Sigma 1-13.
- DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Designs*, 3/11/2004. This manual provides Sigma 14 and 15 access policy.
- DOE Manual 457.1-1A, *Control of Improvised Nuclear Device Information*, 08/10/2006. This manual provides Sigma 20 access policy.

Related Applicable National Policy Requirements

Each national policy document provides additional responsibilities for compliance with the responsibilities for CMPC.

Table 1 lists references for additional requirements for CMPC.

Table 1. References for Additional Requirements for CMPC

Executive Order (E.O.) 12333, as Amended, Sec. 1.3	National Foreign Intelligence Advisory Groups
Executive Order (E.O.) 12333, as Amended, Sec. 1.4	Intelligence Community
Executive Order (E.O.) 12333, Sec. 1.6	The Department of Energy
Executive Order (E.O.) 12333, as Amended, Sec. 1.7 (i)	Senior Officials of the Intelligence Community
Executive Order (E.O.) 12333, as Amended, Sec. 1.12	Intelligence Components Utilized by the Secretary of Defense
E.O. 12829, Part 1	Establishment (<i>of NISP</i>) and Policy
E.O. 12829, Part 2	Operations (<i>NISPOM & ISOO</i>)
E.O. 12968, Sec. 6.1	Agency Implementing Responsibilities
E.O. 12968, Sec. 6.2	Employee Responsibilities
E.O. 13142,	Amendment to E.O. 12958, (<i>automatic declassification & ISOO</i>)
E.O. 13292, Sec. 5.4	General Responsibilities
E.O. 13462, Sec. 8	Functions of Heads of Departments Concerned and Additional Functions of the Director of National Intelligence
NISPOMSUP 1-200	Responsibilities
NISPOM 1-201	Facility Security Officer (FSO)
NISPOM, Chapter 7, Sec. 1	Prime Contractor Responsibilities (<i>entire section</i>)
NISPOM, Sec. 8-105	Users of IS (<i>information systems</i>)

Deviations to Classified Matter Protection and Control

Objective

Establish protocol to determine type of deviation and procedure to request approval of a deviation to a requirement while ensuring the protection of classified information from theft, unauthorized disclosure, loss, or compromise at all times.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to deviations to CMPC: deviation, variance, waiver, exception, exclusion, exemption.

General Deviation Information

DOE Directives

The current U.S. Department of Energy (DOE) deviation policy and Classified Matter Protection and Control (CMPC) requirements are primarily found in two directives:

- DOE M 470.4-1 Change 1, *Safeguards and Security Program Planning and Management*. This manual establishes overall responsibilities within the Safeguards and Security program and procedures to request or grant deviations from Safeguard and Security policies.
- DOE M 470.4-4A, *Information Security*. This manual provides specific responsibilities and requirements to follow within the CMPC cycle to which deviations may be required. Non-conforming storage procedures and burial requirements are discussed within this manual.

Related Applicable National Policy Requirements

Each national policy document provides procedures to request deviations (variances, waivers, exemptions, exceptions, etc.) from the requirements for that document.

Table 2 lists references for additional requirements for deviations to CMPC.

Table 2. References for Additional Requirements for Deviations to CMPC

10 CFR 1016, § 1016.6	Specific Waivers
32 CFR 2004, § 2004.20	National Industrial Security Program Operating Manual (NISPOM)
32 CFR 2003, § 2003.3	Waivers.
E.O. 13292, Sec. 1.6	Identification and Markings
E.O. 13292, Sec. 4.4	Access by Historical Researchers and Certain Former Government Personnel
NISPOMSUP 1-106	Waivers and Exceptions
NISPOM 1-107	Waivers and Exceptions to this Manual

Definitions Within Classified Matter Protection and Control

Objective

Ensure understanding of definition of terms used within the Safeguards and Security classified matter protection and control (CMPC) program to ensure that U.S. Department of Energy (DOE) classified information and classified matter is protected from theft, unauthorized disclosure, loss, or compromise.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to definitions within CMPC: definition.

General Definition Information

DOE Directives

The current DOE definitions for CMPC terms are primarily found in two directives:

- DOE M 470.4-4A, *Information Security*. This manual articulates which security containers, security areas, and other security measures are required for protecting information of a specific classification.
- DOE M 470.4-7, *Safeguards and Security Program References*. This manual provides the definitions used in the CMPC program.

Related Applicable National Policy Requirements

Each federal regulation provides definitions within its policy documents. If there is any question concerning the use of a term, contact the Office of Policy for clarification.

Table 3 lists references for additional requirements for definitions within CMPC.

Table 3. References for Additional Requirements for Definitions Within CMPC

E.O. 12968, Sec. 1.1	Definitions
E.O. 12968, Sec. 1.2	Access to Classified Information
E.O. 12972	Amendment to E.O. 12958 (agency definition)
E.O. 13292, Sec. 6.1	Definitions
NISPOM APPENDIX C,	Definitions
E.O. 12968, Sec. 1.1	Definitions
E.O. 12968, Sec. 1.2	Access to Classified Information

Section A—Classified Matter Protection and Control

Chapter I. Protection and Control Planning

Classified Matter Protection and Control Program Implementation, Strategies and Planning

Objective

Ensure that a classified matter protection and control (CMPC) program is developed and implemented to ensure the protection of U.S. Department of Energy (DOE) classified information from theft, unauthorized disclosure, loss, or compromise.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to definitions within CMPC: program plan, security plan, implementation plan.

General CMPC Program Implementation, Protection Strategies & Planning Requirements

DOE Directives

The current DOE policy for development and implementation of a CMPC program classified matter is primarily found in three directives:

- DOE M 470.4-1 Change 1, *Safeguards and Security Program Planning and Management*. This manual establishes overall responsibilities within the Safeguards and Security program and procedures to develop Safeguards and Security policies, procedures and plans.
- DOE M 470.4-2 Change 1, *Physical Protection*. This manual defines physical security requirements for containers and security areas, establishing or otherwise presenting the requirements that pertain to the physical characteristics of those items necessary for the completion of security plans, self-assessments, and inspections.
- DOE M 470.4-4A, *Information Security*. This manual provides specific instances within the CMPC cycle which are included in security plans, procedures, and training.

Related Applicable National Policy Requirements

Table 4 lists references for additional requirements for CMPC program implementation, strategies and planning.

Table 4. References for Additional Requirements for CMPC Program Implementation, Strategies and Planning

10 CFR 1016, § 1016.43	Inspections
32 CFR 2001, § 2001.60	General
32 CFR 2001, § 2001.61	Coverage
NSDD 84	Safeguarding National Security Information
NISPOMSUP 1-201	Standard Operating Procedures (SOP)
NISPOMSUP 1-206	Security Reviews
NISPOM 1-202	Standard Practice Procedures
NISPOM 1-206	Security Reviews

Disclosure and Release of Classified Matter

Objective

Ensure U.S. Department of Energy (DOE) classified information is only released, disclosed, or otherwise provided to authorized individuals who have the appropriate clearance, formal access authorization, and need-to-know regardless of the method used.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to the disclosure and release of classified matter: access, access authorization, badge, need-to-know, need to know, release, disclosure, disclose, transmission, transmit, transfer, discussion, discuss, presentation, briefing, meeting, visit, visitor, assignee, uncleared, building-only access, facsimile, FAX, e-mail, e Mail, email, voice mail, public, infraction, violation, incident, civil penalties, emergency, emergencies, restrictions.

