

# **SAFEGUARDS AND SECURITY AWARENESS HANDBOOK**

**A REFERENCE FOR  
SECURITY AWARENESS COORDINATORS**

**U. S. Department of Energy  
Safeguards and Security  
Awareness Program**



**Compiled by  
Training Resources and Data Exchange  
Security Awareness Special Interest Group  
for the  
Office of Safeguards and Security Policy and Classification Management  
Office of Safeguards and Security Policy**

**Version 3  
June 2004**

The **Oak Ridge Institute for Science and Education** (ORISE) was established by the U.S. Department of Energy to undertake national and international programs in education, training, health, and the environment. ORISE and its programs are operated by Oak Ridge Associated Universities (ORAU) through a contract with the U.S. Department of Energy.

This document was produced under a contract between the U.S. Department of Energy and Oak Ridge Associated Universities.

© February 2001  
Oak Ridge Associated Universities

# CONTENTS

<b>1.0 INTRODUCTION.....</b>	<b>1</b>
1.1 DOE Safeguards and Security Awareness Program .....	1
Briefings.....	1
Other Program Activity.....	1
1.2 About This Document .....	1
<b>2.0 RESPONSIBILITIES OF THE SECURITY AWARENESS COORDINATOR .....</b>	<b>2</b>
2.1 Qualifications and Training .....	2
2.2 Responsibilities .....	2
Documentation.....	2
Standard Form 312.....	3
Program Enhancements.....	8
Oversight.....	8
2.3 Methods.....	8
<b>3.0 INITIAL BRIEFING .....</b>	<b>9</b>
3.1 Scope and Objectives.....	9
3.2 Scheduling and Coordinating.....	9
3.3 Methods and Materials.....	9
3.4 Briefing Subjects.....	9
Facility Overview.....	9
Protection of Unclassified Controlled Information.....	10
Badging and Access Control Procedures .....	10
Prohibited and Controlled Articles .....	10
Property Protection Procedures.....	10
Reporting Responsibilities .....	10
Substance Abuse Policies .....	10
3.5 Documentation.....	10
3.6 Resources .....	11
3.7 References.....	11
<b>4.0 COMPREHENSIVE BRIEFING .....</b>	<b>12</b>
4.1 Scope and Objectives.....	12
4.2 Scheduling and Coordinating.....	12
4.3 Methods and Materials.....	12
4.4 Briefing Subjects.....	12
4.5 Documentation.....	13
4.6 Resources .....	13
4.7 References.....	13
<b>5.0 TERMINATION BRIEFING .....</b>	<b>14</b>
5.1 Scope and Objectives.....	14
5.2 Scheduling and Coordinating.....	14
5.3 Methods and Materials.....	14

5.4 Briefing Subjects.....	14
Requirements of the DOE F 5631.29.....	14
Penalties .....	15
5.5 Documentation.....	15
5.6 References .....	15
<b>6.0 REFRESHER BRIEFING .....</b>	<b>19</b>
6.1 Scope and Objectives.....	19
6.2 Scheduling and Coordinating.....	19
6.3 Methods and Materials.....	19
6.4 Briefing Subjects.....	19
6.5 Documentation.....	20
6.6 Resources .....	20
6.7 References .....	20
<b>7.0 CONTINUING SAFEGUARDS AND SECURITY AWARENESS .....</b>	<b>21</b>
7.1 Scope and Objectives.....	21
7.2 Methods and Materials.....	21
7.3 Resources .....	21
7.4 References .....	21
<b>APPENDICES .....</b>	<b>22</b>
Appendix A. Required Briefings Matrix .....	A-1
Appendix B. Sample Forms .....	B-1
Appendix C. Classified Information Matrices .....	C-1
Appendix D. Prohibited and Controlled Articles.....	D-1
Appendix E. Resources for the Safeguards and Security Awareness Program .....	E-1
Selected Web Sites.....	E-1
Security Regulations And Directives .....	E-2

**LIST OF FIGURES**

Figure 1.	Standard Form 312, “Classified Information Nondisclosure Agreement” .....	5
Figure 2.	DOE F 5631.29, “Security Termination Statement” .....	18

# 1.0 INTRODUCTION

---

## 1.1 DOE Safeguards and Security Awareness Program

The Department of Energy (DOE) Safeguards and Security Awareness (S&S) Program is established by DOE order to ensure that DOE employees and consultants, contractor and subcontractor employees and consultants, and others with DOE access are made aware of their security responsibilities. DOE O 470.1, Chapter IV, and DOE M 470.1-1 provide requirements for the program. A Security Awareness Coordinator is appointed in writing to oversee a DOE or contractor site/facility awareness program. A goal of the coordinator is to motivate and develop a high level of security awareness using effective instructional methods and communication techniques.

### Briefings

Security awareness briefings make up the core of the program. Required briefings are: 1) initial, 2) comprehensive, 3) termination, and 4) refresher. The initial and comprehensive briefings may, in some cases, be combined into one briefing, depending on how a site chooses to implement these briefings. The refresher briefing is an annual requirement for cleared individuals to remind them of their security responsibilities. Topics may vary each year to address pertinent security issues.