General Disclosure and Release Requirements

DOE Directives

The current DOE policy for control of access to classified matter is primarily found in nine directives:

- DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management*. This manual establishes program planning and management requirements for the DOE's Safeguards and Security.
- DOE M 470.4-2, Chg. 1, *Physical Protection*. This manual establishes requirements for the physical protection of Safeguards and Security interests.
- DOE M 470.4-4A, *Information Security*. This manual articulates the requirement to establish the ability and authorization of the individual to which classified information is provided whether verbally or physically by direct action or by omission of one or more protective measures.
- DOE M 470.4-5, *Personnel Security*. This manual establishes the overall objectives and requirements for the DOE Personnel Security Program.
- DOE M 475.1-1B, *Manual for Identifying Classified Information*. This manual provides detailed requirements to supplement DOE O 475.2, *Identifying Classified Information*.
- DOE O 475.2, *Identifying Classified Information*. This order establishes the program to identify information classified under the Atomic Energy Act [Restricted Data (RD) and Formerly Restricted Data (FRD)] or Executive Order 12958, as amended [National Security Information (NSI)], so that it can be protected against unauthorized dissemination.
- DOE Order 5610.2, *Control of Weapon Data*, 8/1/1980. This order sets the access policy and marking requirements for Sigma 1-13.
- DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Designs*, 3/11/2004. This manual provides Sigma 14 and 15 access policy.

- DOE Manual 457.1-1A, *Control of Improvised Nuclear Device Information*, 08/10/2006. This manual provides Sigma 20 access policy.

Related Applicable National Policy Requirements

Table 5 lists references for additional requirements for closure and release of classified matter.

Table 5. References for Additional Requirements for Closure and Release of Classified Matter

18 USC 798	Disclosure of Classified Information
10 CFR PART 1044	Security Requirements For Protected Disclosures
10 CFR 1046	Physical protection of security interests
32 CFR 1909	Access by Historical Researchers and Former Presidential Appointees Pursuant To 4.5 of Executive Order 12958
32 CFR 2001, § 2001.51	Emergency authority
48 CFR 970, § 970.5245-1	Property
E.O. 12968, Sec. 2	Access Eligibility Policy and Procedure (<i>entire section</i>)
E.O. 12333, as Amended, Sec.1.5	Director of Central Intelligence
E.O. 13292, Sec. 4.1	General Restrictions on Access
E.O. 13292, Sec. 4.2	Distribution Controls
E.O. 13292, Sec. 4.4	Access by Historical Researchers and Former Presidential Appointees
NSDD 19	Protection of Classified National Security Council and Intelligence Information
NISPOMSUP 2-201	Program Accessing Requirements and Procedures
NISPOM 1-208	Classified Information Procedures Act (CIPA)
NISPOM 1-303	Reports of Loss, Compromise, or Suspected Compromise
NISPOM 5-101	Safeguarding Oral Discussions
NISPOM 5-104	Emergency Procedures
NISPOM 5-501	Disclosures to Employees
NISPOM 5-502	Disclosure to Subcontractors
NISPOM 5-503	Disclosure between Parent and Subsidiaries
NISPOM 5-504	Disclosure in an MFO
NISPOM 5-505	Disclosure to DoD Activities
NISPOM 5-506	Disclosure to Federal Agencies
NISPOM 5-507	Disclosures of Classified Information to Foreign Persons
NISPOM 5-508	Disclosure of Export Controlled Information to Foreign Persons
NISPOM 5-509	Disclosure to Other Contractors
NISPOM 5-510	Disclosure of Classified Information in Connection with Litigation
NISPOM 5-511	Disclosure to the Public
NISPOM Chapter 6	Visits and Meetings (<i>entire chapter</i>)

Classified Matter Protection and Control Training

Objective

Ensure U.S. Department of Energy (DOE) employees and contractors have been sufficiently trained in order to protect classified information and matter from theft, unauthorized disclosure, loss, or compromise.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to classified matter protection and control training: the brief, briefing, training, initial training, specialized training, detailed training.

General Training Requirements

DOE Directives

The current DOE policy for Classified Matter Protection and Control (CMPC) training requirements is primarily found in three directives:

- DOE M 470.4-1 Change 1, *Safeguards and Security Program Planning and Management*. This manual establishes overall requirements for the National Training Center and for Safeguards and Security training programs.
- DOE M 470.4-4A, *Information Security*. The information security manual provides specific responsibilities by individuals required to protect classified information throughout the CMPC cycle.
- DOE M 470.4-5, *Personnel Security*. This manual provides the initial training requirements when access authorizations (clearances and/or security badges) are provided to employees for the first time, and for annual security refresher briefing content.

Related Applicable National Policy Requirements

Table 6 lists references for additional requirements for CMPC training.

Table 6. References for Additional Requirements for CMPC Training

10 CFR Part 824	Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations
32 CFR Part 2001, Section 2001.70	General
32 CFR Part 2001, Section 2001.71	Coverage
E.O. 13292, Sec. 4.1	General Restrictions on Access
E.O. 13292, Sec. 5.4	General Responsibilities.
NISPOMSUP, Chapter 3, Sec. 1	Security Training and Briefings (<i>entire section</i>)
NISPOM 1-205	Security Training and Briefings
NISPOM, Chapter 3	Security Training and Briefings (<i>entire chapter</i>)
NISPOM, 9-302	Key Concepts

Chapter II. Classified Matter Protection and Control Requirements

Classified Matter Protection and Control General Requirements

Objective

Provide basic requirements to ensure the U.S. Department of Energy (DOE) classified information is protected from theft, unauthorized disclosure, loss, or compromise, such as information on recognizing classified matter, handling classified matter in an emergency, basic definitions, reporting requirements, draft documents, and cyber issues.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to Classified Matter Protection and Control (CMPC) general requirements: North Atlantic Treaty Organization, NATO, protection, classification, classification review, marking, emergency procedures, designated approving authority, DAA, output, hard copy, hardcopy, electronic medium, accreditation level, permits, sanctions, reciprocity, Naval Nuclear Propulsion Information, NNPI, infraction, violation, loss, compromise, unauthorized access, Restricted Data, RD, Formerly Restricted Data, FRD, foreign atomic energy activities, intelligence information, foreign visits and assignments, international visits, control of foreign nationals, controlled information, media, DoD Critical Nuclear Weapon Design Information, CNWDI, Sigma.

CMPC General Requirements

DOE Directives

The current general DOE CMPC policy is primarily found in the following directives:

- DOE O 200.1A, *Information Technology Management*. This order establishes requirements and assigns responsibilities for employees' limited personal use of government resources (office equipment and other resources including information technology) within DOE, including the National Nuclear Security Administration.
- DOE M 205.1-4, *National Security System Manual*. This manual provides baseline requirements and controls for the graded protection of the confidentiality, integrity, and availability of classified information and information systems used or operated by DOE.
- DOE M 205.1-5, *Cyber Security Incident Management Manual*. This manual establishes minimum requirements for a structured cyber security incident detection and management process for detecting, identifying, categorizing, containing, reporting, and mitigating cyber security incidents involving DOE information and information systems operated by DOE or by contractors on behalf of DOE.
- DOE O 205.1A, *Department of Energy Cyber Security Management*. The purpose of the DOE Cyber Security Management Program is to protect all DOE cyber information and information systems in order to implement the requirements of applicable laws required to maintain national security and ensure DOE business operations proceed without security events such as interruption or compromise.

- DOE M 470.4-4A, *Information Security*. This manual articulates which security containers, security areas, and other security measures are required for protecting information of a specific classification.
- DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Designs*, 3/11/2004. This manual provides Sigma 14 and 15 access policy.
- DOE Manual 457.1-1A, *Control of Improvised Nuclear Device Information*, 08/10/2006. This manual provides Sigma 20 access policy.
- DOE Order 5610.2, *Control of Weapon Data*, 8/1/1980. This manual sets the access policy and marking requirements for Sigma 1-13.

Related Applicable National Policy Requirements

Table 7 lists references for additional requirements for CMPC.

Table 7. References for Additional Requirements for CMPC

42 U.S.C., Chapter 23	Atomic Energy Act of 1954 (AEA), as amended
50 USC Sec. 2656	Notice to congressional committees of certain security and counterintelligence failures within nuclear energy defense programs
10 CFR 710	Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material. (<i>entire section</i>)
10 CFR 725	Permits for Access to Restricted Data
10 CFR 810	Assistance to Foreign Atomic Energy Activities. (<i>entire section</i>)
10 CFR 820, § 820.11	Information requirements.
10 CFR 820, § 820.12	Classified, confidential, and controlled information
10 CFR 1016, § 1016.42	Reports
10 CFR 1016, § 1016.44	Violations
32 CFR 2001, § 2001.47	Loss, possible compromise or unauthorized disclosure
E.O. 13292, Sec. 5.1	Program Direction
E.O. 13292, Sec. 5.5	Sanctions
NSDD 84	Safeguarding National Security Information
SPBI 4-97	National Policy on Reciprocity of Use and Inspection of Facilities
SPBI 5-97	Guidelines for the Implementation and Oversight of the Policy on Reciprocity of Use and Inspection of Facilities
NAVSEAINST C5511.32B	Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)
NISPOMSUP 1-300	General (Reporting Requirements)
NISPOMSUP 1-301	Security Violations and Infractions
NISPOMSUP 5-500	Transmission
NISPOM 1-301	Reports to be Submitted to the FBI
NISPOM 1-302	Reports to be Submitted to the CSA
NISPOM 1-303	Reports of Loss, Compromise, or Suspected Compromise
NISPOM 1-304	Individual Culpability Reports
NISPOM 5-701	Retention of Classified Material

Table 7. (contd)

NISPOM 5-702	Termination of Security Agreement
NISPOM 8-309	Protection of Media
NISPOM 8-310	Review of Output and Media
NISPOM Chapter 9, Section 1	RD and FRD (<i>entire section</i>)
NISPOM Chapter 9, Section 2	DoD Critical Nuclear Weapon Design Information (CNWDI) (<i>entire section</i>)
NISPOM Chapter 9, Section 3	Intelligence Information (<i>entire section</i>)
NISPOM Chapter 10, Section 5	International Visits and Control of Foreign Nationals (<i>entire section</i>)

Classified Matter in Use

Objective

Ensure U.S. Department of Energy (DOE) employees and contractors have been sufficiently trained in the handling and use of classified matter that is not in storage, and to protect classified information and matter from theft, unauthorized disclosure, loss, or compromise.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to classified matter in use: access, accountability, responsibility, National Industrial Security Program Operating Manual, NISPOM, inventory management, property.

Classified Matter in Use Requirements

DOE Directives

The current DOE handling and use policy for classified matter is primarily found in three directives:

- DOE M 470.4-2 Change 1, *Physical Protection*. This manual defines physical security badge specifications as they relate to the requirements access to security areas.
- DOE M 470.4-4A, *Information Security*. This manual provides specific responsibilities by individuals required to protect classified information throughout the classified matter protection and control (CMPC) cycle.
- DOE M 470.4-5, *Personnel Security*. This manual provides information on what is required for access authorizations (clearances and/or security badges) in order to determine whether individuals are eligible for access to classified matter.

Related Applicable National Policy Requirements

Table 8 lists references for additional requirements for classified matter in use.

Table 8. References for Additional Requirements for Classified Matter in Use

10 CFR 202	Production or Disclosure of Material or Information (<i>entire section</i>)
10 CFR 820, § 820.12	Classified, confidential, and controlled information
10 CFR 1016, § 1016.22	Protection while in use
10 CFR 1016, § 1016.24	Special handling of classified material
10 CFR 1016, § 1016.31	Access to Restricted Data
10 CFR 1016, § 1016.34	Accountability for Secret Restricted Data
32 CFR 2001, § 2001.23	Additional requirements
32 CFR 2001, § 2001.40	General
32 CFR 2001, § 2001.41	Responsibilities of holders
32 CFR 2001, § 2001.44	Information controls
32 CFR 2004, § 2004.20	National Industrial Security Program Operating Manual (NISPOM)
32 CFR 2004, § 2004.21	Protection of Classified Information
41 CFR PART 109–27	Inventory Management
48 CFR 970.5245-1	Property

Marking Classified Matter

Objective

Ensure U.S. Department of Energy (DOE) employees and contractors have been sufficiently trained in the recognition of required marking of classified documents and material to include media, in order to protect classified information and matter from theft, unauthorized disclosure, loss, or compromise.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to marking classified matter: classification level, classification category, National Security Information, NSI, Restricted Data, RD, Formerly Restricted Data, FRD, mixed levels, component, portion marking, foreign government information, FGI, C/FGI-MOD, caveat, Special Control Markings, dissemination control, upgrade, upgrading, downgrade, downgrading, declassify, declassification, derivative classifier, original classifier, automatic declassification, working paper, draft, living document, finished document, final document, redacted documents, OGA, cover sheet.

Marking Classified Matter Requirements

DOE Directives

The current DOE marking policy for classified matter is found in the following directives:

- DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Designs*, 3/11/2004. This manual provides Sigma 14 and 15 access and marking policy.
- DOE Manual 457.1-1A, *Control of Improvised Nuclear Device Information*, 08/10/2006. This manual provides Sigma 20 access and marking policy.
- DOE M 470.4-2 Change 1, *Physical Protection*. This manual defines physical security badge specifications as they relate to the requirements access to security areas.
- DOE M 470.4-4A, *Information Security*. This manual provides specific responsibilities by individuals required to protect classified information throughout the classified Matter Protection and Control (CMPC) cycle.
- DOE M 475.1-1B, *Manual for Identifying Classified Information*. This manual provides detailed requirements to supplement DOE O 475.2, *Identifying Classified Information*.
- DOE O 475.2, *Identifying Classified Information*. This order establishes the program to identify information classified under the Atomic Energy Act [Restricted Data (RD) and Formerly Restricted Data (FRD)] or Executive Order 12958, as amended [National Security Information (NSI)], so that it can be protected against unauthorized dissemination.
- DOE Order 5610.2, *Control of Weapon Data*, 8/1/1980. This order sets the access policy and marking requirements for Sigma 1-13.