At some sites, other programs with briefing requirements related to security, such as Operations Security (OPSEC), Counterintelligence (CI), Computer Security, and Classified Matter Protection and Control (CMPC), may coordinate the delivery and documentation of those briefings with the Security Awareness Coordinator.

### Other Program Activity

In addition to briefings, an effective awareness program makes use of posters, newsletters, and other promotional media to motivate and sustain awareness of security issues.

## 1.2 About This Document

The Steering Committee of the Security Awareness Special Interest Group (SASIG) provided the technical expertise and effort to develop and publish this document. This document was developed in 1990 and revised and reissued in 2001 and 2003. This document will be updated as required. A Web-based version will be maintained by SASIG on its home page at <http://www.ornl.gov/sa>.

## **2.0 RESPONSIBILITIES OF THE SECURITY AWARENESS COORDINATOR**

---

### **2.1 Qualifications and Training**

A Security Awareness Coordinator responsible for managing a Federal or contractor Security Awareness Program must be appointed in writing. DOE elements appoint coordinators who develop and/or maintain their Safeguards and Security Awareness Program. Security Awareness Coordinators for contractor sites/facilities are appointed by the contractor organizations.

Within one year of appointment, contingent on course availability, the person must successfully complete the Safeguards and Security Awareness Coordinators Training offered through the DOE National Training Center/Central Training Academy (NTC/CTA). Security Awareness Coordinators are expected to have excellent oral presentation, writing, editing, and multimedia skills, and knowledge of the following:

- DOE security directives
- Locally implemented (site) security directives
- DOE security systems and protection programs
- Generic and local security threats and vulnerabilities
- Security-related incidents and concerns
- Approaches and recruitment techniques used by hostile intelligence services
- Countries designated by DOE as “sensitive”
- Site layout

The coordinator should stay up-to-date on local, national, and world events as well as regulatory changes to maintain a valid and sufficient base of briefing information.

### **2.2 Responsibilities**

#### Briefings

Security Awareness Coordinators ensure that employees, both cleared and uncleared, are aware of their security responsibilities. Such awareness is conveyed through delivery of the briefings required by the Safeguards and Security Awareness Program (see Appendix A).

Coordinators serve as security resources in providing assistance and materials as needed to other security-related programs.

#### Documentation

Appendix B contains sample forms that may be used or adapted as documentation of the briefings. The coordinator has responsibility for maintaining documentation not only for on-site employees but also for those working off-site, and in some cases, second- and third-tier subcontractors. Records of required briefings for all individuals must be up-to-date and complete. With accountability at stake, coordinators are advised to develop a plan for the organization of records.

The Safeguards and Security Self-Assessment Program requires a periodic audit of briefing records for accuracy and completeness. If information is found to be missing or incomplete (e.g., someone has failed to take the refresher briefing), the coordinator should follow up with the individual preferably in writing, giving a deadline for completion. If necessary, the person's supervisor or point-of-contact can be notified to ensure compliance. Remember, the Security Awareness Coordinator and the local Security Office are held accountable for an individual's noncompliance to receive a required briefing. A coordinator should document all contacts made along with any responses. A person's failure to comply with briefing requirements may affect his/her access authorization.

Computer-based data management may facilitate and consolidate storage of briefing records. Records for security-related briefings should be readably retrievable and able to be separated from other records for audit accountability.

### Standard Form 312

A completed Standard Form 312 (Rev. 1-00), "Classified Information Nondisclosure Agreement" (SF-312), must be retained in a file system from which the form can be expeditiously retrieved if the United States must seek its enforcement or a subsequent employer must confirm its prior execution. See Figure 1 for a copy of the SF-312.

For Federal employees, the active SF-312 may be filed in the right-hand side of the official personnel folder. The form must not be filed in an individual's Personnel Security File. Contractor security offices should coordinate retention of the SF-312 with the cognizant DOE office. At the contractor's discretion, copies of the executed form may be maintained at subcontractor sites for audit purposes.

When an employee terminates employment, the original SF-312 must be provided to the cognizant DOE office for retention purposes. The form is retained for 70 years following the date of execution.

The form has separate signature lines for witnessing its execution by the individual and for accepting the agreement on behalf of the government. Any DOE employee can witness a DOE official or contractor employee's Agreement, but only an authorized DOE official may accept a DOE employee's Agreement. An authorized DOE official may also accept a contractor employee's Agreement, or a contractor representative may be authorized in writing by the cognizant DOE office to witness and to accept an Agreement from a contractor employee on behalf of the U.S. Government.