Related Applicable National Policy Requirements

Table 9 lists references for additional requirements for marking classified matter.

Table 9. References for Additional Requirements for Marking Classified Matter

Marking	
E.O. 13292, Sec. 1.3	Classification Levels
E.O. 13292, Sec. 1.6	Identification and Markings
NISPOM Chapter 4	Classification and Marking (<i>entire chapter</i>)
NISPOM 5-203	Generation of Classified Material
NISPOM 8-306	Marking Hardware, Output, and Media
NISPOM 9-303	Control Markings Authorized for Intelligence Information
NISPOM 10-304	Marking U.S. Documents Containing FGI
NISPOM 10-305	Marking Documents Prepared For Foreign Governments
Marking Material	
E.O. 13292, Sec. 1.3	Classification Levels
E.O. 13292, Sec. 1.6	Identification and Markings
NISPOMSUP Chapter 4, Sec. 2	Marking Requirements (<i>entire section</i>)
NISPOM 8-306	Marking Hardware, Output and Media

Control Systems and Accountability for Classified Matter

Objective

Ensure that the most valuable classified matter is controlled and U.S. Department of Energy (DOE) employees and contractors recognize and appropriately control accountable classified matter from theft, unauthorized disclosure, loss, or compromise.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to control systems and accountability for classified matter: accountable, accountable matter, classified removable electronic media, CREM, accountable classified removable electronic media, ACREM, audit trail, unique identification number, ACREM custodian, alternate ACREM custodian, Sigma, inventory, report, Top Secret, international treaty, Special Access Program, SAP, NEST, ARG, deploy, North Atlantic Treaty Organization, NATO.

Control Systems and Accountability Requirements

DOE Directives

The current DOE control systems and accountability policy for classified matter is primarily found in the following directives:

- DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Designs*, 3/11/2004. This manual establishes a general process and provides direction for controlling access to, marking and disseminating Sigma 14 and 15 nuclear weapon data, specifically Chapter II, Paragraphs 2.f., Accountability and Paragraph 2.f.(1), Inventory (Sigma 14 and 15 matter).
- DOE Manual 457.1-1A, *Control of Improvised Nuclear Device Information*, 08/10/2006. This manual provides the Sigma 20 access policy.
- DOE M 470.4-4A, *Information Security*. This manual provides specific responsibilities required to protecting accountable classified information from generation throughout the Classified Matter Protection and Control (CMPC) cycle to final destruction.
- DOE Order 5610.2, *Control of Weapon Data*, 8/1/1980. This order sets the access policy and marking requirements for Sigma 1-13.

Related Applicable National Policy Requirements

Table 10 lists references for additional requirements for control systems and accountability for classified matter.

Table 10. References for Additional Requirements for Control Systems and Accountability for Classified Matter

NISPOMSUP Chapter 5, Sec. 2	Control and Accountability
NISPOM 5-200	Policy
NISPOM 5-201	Accountability for TOP SECRET
NISPOM 5-203	Generation of Classified Material

Reproduction of Classified Matter

Objective

Ensure that the reproduction of classified matter is done on approved equipment and in a manner that appropriately protects the matter from theft, unauthorized disclosure, loss, or compromise.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to reproduction of classified matter: reproduce, reproduction, copy, copy machine, Foreign Government Information, FGI, North Atlantic Treaty Organization, NATO, marking copies, marking.

Control Systems and Accountability Requirements

DOE Directives

The current U.S. Department of Energy (DOE) reproduction policy for classified matter is primarily found in DOE M 470.4-4A, *Information Security*. This manual provides specific responsibilities required to reproduce the U.S. Department of Energy (DOE) and other government agencies' or entities' classified matter and ensure its protection from unauthorized access.

Related Applicable National Policy Requirements

Table 11 lists references for additional requirements for the reproduction of classified matter

Table 11. References for Additional Requirements for the Reproduction of Classified Matter

10 CFR 1016, § 1016.35	Authority to reproduce Restricted Data
E.O. 13292, Sec. 2.1	Use of Derivative Classification
E.O. 13292, Sec. 4.1	General Restrictions on Access
NISPOMSUP Chapter 5, Sec. 6	Reproduction (<i>entire section</i>)
NISPOM 4-102	Derivative Classification Responsibilities
NISPOM Chapter 5, Sec. 5	Reproduction (<i>entire section</i>)
NISPOM 10-309	Reproduction (<i>FGI</i>)
NISPOM 10-715	Reproduction (<i>NATO</i>)
NISPOM 11-204	DTIC Downgrading or Declassification Notices

Receiving and Transmitting Classified Matter

Objective

Ensure that the classified matter is appropriately marked, wrapped, transmitted, and received both inside a facility and outside a facility, to ensure the protection from theft, unauthorized disclosure, loss, or compromise.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to receiving and transmitting classified matter: receive, receiving, receipt, sender, recipient, control station, mail room, common carrier, courier, express carrier, reproduce, reproduction, copy, copy machine, Foreign Government Information, FGI, North Atlantic Treaty Organization, NATO, marking copies, marking, double wrap, wrapping, container, escorts, train, airplane, domestic, foreign, overnight, contingency plan, hand carry, register, certify, report, suspense.

Receiving and Transmitting Classified Matter Requirements

DOE Directives

The current U.S. Department of Energy (DOE) policy for receiving and transmitting classified matter is primarily found in the following directives:

- DOE Manual 452.4-1A, *Protection of Use Control Vulnerabilities and Designs*, 3/11/2004. This manual covers Sigma 14 and 15 access policy.
- DOE Manual 457.1-1A, *Control of Improvised Nuclear Device Information*, 08/10/2006. This manual contains Sigma 20 access policy and marking requirements.
- DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management*. This manual establishes program planning and management requirements for the DOE Safeguards and Security.
- DOE M 470.4-4A, *Information Security*. This manual provides specific responsibilities required to receive or transmit DOE and other government agencies' or entities' classified matter and ensure its protection from unauthorized access.
- DOE Order 5610.2, *Control of Weapon Data*, 8/1/1980. This manual sets the access policy and marking requirements for Sigma 1-13.

Related Applicable National Policy Requirements

Table 12 lists references for additional requirements for receiving and transmitting classified matter.

Table 12. References for Additional Requirements for Receiving and Transmitting Classified Matter

E.O. 13292, Sec. 4.1. Para. (g).	General Restrictions on Access
10 CFR 1016 § 1016.33	External transmission of documents and material
32 CFR 2001 § 2001.45	Transmission
32 CFR 2001 § 2001.49	Telecommunications automated information systems and network security
NISPOMSUP Chapter 5, Sec. 4	Transmission (<i>entire section</i>)
NISPOM 5-202	Receiving Classified Material
NISPOM Chapter 5, Section 4	Transmission (<i>entire section</i>)
NISPOM 5-412	Use of Escorts for Classified Shipments
NISPOM 5-413	Functions of an Escort

Destruction of Classified Matter

Objective

Ensure that the classified matter has been destroyed beyond recognition to prevent subsequent access to any classified information or matter, so that it is appropriately protected from theft, unauthorized access, loss, or compromise, and that destruction has been appropriately documented, when required.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to the destruction of classified matter: destroy, destruction, residue, burning, shredding, pulping, melting, mutilating, pulverizing, chemical decomposition, witness, off site.

Receiving and Transmitting Classified Matter Requirements

DOE Directives

The current U.S. Department of Energy (DOE) destruction policy for classified matter is primarily found in one directive: DOE M 470.4-4A, *Information Security*. This manual provides specific responsibilities required to reproduce DOE and other government agencies' or entities' classified matter and ensure its protection from unauthorized access.

Related Applicable National Policy Requirements

Table 13 lists references for additional requirements for the destruction of classified matter.

Table 13. References for Additional Requirements for the Destruction of Classified Matter

E.O. 13292, Sec. 4.1	General Restrictions on Access
NISPOMSUP Chapter 5, Sec. 7	Disposition and Retention (<i>entire section</i>)
NISPOM 5-703	Disposition of Classified Material Not Received Under a Specific Contract
NISPOM 5-704	Destruction
NISPOM 5-705	Methods of Destruction
NISPOM 5-706	Witness to Destruction
NISPOM 5-707	Destruction Records
NISPOM 5-708	Classified Waste

Classified Foreign Government Information

Objective

Ensure the U.S. Department of Energy (DOE) protects classified information and classified matter that is received from a foreign government or entity in confidence, that is generated by collaboration with a foreign government or entity, or that is generated by DOE under an approved agreement or treaty with a foreign government or entity to appropriately protect the information from theft, unauthorized, disclosure, loss, or compromise.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to classified foreign government information: foreign government, foreign government information, FGI, Confidential Foreign Government Information Modified Handling Authorized, C/FGI-MOD, international treaty.

General Storage Requirements

DOE Directives

The current DOE foreign government information policy for classified matter is primarily found in three directives:

- DOE M 470.4-4A, *Information Security*. This manual provides the security measures required for protecting classified information that meets the definition of foreign government information.
- DOE M 475.1-1B, *Manual for Identifying Classified Information*. This manual provides detailed requirements to supplement DOE O 475.2, *Identifying Classified Information*.
- DOE O 475.2. *Identifying Classified Information*. This order establishes the program to identify information classified under the Atomic Energy Act [restricted data (RD) and formerly restricted data (FRD)] or Executive Order 12958, as amended [National Security Information (NSI)], so that it can be protected against unauthorized dissemination.

Related Applicable National Policy Requirements

Table 14 lists references for additional requirements for classifying foreign government information.

Table 14. References for Additional Requirements for Classifying Foreign Government Information

10 CFR 810	Assistance to Foreign Atomic Energy Activities
32 CFR 2001, Sec. 2001.23	Additional Requirements, Foreign Government Information
32 CFR 2001, Sec. 2001.40	NATO
32 CFR 2001, Sec. 2001.45	Transmission
32 CFR 2001, Sec. 2001.47	Loss, possible compromise or unauthorized disclosure
32 CFR 2001, Sec. 2001.53	Foreign Government Information
E.O. 13292, Sec. 1.1	Classification Standards
E.O. 13292, Sec. 1.4	Classification Categories
E.O. 13292, Sec. 1.6	Identification and Marking
E.O. 13292, Sec. 3.3	Automatic Declassification
E.O. 13292, Sec. 4.1	General Restrictions on Access
E.O. 13292, Sec. 6.1	Definitions
United States Security Authority for NATO Affairs Instruction 1-07	Implementation of NATO Security Requirements
NDP-1	National Policies and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organization
NISPOM 4-210	Marking Special Types of Material
NISPOM 5-405	Transmission Outside the United States and Its Territorial Areas
NISPOM 9-103	International Requirements (<i>for RD/FRD</i>)
NISPOM Chapter 10	International Security Requirements
DODD 5230.11, Sec. 4	Classified Military Information
DODD 5340.11, E3.1.1.1	Disclosure
DCID 1/7 9.4	"NOT RELEASABLE TO FOREIGN NATIONALS" – NOFORN (NF)
DCID 1/7 9.5	"AUTHORIZED FOR RELEASE TO ... (name of country(ies)/international organization)" (REL TO)

Chapter III. Storage Requirements for Classified Matter

Storage of Classified Matter

Objective

Ensure U.S. Department of Energy (DOE) classified information and classified matter that is not in use (i.e., not under the direct control of an authorized person) is protected from theft, unauthorized disclosure, loss, or compromise.

Suggested Key Words

These key words are provided as an additional resource to search for requirements related to storage of classified matter: storage, store, security container, vault, vault-type room, SF-700 Form, standard form, custodian, CREM, ACREM, combination, burial, supplemental, closed area, open area, repository, custodian, inventory, special access program, SAP, sensitive compartmented information, SCI.

General Storage Requirements

DOE Directives

The current DOE secure storage policy for classified matter is primarily found in three directives:

- DOE M 470.4-2 Change 1, *Physical Protection*. This manual defines security containers and security areas, establishing or otherwise presenting the requirements that pertain to the physical characteristics of those items.
- DOE M 470.4-4A, *Information Security*. This manual articulates which security containers, security areas, and other security measures are required for protecting information of a specific classification.
- DOE M 452.4-1A, *Appendix (Sigma 1 Sigma 3 Sigma 4 Sigma 11 Sigma 12 Sigma 13 Sigma 14 Sigma 15 Sigma 20)*.

Related Applicable National Policy Requirements

Code of Federal Regulations

32 CFR Parts 2001 and 2004, Classified National Security Information Directive No. 1

“Continuous protection by cleared guard or duty personnel” is not explicitly included as a supplemental protection option for Top Secret information in DOE M 470.4-4A, because for this scenario, the classified information may be established as being under the personal control of an appropriately cleared individual.

“Security-in-Depth”, in this context is considered to be satisfied by meeting the DOE requirements for a Limited Area or higher security area.

An “open storage area”, as applied in this context, correlates with a vault-type-room in DOE. Specific requirements for each should be evaluated and if any contradictory requirements exist between the two sets, the more rigorous standard applies.

National Industrial Security Program Operating Manual (NISPOM)

“Closed Areas,” this would be similar to open storage areas within DOE.

“Restricted Areas,” this could be a room that is normally not used for classified meetings that has been established for one. This could also be a building housing a large piece of production equipment.

“Security in Depth,” this is similar to the use of security areas within the DOE, generally Limited Areas and higher.

Table 15 lists references for additional requirements for storing classified information.