In completing and signing this form, individuals accept the terms of the agreement and certify that the briefing official has made available to them the texts of the following laws and orders:

- Title 5, United States Code, Sections 2302(b)(8) and 7211
- Title 16, United States Code, Section 1034
- Title 18, United States Code, Sections 641, 793, 794, 798, 952, and 1924
- Title 50, United States Code, Section 421 et seq. and 783 (b) (Note: 50 U.S.C. 421 is the Intelligence Identities Protection Act)

- Executive Order 12958, as amended, “Classified National Security Information”  
(see E.O.13292 for E.O. 12958 with amendments incorporated)

# **FIGURE 1**

**SF-312 (Rev. 1-00)**

## **“CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT”**

(on the following two pages)

---

## 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 12958, 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, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information 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 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 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, \*952 and 1924, 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 Sections 793 and/or 1924, 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.

*(Continue on reverse.)*

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 12958, 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 expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 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.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER <i>(See Notice below)</i>
-----------	------	---

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER)  
*(Type or print)*

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS <i>(Type or print)</i>		NAME AND ADDRESS <i>(Type or print)</i>	

**SECURITY DEBRIEFING ACKNOWLEDGEMENT**

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
-----------------------	------

NAME OF WITNESS <i>(Type or print)</i>	SIGNATURE OF WITNESS
--	----------------------

**NOTICE:** The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

\*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

### Program Enhancements

Coordinators are encouraged to supplement the required briefings with posters, booklets, newsletters, and other promotional activities to maintain a high level of security awareness.

### Oversight

The Security Awareness Coordinator may be responsible for monitoring program compliance by subcontractors and other organizations working with DOE (e.g., Cooperative Research and Development Agreement partners).

## **2.3 Methods**

Security awareness briefing methods can range from live presentations for large groups to informal briefings for individuals. Other methods of delivery for required briefings include videotapes and computer- and Web-based presentations. In addition, handouts provide an effective means of highlighting and reinforcing essential learning points.

## **3.0 INITIAL BRIEFING**

---

### **3.1 Scope and Objectives**

The initial briefing is given to all individuals, cleared and unclassified, who are newly hired, or newly assigned to a facility or transferred to a new site, to acquaint them with the facility's programs, activities, and security procedures and their own security responsibilities.

### **3.2 Scheduling and Coordinating**

The initial briefing must be completed before individuals report to their work areas, generally as a part of in-processing. When employment or assignment coincides with access authorization, initial and comprehensive security briefings may be combined.

### **3.3 Methods and Materials**

The initial briefing may be presented through various methods that include oral presentations, videotapes, and computer- and Web-based briefings. They may be supported by employee handouts, such as:

- A Security handbook
- List of reporting requirements
- List of prohibited articles
- Site map
- List of security contacts
- Current security newsletter
- Security promotional items

### **3.4 Briefing Subjects**

Required briefing subjects are described in DOE M 470.1-1. The suggested topics below cover the requirements.

#### Facility Overview

The briefing must include an overview of facility programs and activities commensurate with new employees' need-to-know. Relevant site security issues should be discussed.

#### Classification and Access Authorization Procedures

The briefing must inform that Federal law protects certain government information, documents, and material through the process of classification, which categorizes and ranks classified matter in proportion to the potential damage its unauthorized disclosure could cause to national security. Access to any level of classified matter is restricted to individuals who are authorized or "cleared" through DOE's Personnel Security Program. See Appendix C for classified information matrices. A discussion of classification markings must be included in the briefing.

### Protection of Unclassified Controlled Information

A discussion of how to protect unclassified but controlled information, including Unclassified Controlled Nuclear Information (UCNI) and Official Use Only (OUO), must be part of the initial briefing.

### Badging and Access Control Procedures

At sites employing more than 30 persons, physical entry into the facility and into security areas within the facility is controlled through the use of badges that designate the type of the bearer's access authorization. Escorted visitors are given temporary badges for the duration of a visit. Badges must be worn conspicuously on the upper portion of the body while in designated areas unless prohibited by safety considerations. Employees must report lost, stolen and misused badges immediately to the local security office.

Local access control procedures, including escorting policies and security areas, must be explained. Within the bounds of security precautions considering the employees' clearance type and need-to-know, a general site layout map may be helpful.

### Prohibited and Controlled Articles

Individuals must be briefed on a complete list of prohibited and controlled articles (see Appendix D).

### Property Protection Procedures

Local policies on property passes and the removal of government property, special parking regulations, searches, and procedures for vehicle and personal protection must be explained. Individuals should be informed of known local threats to personal and government property. Individuals must be informed of their responsibilities for protecting government property.

### Reporting Responsibilities

See *Safeguards and Security Reporting Requirements for and about Individuals* posted on the SASIG Web site at <http://www.ornl.gov/sa>. This document is regularly updated. Click here for Reporting Requirements.

### Substance Abuse Policies

DOE participates in the Federal effort to achieve a working environment free of substance abuse. At some sites, the Security Awareness Coordinator may be asked to communicate drug awareness and substance abuse policies.

## **3.5 Documentation**

The initial briefing must be documented and the documentation retained in local security files. See Appendix B for a sample briefing verification form that may be used or adapted for this purpose.

### **3.6 Resources**

Appendix E contains sources of useful information and materials applicable to a Safeguards and Security Awareness Program.