Table 15. References for Additional Requirements for Storing Classified Information

SECURE STORAGE REQUIREMENTS AND RESTRICTIONS	
32 CFR 2001.43	Storage
NISPOM 5-102	End of Day Checks
NISPOM 5-103	Perimeter Controls
STORAGE REQUIREMENTS BY CLASSIFICATION LEVEL	
32 CFR 2001.43	Storage
NISPOM 5-300	General
NISPOM 5-304	CONFIDENTIAL Storage
NISPOM 5-303	SECRET Storage
NISPOM 5-302	TOP SECRET Storage
NISPOM 5-307	Supplemental Protection
NISPOM 5-313	Automated Access Control Systems
NISPOM 5-900	General
STORAGE—REPOSITORY REQUIREMENTS	
32 CFR 2001.42	Standards for Security Equipment
NISPOM 5-301	GSA Storage Equipment
NISPOM 5-305	Restricted Areas
NISPOM 5-306	Closed Areas
NISPOM 5-308	Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas
NISPOM 5-309	Changing Combinations
NISPOM 5-310	Supervision of Keys and Padlocks
NISPOM 5-311	Repair of Approved Containers
GSA AA-F-358H 3.8.2	Identification label

Table 15. (contd)

STANDARD FORMS - SF 700, SF 701 and SF 702	
NISPOM 5-102	End of Day Security Checks
NISPOM 5-308	Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas
32 CFR 2003.1	Purpose
32 CFR 2003.2	Scope
32 CFR 2003.21	Security Container Information: SF 700
32 CFR 2003.22	Activity Security Checklist: SF 701
32 CFR 2003.23	Security Container Check Sheet: SF 702
COMBINATIONS	
NISPOM 5-309	Changing Combinations
NON-CONFORMING STORAGE	
10 CFR 1016.24	Special handling of classified material
32 CFR 2001.52	Open Storage Areas
NISPOM 5-305	Restricted Areas
NISPOM 5-306	Closed Areas
NISPOM 5-312	Supplanting Access Control Systems or Devices
NISPOM 5-314	Electronic, Mechanical, or Electro-mechanical Devices

Appendix A

Forms Usage in Classified Matter Protection and Control Programs

Appendix A

Forms Usage in Classified Matter Protection and Control Programs

Table A.1 lists the forms used in Classified Matter Protection and Control programs.

Table A.1. Forms Used in Classified Matter Protection and Control Programs

32 CFR 2003, § 2003.1	Purpose - The purpose of the standard forms prescribed in subpart B is to promote the implementation of the government-wide information security program. Standard forms are prescribed when their use will enhance the protection of national security information and/or will reduce the costs associated with its protection.
32 CFR 2003, § 2003.2	Scope - The use of the standard forms prescribed in subpart B is mandatory for all departments, and independent agencies or offices of the executive branch that create and/or handle national security information. As appropriate, these departments, and independent agencies or offices may mandate the use of these forms by their contractors, licensees or grantees who are authorized access to national security information.
32 CFR 2003, § 2003.3	Waivers - Except as specifically provided, waivers from the mandatory use of the standard forms prescribed in subpart B may be granted only by the Director of ISOO.
32 CFR 2003, § 2003.4	Availability - Agencies may obtain copies of the standard forms prescribed in subpart B by ordering through FEDSTRIP/MILSTRIP or from the General Services Administration (GSA) Customer Supply Centers (CSCs). The national stock number of each form is cited with its description in subpart B.
32 CFR 2003, § 2003.20	Classified Information Nondisclosure Agreement: SF 312; Classified Information Nondisclosure Agreement: SF 189; Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government): SF 189-A
32 CFR 2003, § 2003.21	Security Container Information: SF 700
32 CFR 2003, § 2003.22	Activity Security Checklist: SF 701
32 CFR 2003, § 2003.23	Security Container Check Sheet: SF 702
32 CFR 2003, § 2003.24	TOP SECRET Cover Sheet: SF 703
32 CFR 2003, § 2003.25	SECRET Cover Sheet: SF 704
32 CFR 2003, § 2003.26	CONFIDENTIAL Cover Sheet: SF 705
32 CFR 2003, § 2003.27	TOP SECRET Label SF 706
32 CFR 2003, § 2003.28	SECRET Label SF 707
32 CFR 2003, § 2003.29	CONFIDENTIAL Label SF 708
32 CFR 2003, § 2003.30	CLASSIFIED Label SF 709 ***** NOTE ***** This form is available to U.S. government agencies, but cannot be placed on the website because of unique construction. It can be ordered by calling Federal Supply Service customer assistance on 800-525-8027 Option 3. Current Revision Date: 01/1987

Table A.1. (contd)

32 CFR 2003, § 2003.31	UNCLASSIFIED Label SF 710
32 CFR 2003, § 2003.32	DATA DESCRIPTOR Label SF 711 ***** NOTE ***** This form is available to U.S. government agencies, but cannot be placed on the website because of unique construction. It can be ordered by calling Federal Supply Service customer assistance on 800-525-8027 Option 3. Current Revision Date: 01/1987
41 CFR 2005 Part 102-194	Standard and Optional Forms Management Program - The Standard and Optional Forms Management Program is a Government wide program that promotes economies and efficiencies through the development, maintenance and use of common forms.
DOE F 470.1	Contract Security Classification Specification
DOE F 470.2	Facility Data Approval Record (FDAR)
DOE F 470-9	C/FGI-MOD Coversheet
DOE F 5635.3	Classified Document Receipt
DOE F 5635.9	Record of Destruction
DD Form 254	Contract Security Classification Specification, Department of Defense
OF 89	Maintenance Record for Security Containers/Vault Doors

Appendix B

Examples of Forms Usage in Classified Matter Protection and Control Programs

Exhibit B.1 shows examples of the Forms Used in Classified Matter Protection and Control programs.

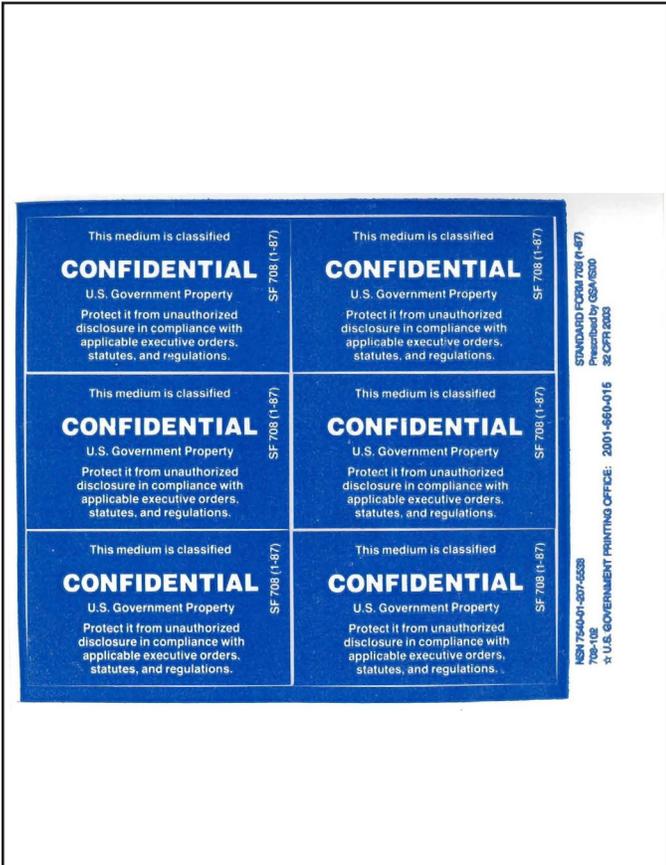
Exhibit B.1. Examples of Forms Used in Classified Matter Protection and Control Programs



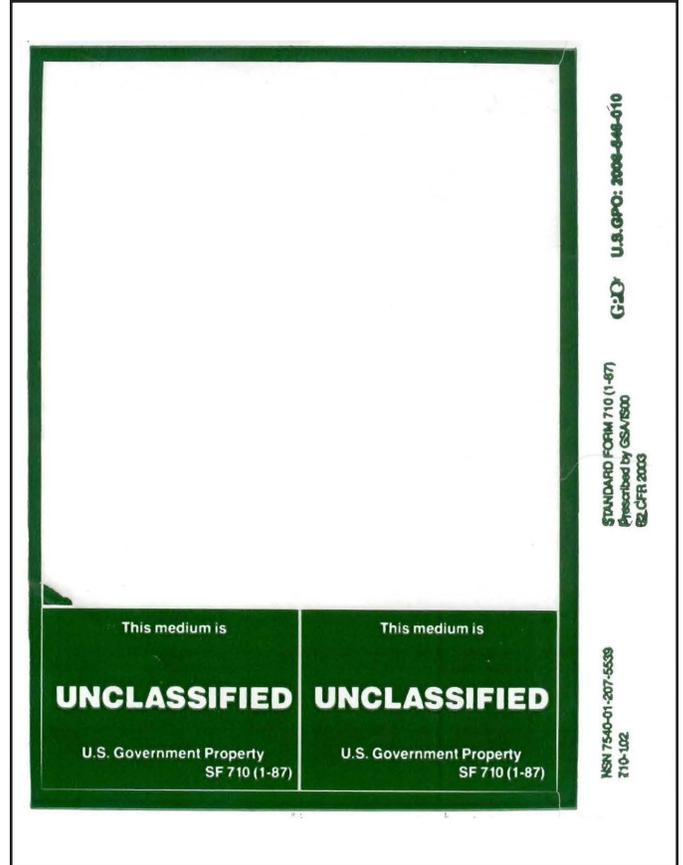
TOP SECRET Label SF 706



SECRET Label SF 707



CONFIDENTIAL Label SF 708



UNCLASSIFIED Label SF 710

Exhibit B.1. Examples of Forms Used in Classified Matter Protection and Control Programs

DOE F 470.1 (05-05)
Replaces DOE F 470.1 (11-02)
All Other Editions are Obsolete

U.S. Department of Energy
CONTRACT SECURITY CLASSIFICATION SPECIFICATION (CSCS)

- 1 -

1. CSOS No.:		2. Previous CSOS No.:		3a. Reason for Action: (Check One) <input type="checkbox"/> Add <input type="checkbox"/> Change <input type="checkbox"/> Terminate	
4. This Specification is For: (Complete as Applicable)		5. Specification is: (Complete as Applicable)			
(Check One)		a. Original (Complete data in all cases)			
a. <input type="checkbox"/> Contract or Other Number <input type="checkbox"/> Solicitation Contract Type:		b. Revised (Supersedes all previous specifications)		Date	
b. Contract Number: _____ End Date: (Estimated) _____		c. Certificate of Possession			
c. Contract Number of Prime: (Complete if registering or soliciting a subcontract)		Retention of Classified Matter is Authorized Until		Date	
		d. Final		Date	
6. General Identification of this Procurement		Certificate of Non-Possession or Equivalent			
7. Contractor					
a. Facility Code		b. Name, Address, and Zip Code		c. Cognizant Security Office (Name, Address, and Zip Code)	
8. Prime Contractor (Complete if registering or soliciting a subcontract)					
a. Facility Code		b. Name, Address, and Zip Code		c. Cognizant Security Office (Name, Address, and Zip Code)	
9. Actual Place of Performance (DOE Facilities) (Attach additional entries as necessary on page 3)					
a. Facility Code		b. Name, Address, and Zip Code		c. Cognizant Security Office (Name, Address, and Zip Code)	
Actual Place of Performance (NON DOE Facilities) (Attach additional entries as necessary)					
a. ID Code		b. Name, Address, and Zip Code		c. Cognizant Security Office (Name, Address, and Zip Code)	
10. Clearance and Storage (enter level and category)					
a. Classification of Matter to be Accessed:					
<input type="checkbox"/> TSRD <input type="checkbox"/> TSFRD <input type="checkbox"/> TSNSI <input type="checkbox"/> SFRD <input type="checkbox"/> SFRDI <input type="checkbox"/> SNSI					
<input type="checkbox"/> CRD <input type="checkbox"/> CFRD <input type="checkbox"/> CNSI <input type="checkbox"/> U					
b. Level of Storage Required at Contractor Facility:					
<input type="checkbox"/> TSRD <input type="checkbox"/> TSFRD <input type="checkbox"/> TSNSI <input type="checkbox"/> SFRD <input type="checkbox"/> SFRDI <input type="checkbox"/> SNSI					
<input type="checkbox"/> CRD <input type="checkbox"/> CFRD <input type="checkbox"/> CNSI <input type="checkbox"/> U					
c. Level of Storage for this Contract:					
<input type="checkbox"/> TSRD <input type="checkbox"/> TSFRD <input type="checkbox"/> TSNSI <input type="checkbox"/> SFRD <input type="checkbox"/> SFRDI <input type="checkbox"/> SNSI					
<input type="checkbox"/> CRD <input type="checkbox"/> CFRD <input type="checkbox"/> CNSI <input type="checkbox"/> U					
d. Access Authorization: <input type="checkbox"/> O <input type="checkbox"/> L					
12. In Performing this Contract, the Contractor Will:					
<input type="checkbox"/> Have Access to Classified Information Only at Another Contractor's Facility or a Government Activity		<input type="checkbox"/> Receive Classified Matter			
<input type="checkbox"/> Generate Classified Matter		<input type="checkbox"/> Fabricate, Modify, or Store Classified Items (e.g., Hardware or Substances)			
<input type="checkbox"/> Perform Services That Require Unescorted Access to Security Areas		<input type="checkbox"/> Be Authorized to Use the Services of the Office of Scientific & Technical Information to Receive Classified Matter			
<input type="checkbox"/> Have Access to U.S. Classified Information Outside the U.S., Puerto Rico, U.S. Possessions and Trust Territories		<input type="checkbox"/> Require a COMSEC Account			
<input type="checkbox"/> Other (Specify)		<input type="checkbox"/> Be Authorized to Use the Defense Courier Service			

Contract Security Classification Specification

DOE F 470.2 (05-05)
Replaces DOE F 470.2 (09-01)
All Other Editions are Obsolete

U.S. Department of Energy
FACILITY DATA AND APPROVAL RECORD (FDAR)