### **3.7 References**

DOE O 470.1 and DOE M 470.1-1  
DOE O 472.1C and DOE M 472.1-1B

See also the Security Regulations and Directives in Appendix E.

## **4.0 COMPREHENSIVE BRIEFING**

---

### **4.1 Scope and Objectives**

The comprehensive briefing is given to individuals granted DOE access authorizations and to cleared individuals who are being transferred between organizational elements to a new primary working environment. The purpose of the briefing is to inform individuals of the laws, policies and procedures regulating classified matter and of their security responsibilities for the protection and control of classified matter. As a condition of access to classified matter, individuals must complete the SF-312.

### **4.2 Scheduling and Coordinating**

After an access authorization is granted, the individual must be given a comprehensive briefing before he or she is given access to classified matter or special nuclear materials. This briefing should be conducted as soon as possible after the access authorization is granted. When this process coincides with the beginning of employment, initial and comprehensive briefings may be combined.

### **4.3 Methods and Materials**

Comprehensive briefings are presented through various methods to include oral presentations, videotapes, and computer- and Web-based briefings, supported by employee handouts. Examples of handouts are:

- A Security handbook
- List of Personnel Security reporting requirements
- List of prohibited articles
- Site map
- List of security contacts
- Security promotional items
- Samples of document cover sheets (e.g., Secret, Confidential)
- Examples of incidents requiring notification to local security office
- Classified information matrices (see Appendix C)

When possible, this briefing should involve subject matter experts from other security-related programs.

### **4.4 Briefing Subjects**

Security Awareness Coordinators often include information in the comprehensive briefing that satisfies the requirements of other security-related programs. Required briefing subjects are described in DOE M 470.1-1 and are detailed in several DOE orders and manuals.

#### **4.5 Documentation**

The briefing must be documented and records maintained so that they are readily retrievable. The SF-312 may be used to document this briefing, or see Appendix B for a sample briefing verification form that may be used or adapted for this purpose.

#### **4.6 Resources**

Appendix E contains sources of useful information and materials applicable to a Safeguards and Security Awareness Program.

#### **4.7 References**

Executive Order 12958, as amended, “Classified National Security Information”  
(see E.O.13292 for E.O. 12958 with amendments incorporated)

*Briefing Booklet* for Classified Information Nondisclosure Agreement (SF-312), Information Security Oversight Office, Spring 2001

See the Security Regulations and Directives in Appendix E.

## **5.0 TERMINATION BRIEFING**

---

### **5.1 Scope and Objectives**

A termination briefing is required whenever an individual's access authorization has been or will be terminated. The termination briefing is given to impress upon each individual the continuing responsibility not to disclose classified information to which the person had access and the obligation to return all wholly or partially classified documents and materials in the person's possession to the appropriate DOE official. The briefing must also cover the potential penalties for noncompliance.

### **5.2 Scheduling and Coordinating**

The termination briefing must be conducted on the individual's last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified matter or special nuclear materials, whichever is sooner.

A site's Human Resources office typically notifies the site Security Office when an individual with an access authorization is to be terminated. A subcontractor company also notifies site Security of subcontractor employee termination. When it is determined that an individual no longer requires an access authorization, notification must be made electronically or verbally to the cognizant DOE Personnel Security organization within two working days.

The termination briefing may be provided by personnel outside of the Security Awareness Program. Security Awareness Coordinators should ensure that persons delivering the briefing are aware of the responsibilities for content and documentation.

### **5.3 Methods and Materials**

The termination briefing may be delivered by various methods, including oral presentation, videotapes, and computer- and Web-based presentations. Under unique circumstances, a termination briefing can be accomplished by mail, phone, fax, or with the assistance of a representative of another organization or facility.

### **5.4 Briefing Subjects**

#### Requirements of the DOE F 5631.29

The obligations accepted in signing the SF-312 remain in effect even after DOE access authorization is terminated, and items 3, 4, 5, 7, and 8 of that document must be emphasized. Furthermore, completion of a termination security briefing requires that individuals give their assurance that all classified matter in their possession or charged to them has been returned to designated parties or destroyed in accordance with security regulations. This assurance is given by signing DOE F 5631.29, "Security Termination Statement," in which an individual repeats

his/her pledge not to reveal any classified information except as authorized in writing by DOE officials empowered to give such permission. See Figure 2 for a copy of the DOE F 5631.29.

### Penalties

The briefing must include the penalties for unauthorized disclosure of classified information and UCNI as specified in the Atomic Energy Act of 1954 and Title 18 of the United States Code.

## **5.5 Documentation**

The Security Termination Statement, DOE F 5631.29, must be completed and forwarded to the cognizant DOE office that maintains the site/facility's Personnel Security Files.

To document the briefing in the local Security Office, a copy of the signed DOE F 5631.29 may be filed or an alternate briefing verification form may be used as documentation (see Appendix B). If an individual is not available for this briefing, the unavailability must be documented on DOE F 5631.29 on the employee signature line, along with reason for termination.

Appendix B also shows a sample Termination Checklist that may be used or adapted as an in-house termination form. In addition, a "briefing card" may be useful as a reminder of all essential actions associated with termination.

## **5.6 References**

DOE O 470.1 and DOE M 470.1-1  
DOE O 472.1C and DOE M 472.1-1B

## **FIGURE 2**

### **“SECURITY TERMINATION STATEMENT”**

(on the following two pages)

\_\_\_\_\_  
(Facility or Installation Where Terminated)

## U.S. Department of Energy

### SECURITY TERMINATION STATEMENT

NAME AND TITLE (Print all blocks)	EMPLOYER YOU ARE LEAVING
FUTURE RESIDENCE	NAME AND ADDRESS OF FUTURE EMPLOYER
REASON FOR TERMINATION	
SOCIAL SECURITY NUMBER	DATE OF BIRTH
DATE OF TERMINATION	DOE NUMBER (IF KNOWN)

I make the following statement in connection with the forthcoming termination of my access authorization (security clearance) granted by the U.S. Department of Energy (DOE).

1. In accordance with DOE security regulations, I have destroyed or transferred to persons designated by the DOE all classified documents and material for which I was charged or which I had in my possession.
2. I have returned to a DOE official or person acting for the DOE all security badges, credentials, or other identification or access media issued to me by the DOE or its contractors.
3. I will not reveal to any person any Restricted Data, Formerly Restricted Data, or other classified information of which I have gained knowledge except as authorized by law, regulations of the DOE, or in writing by officials of the DOE empowered to grant permission for such disclosure.
4. I will immediately report to the Federal Bureau of Investigation (FBI) any attempt by an unauthorized individual to acquire classified information from me.
5. I am aware that the Atomic Energy Act of 1954 and U.S. Code, Title 18 "Crimes and Criminal Procedures," prescribe penalties for unauthorized disclosure of Restricted Data, Formerly Restricted Data, and other information relating to the national defense.
6. I am aware that I may be subject to criminal penalties if I have made any statement of material facts knowing that such statement is false or if I willfully conceal any material fact (Title 18, U.S. Code, Section 1001).

\_\_\_\_\_  
(Signature of Person Conducting Interview)

\_\_\_\_\_  
(Signature of Person Whose Access  
Authorization is Being Terminated)

\_\_\_\_\_  
(Title of Position)

\_\_\_\_\_  
(Date)

**See Reverse for Privacy Act Statement.**

## **PRIVACY ACT STATEMENT**

Collection of the information requested is authorized by the Atomic Energy Act of 1954, as amended, and by Executive Orders 10450, 10865, and 12356.

Disclosure of the information on this form is voluntary; however, your decision not to complete this form could result in a delay in processing any future request for reinstatement of your U.S. Department of Energy (DOE) access authorization (security clearance). Your DOE access authorization can be terminated regardless of whether this form is completed. Your name, Social Security Number, and date of birth are used as identifying factors to establish and maintain records of DOE access authorization actions in the DOE System of Records, DOE-42, "Personnel Security Clearance Index," and this -form will be maintained in your DOE Personnel Security File (DOE System of Records, DOE-43, "Personnel Security Clearance Files"). Access to these records is permitted as stipulated in DOE 5631.2, "Personnel Security Program," and as listed in Routine Uses in Appendix B to the DOE System of Records.

## **OMB BURDEN DISCLOSURE STATEMENT**

Public reporting burden for this collection of information is estimated to average 5 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of Information Resources Management, AD-241.2 - GTN, Paperwork Reduction Project (1910-1800), U.S. Department of Energy, 1 000 Independence Avenue, S.W., Washington D.C. 20585; and to the Office of Management and Budget, Paperwork Reduction Project (1910-1800), Washington, D.C. 20503.

## **6.0 REFRESHER BRIEFING**

---

### **6.1 Scope and Objectives**

A refresher briefing is required annually for all individuals who have access authorizations. The objectives are to supplement, update, and reinforce security-related knowledge; to sustain heightened awareness of security issues; and to motivate fulfillment of security responsibilities.

### **6.2 Scheduling and Coordinating**

A refresher briefing is presented annually at approximately a 12-month interval.

Security offices maintain a record of individuals who possess access authorizations. If the briefing is presented in a group setting, the Security Awareness Coordinator must coordinate attendance at refresher briefings with Security or with administrative representatives of the site/facility organizations. These representatives will notify individuals of the requirement to attend specific briefings and announce administrative sanctions for failure to attend. One or more make-up briefings may be required to achieve full compliance.

### **6.3 Methods and Materials**

The refresher briefing offers a critical opportunity to influence and affect a person's understanding and knowledge of security. It is essential that coordinators stay aware of local and national security developments, issues, and concerns. The need to develop effective presentations on specific and sometimes sensitive issues makes networking and information exchange among coordinators highly desirable.

Appendix E contains sources of security awareness program ideas and materials.