1. Facility Code		2. Reason for Action: <input type="checkbox"/> Reviling Action <input type="checkbox"/> Add <input type="checkbox"/> Change <input type="checkbox"/> Terminate <input type="checkbox"/> Suspend <input type="checkbox"/> Reinstatement		3. Previous FDAR No. and Date:		4. FDAR No.:	
5a. Facility Name:		6. Acronym		7. Importance Rating: <input type="checkbox"/> DA <input type="checkbox"/> CB <input type="checkbox"/> CC <input type="checkbox"/> CD <input type="checkbox"/> CE <input type="checkbox"/> CNP <input type="checkbox"/> CPP		8. Facility Type:	
5b. Doing Business As:		9. Facility Location:		10. Item Numbers Modified:			
11. Unclassified Mailing Address:				12. Offices:			
				a. Cognizant Security Agency: _____ Agreement Date: _____			
				b. Program Secretarial Office: _____			
				c. Cognizant Security Office: _____			
				d. Designated Responsible Officer: _____			
				e. Survey Office: _____			
				f. Facility Clearance Office: _____			
				g. FOCI Office: _____			
13. Classified Mailing Address:				14. RIS Code(s):			
a. Inner Envelope:				a. Special Nuclear Material:			
				a. Category <input type="checkbox"/> I <input type="checkbox"/> II <input type="checkbox"/> III <input type="checkbox"/> IV <input type="checkbox"/> V			
				b. Attributiveness Level: <input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D <input type="checkbox"/> E			
b. Outer Envelope:				16. Facility Clearance:			
				a. Classification Level and Category: <input type="checkbox"/> TSRD <input type="checkbox"/> TSFRD <input type="checkbox"/> TSNSI <input type="checkbox"/> SFRD <input type="checkbox"/> SFRDI <input type="checkbox"/> SNSI <input type="checkbox"/> CRD <input type="checkbox"/> CFRD <input type="checkbox"/> CNSI <input type="checkbox"/> U			
				b. Approved Special Access(es): <input type="checkbox"/> COMSEC <input type="checkbox"/> SCI <input type="checkbox"/> OTHER DCI CAVEATS <input type="checkbox"/> FGI <input type="checkbox"/> OTHER <input type="checkbox"/> NATO <input type="checkbox"/> WDSIGMAS _____			
				c. <input type="checkbox"/> Interim Facility Clearance <input type="checkbox"/> Limited Facility Clearance			
17. Classified Shipping Address:				18. Storage Capability:			
				a. Matter Classification Level and Category: <input type="checkbox"/> TSRD <input type="checkbox"/> TSFRD <input type="checkbox"/> TSNSI <input type="checkbox"/> SFRD <input type="checkbox"/> SFRDI <input type="checkbox"/> SNSI <input type="checkbox"/> CRD <input type="checkbox"/> CFRD <input type="checkbox"/> CNSI <input type="checkbox"/> U			
				b. Approved Special Access(es): <input type="checkbox"/> COMSEC <input type="checkbox"/> SCI <input type="checkbox"/> OTHER DCI CAVEATS <input type="checkbox"/> FGI <input type="checkbox"/> OTHER <input type="checkbox"/> NATO <input type="checkbox"/> WDSIGMAS _____			
				c. Material Classification Level: <input type="checkbox"/> TS <input type="checkbox"/> S <input type="checkbox"/> C <input type="checkbox"/> U			
				19. Approved Classification Processing: <input type="checkbox"/> Computer <input type="checkbox"/> Communication Center <input type="checkbox"/> SCAT			
20. Classified Overnight/Common Carrier:				21. Key Security Personnel:			
a. Company Name:				a. Facility Security Officer			
				Name: _____ Phone: _____			
b. Address:				b. Nuclear Material Control & Accountability Manager			
				Name: _____ Phone: _____			
22. General Comments:				23. Basis for Facility Action			
				a. Approved Safeguards and Security Plan: _____			
				b. Foreign Ownership Control or Influence (FOCI) SF-328 Determination: _____			
				c. Parent Code(s): _____			
				d. Host Entity Code(s): _____			
				e. Home Office Code: _____			
				f. DOD Cage Code: _____			
				g. DOD Clearance Level: _____			
				h. Survey: Initial _____ Rating _____			
				Termination _____ Rating _____			
				i. Other: _____			
24. Created By: _____ Date: _____		25. Approved By: _____ Date: _____		26. SSMS Data Entry By: _____ Date: _____			

Facility Data Approval Record (FDAR)

DOE F 470.9 (08/2005)
All Other Editions are Obsolete

U.S. DEPARTMENT OF ENERGY
C/FGI-MOD

CONFIDENTIAL FOREIGN GOVERNMENT INFORMATION
- MODIFIED HANDLING AUTHORIZED -

As defined by Executive Order 12958, Section 1.1(3), "Foreign Government Information" means:

(1) 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;

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

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

The attached document contains *Foreign Government Information (FGI)*, as defined by Executive Order 12958, "Classified National Security Information," that the foreign government protects at a level lower than U.S. CONFIDENTIAL.

Access to the attached information does not require an access authorization or personnel security clearance. However, access to this information must only be granted to persons with an established need to know and whose official duties require access. This information must not be disclosed to a third party government, individual, group, or organization not involved in the applicable agreement or treaty without the expressed, written permission from the originator.

When not in use, this document must be stored in a locked receptacle (e.g., file cabinet, desk, bookcase) that is accessible only by persons who have a need to know the information to perform their official duties to ensure protection against unauthorized disclosure or access by unauthorized personnel.

This Cover Sheet May Be Applied To All Qualified FGI Documents While Under U.S. Control in U.S. Facilities.

C/FGI-MOD

This document contains Germany information
(Insert name of country)

18 U.S.C. SECTION 1010; ACT OF JUNE 25, 1948; 62 STAT 749; MAKES IT A CRIMINAL OFFENSE TO MAKE A WILLFULLY FALSE STATEMENT OR REPRESENTATION TO ANY DEPARTMENT OR AGENCY OF THE UNITED STATES AS TO ANY MATTER WITHIN ITS JURISDICTION.

Printed on recycled paper

C/FGI-MOD Coversheet

Non Fillable

DOE F 4635.3 (09-95)
05-94 editions may be used

U.S. DEPARTMENT OF ENERGY
CLASSIFIED DOCUMENT RECEIPT

OMB Control No. 1910-180
OMB Review Disclosure Statement on Reverse

TO		POSTAL NUMBER	
		DATE MAILED	
FROM		INSTRUCTIONS	
		<ol style="list-style-type: none"> 1. Verify addressee's classified mailing address. 2. Describe document by subject or title and originator. See DOE 4635.1A for when this form is required. 3. Show classification and extra markings. 4. Forward original and duplicate to addressee. 5. Retain copy pending return of signed original by addressee. 	
DESCRIPTION OF DOCUMENT (Subject or title and originator)	IDENTIFICATION NUMBER	DATE OF DOCUMENT	CLASSIFICATION (Indicate whether or not RD, FRD or NSI)
I have received the document(s) listed above and assume responsibility for safeguarding in accordance with security regulations.			
Signature of addressee or name of addressee and signature of recipient		Date	
Received for addressee by _____		Date _____	
(to be used only by mail rooms)			
1. Return to Sender		2. Addressee's Copy	
3. Pending Copy			

Printed with soy ink on recycled paper

Classified Document Receipt