The refresher briefing is delivered by various methods, including oral presentation, videotapes, and computer- and Web-based presentations. Guest speakers, games, puzzles, and promotional items such as pens or memo pads can also serve as effective means of reinforcement for briefing points or general security awareness.

### **6.4 Briefing Subjects**

The briefing must selectively reinforce the information provided in the comprehensive briefing. Security developments over time, site-specific considerations, recent security incidents, and current events can guide subject selection. Suggestions for briefing content are:

- Reporting requirements
- CMPC requirements and procedures
- UCNI
- OUO
- Need-to-know criteria
- Escorting procedures

- Insider threat
- Hostile intelligence threat

Every effort should be made to make these briefings informative and interesting.

## **6.5 Documentation**

A record of attendance must be maintained in the local security office for each individual attending the briefing. Signatures in an attendance log will suffice in some organizations, while others may use badge readers and computer-based data management and storage.

## **6.6 Resources**

Appendix E contains sources of information and materials applicable to a Security Awareness Program.

## **6.7 References**

DOE O 470.1 and DOE M 470.1-1

See also the Security Regulations and Directives in Appendix E.

## **7.0 CONTINUING SAFEGUARDS AND SECURITY AWARENESS**

---

### **7.1 Scope and Objectives**

The Safeguards and Security Awareness Program is designed to sustain awareness for all individuals and to provide information about relevant changes.

### **7.2 Methods and Materials**

Various methods and ideas can be employed to motivate individuals to maintain a high level of security awareness. Some examples of motivational tools are:

- Posters/banners
- Booklets
- Newsletters
- Cartoons
- Contests, self-tests, and give-away items
- Web pages
- Games, puzzles
- Security-related e-mail messages
- Screen savers
- Videos

### **7.3 Resources**

Appendix E contains sources of information and materials applicable to a Safeguards and Security Awareness Program.

### **7.4 References**

DOE O 470.1 and DOE M 470.1-1

See also the Security Regulations and Directives in Appendix E.

# **APPENDICES**

---

**Appendix A.** Required Briefings Matrix

**Appendix B.** Sample Forms

**Appendix C.** Classified Information Matrices

**Appendix D.** Prohibited and Controlled Articles

**Appendix E.** Resources for the Safeguards and Security Awareness Program

# APPENDIX A

## Required Briefings Matrix

BRIEFING ACTIONS	Initial	Comprehensive	Termination	Refresher
<b>1. Scheduling and Coordinating</b>				
a. The initial briefing is given before newly hired or assigned individuals report to their work stations, generally as a part of in-processing. When employment or assignment coincides with receiving an access authorization, initial and comprehensive briefings may be combined.	I			
b. The comprehensive briefing is given as a part of the authorization process before access to classified matter or special nuclear materials is granted and must be scheduled with a frequency that ensures minimum delay in the granting of access. When this process coincides with the beginning of employment, initial and comprehensive briefings may be combined. Where possible, the presentation of this briefing may be coordinated with individuals' respective organizations to ensure it does not duplicate the job-specific briefing they will receive later.		C		
c. The termination briefing is given on the final day that the access authorization is active, whether it is being terminated because of the end of employment, transfer from the facility, or administrative reasons. When employment is also terminating, the briefing may be coordinated with the personnel out-processing schedule.			T	
d. The refresher briefing is given to all cleared employees each calendar year at approximately a 12-month interval.				R
<b>2. Updating</b>				
a. New laws, regulations, and directives can require changes in administration and content of any of the briefings.	I	C	T	R

	Initial	Comprehensive	Termination	Refresher
<b>BRIEFING ACTIONS</b>				
b. Information on current or recent trends, issues, events, and cases must be gathered, maintained, and integrated into several types of briefings.	I	C		R
<b>3. Documenting</b>				
a. All briefings must be documented in the local security office.	I	C	T	R
b. In two cases, specific forms must be completed:				
“Classified Information Nondisclosure Agreement” SF-312		C		
“Security Termination Statement” DOE F 5631.29			T	
<b>4. Briefing Subjects</b>				
a. Overview of facility programs, activities, and layout	I			
b. Fundamental concepts of classification and access authorization	I			
c. Badging and access control procedures	I			
d. Prohibited and controlled articles	I			
e. Property protection procedures	I			
*f. Reporting responsibilities and procedures	I	C		R
g. Substance abuse policies	I			
h. Authority for DOE classified matter		C		
i. Categories and levels of classified matter		C		
j. Classification and declassification process		C		
k. Control and management of classified matter		C		
l. Computer security		C		
m. Security systems requirements		C		
n. Access authorization types and procedures		C		
o. Badging systems and escort procedures		C		
p. Hostile intelligence services targeting and recruitment		C		
q. Sanctions imposed for security infractions and violations	I	C	T	
r. Current threat information	I			
s. Reporting and other security obligations after access is terminated			T	

\*The *Safeguards and Security Reporting Requirements for and about Individuals* is posted on the SASIG Web site at: <http://www.ora.gov/sa>.

# **APPENDIX B**

## **Sample Forms**

INITIAL BRIEFING VERIFICATION

NAME: \_\_\_\_\_  
(last, first, middle initial)

ORGANIZATION: \_\_\_\_\_

BRIEFING SUBJECTS:

- Overview of facility/organization missions
- Overview of facility/organization safeguards and security program responsibilities
- Legal requirements for the briefings
- Penalties for infractions
- Identification of classified markings
- Protection of unclassified controlled information
- Property protection procedures
- Badging and access control procedures
- Escorting procedures
- Prohibited and controlled articles
- Current threat information
- Reporting responsibilities and procedures
- Substance abuse policies

This initial briefing was conducted on \_\_\_\_\_.  
(date)

EMPLOYEE: \_\_\_\_\_  
(signature)

BRIEFING OFFICIAL: \_\_\_\_\_  
(signature)  
\_\_\_\_\_  
(printed name)

# COMPREHENSIVE BRIEFING VERIFICATION

NAME: \_\_\_\_\_  
(last, first, middle initial)

ORGANIZATION: \_\_\_\_\_

## BRIEFING SUBJECTS:

- Definition of classified information
- Authority and purpose for DOE classification and declassification program
- Levels and categories of classified information
- Damage criteria associated with each level of classification markings
- Procedures for challenging classification status of information
- Procedures for protection and control of classified matter and unclassified controlled information, including telecommunications and electronic transmissions
- Definition of unauthorized disclosures
- Penalties for unauthorized disclosures
- Conditions and restrictions for access to classified information
- Safeguards and Security reporting requirements
- Legal and administrative sanctions for security infractions and violations of law
- Information on security badges, access authorization types, and access controls
- Responsibilities associated with escorting
- Intelligence services' targeting and recruitment methods
- General information concerning protection of special nuclear materials, if applicable
- Requirements, responsibilities, and purpose of the "Classified Nondisclosure Agreement" (SF-312)

This comprehensive briefing was conducted on \_\_\_\_\_.  
(date)

EMPLOYEE: \_\_\_\_\_  
(signature)

BRIEFING OFFICIAL: \_\_\_\_\_  
(signature)

\_\_\_\_\_  
(printed name)

## TERMINATION BRIEFING VERIFICATION

NAME: \_\_\_\_\_  
(last, first, middle initial)

ORGANIZATION: \_\_\_\_\_

### BRIEFING SUBJECTS:

- Ongoing security obligations as stated in SF-312
- Reporting responsibilities
- Penalties for security violations

### REQUIRED ACTION:

- Return or destroy all classified matter
- Surrender badges and credentials
- Execute Security Termination Statement, DOE F 5631.29

This termination briefing was conducted on \_\_\_\_\_.  
(date)

EMPLOYEE: \_\_\_\_\_  
(signature)

BRIEFING OFFICIAL: \_\_\_\_\_  
(signature)

\_\_\_\_\_  
(printed name)

## SAMPLE TERMINATION CHECKLIST

Name: \_\_\_\_\_ Effective Date: \_\_\_\_\_

Employee ID/Badge Number: \_\_\_\_\_

WHO	WHAT	CHECK OFF WHEN COMPLETED
Security Office	Prepare Security Termination Statement, DOE F 5631.29	
	Conduct Termination Briefing	
Individual with Access Authorization	Sign Termination Statement	
	Leave badge at gate or Security Office when exiting	
Security Office	Call perimeter gate to have badge sent to Personnel Security (if applicable)	
	Fax Termination Statement to appropriate DOE Office	
	Enter termination date in database	
	Deny badge access in electronic system	
	File copy of the Termination Statement and Termination Checklist in individual's file; write month and year of termination on label, and re-file in "Terminated Clearances" (or similar) file	
	Destroy badge, and note destruction in database	
	Send letter to retrieve badge if individual's access authorization is terminated and person is unavailable for signature	

**SAMPLE TERMINATION ACTION CARD**  
(may be worn with badge)

**SUSPENSION/TERMINATION**

**HR Action**

- Coordinate suspension/termination with employee's manager.
- Notify individual of the suspension/termination and ask if person wants to talk to a union representative. If declined, notify the union representative before individual leaves the site.
- Retrieve from individual at time of suspension/termination pagers, radios, keys, etc.
- Ask person if he/she has personal belongings to retrieve and determine if person has transportation home.
- Have person read and sign exit papers (such as medical questionnaire).
- Prepare memo describing the action.
- Notify Payroll.

**Personnel Security Action**

- Follow Termination Checklist for termination briefing.
- Notify appropriate security program managers of termination.

# APPENDIX C

## Classified Information Matrices

Classification Level	Classified Matter Category		
	Restricted Data (RD)	Formerly Restricted Data (FRD)	National Security Information (NSI)
Top Secret	Q	Q	Q
Secret	Q	Q&L	Q&L
Confidential	Q&L	Q&L	Q&L

**Matrix 1: Access to Classified Matter Allowed by Type of DOE Access Authorization**

Classification Level	Category	Damage to National Security
Top Secret	NSI, RD, or FRD	Unauthorized disclosure would cause <b>exceptionally grave damage</b> to national security.
Secret	NSI, RD, or FRD	Unauthorized disclosure would cause <b>serious damage</b> to national security.
Confidential	NSI, RD, or FRD	Unauthorized disclosure would cause <b>damage</b> to national security.

**Matrix 2: Classification Levels**

# APPENDIX D

## Prohibited and Controlled Articles

### *Prohibited Articles*

The following articles are prohibited from security areas, unless authorized in accordance with local procedures (reference DOE M 473.1-1, Chapter V, Paragraph 1.a.):

Any dangerous weapon, explosive, or other instrument or material likely to produce substantial injury to persons or damage to property; controlled substances; any other item prohibited by law. (Reference Title 10 CFR Part 860, and Title 41 CFR 101-20.3)

### *Controlled Articles*

The following privately owned articles are not permitted in a Limited Area, Exclusion Area, Protected Area, Vital Area, or Material Access Area without prior authorization (reference DOE M 473.1-1, Chapter V, Paragraph 1.b.):

Portable electronic devices capable of recording information or transmitting data (e.g., radio frequency, infrared, and/or data link electronic equipment) are not permitted in a Limited Area, Exclusion Area, Protected Area, Vital Area, or Material Access Area without authorization.

The cognizant DOE authority must approve use of this equipment based on the following criteria: (a) the equipment is mission-essential, (b) the equipment is Government-owned or -leased (therefore, involving no additional expense), and (c) a risk analysis identifying vulnerabilities inherent with the characterization and operation of the device has been performed. Authorization for use of such devices in one security area does not apply to all other security areas.

Persons planning to purchase electronic equipment for use at work should contact their Security or TSCM Officer for guidance. If the proposed or existing equipment is to be incorporated into an Automated Information System, DOE Manual 471.2-2 requires a security plan to be prepared and approved by a Designated Approving Authority. Several of the devices are prohibited in designated security areas, such as a Limited and Protected Areas.

Check with Security on what must be done to get authorization for the following:

Personal Digital Assistants and Wireless Systems

These information systems are handheld computers or "palm pilots" which offer a host of features including a capability to transmit and/or receive information through radio frequency (RF) or infrared (IR) energy.

Devices that Record or Use Radio Frequencies for Communications

Devices with recorder and/or RF capability can include 2-way pagers, calculators, cameras, and watches with data ports, hand-held document scanners, and plug-in RF modems.

Laptop Computer and Data Diaries

Personally owned laptop computers and data diaries

Microphones, Video, Digital or Conventional Cameras, Multimedia, Video Conferencing, or Voice Recognition Software

Except as specifically purchased by the U.S. Government to meet a specific and well-documented operational need, these are prohibited unless waivers are granted by DOE Headquarters, SO-1.

Pocket calculators and electronic address or appointment books with no RF, IR, or other communications capability, keyless automobile entry systems, garage door openers, and one-way (receive only) commercial radios and pagers are generally not prohibited unless found, during a technical survey or inspection, to be transmitting or broadcasting data, voice, or information in any other format to outside of the secured area. Individuals should check with their Security or TSCM Officer for guidance.

# APPENDIX E

## Resources for the Safeguards and Security Awareness Program

### SELECTED WEB SITES

TRADE SASIG home page: <http://www.ora.gov/sa>

Defense Security Service: [www.dss.mil](http://www.dss.mil)

DOE Directives: <http://www.directives.doe.gov>

DOE Glossary, draft redline version  
<http://www.directives.doe.gov/pdfs/doegeninfo/draft/glossary.pdf>

Federal Information Systems Security Educators' Association (FISSEA)  
<http://csrc.nist.gov/organizations/fissea.html>

Information Security Oversight Office - National Archives and Records Administration  
<http://www.archives.gov/isoo>

National Classification Management Society: <http://www.classmgmt.com>

National Counterintelligence Executive: [www.nacic.gov](http://www.nacic.gov)

National Training Center (NTC): <http://www.ntc.doe.gov>

## SECURITY REGULATIONS AND DIRECTIVES

### Regulations

Office of Security regulations are as follows:

- 10 CFR 710, “Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material”
- 10 CFR 712, “Human Reliability Program”
- 10 CFR 1016, “Safeguarding of Restricted Data”
- 10 CFR 1045, “Nuclear Classification and Declassification”
- 32 CFR 2001, “Classified National Security Information”
- 10 CFR 1046, “Physical Protection of Security Interests”
- 10 CFR 1047, “Limited Arrest Authority and Use of Force by Protective Force Officers”
- 10 CFR 1048, “Trespassing on Strategic Petroleum Reserve Facilities and Other Property”
- 10 CFR 1049, “Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve”

Some other regulations of interest to DOE Security are as follows:

- 10 CFR 709, “Polygraph Examination Rules”
- 10 CFR 1004, “Freedom of Information”
- 10 CFR 1008, “Records Maintained on Individuals (Privacy Act)”

The Code of Federal Regulations can be searched online at <http://www.access.gpo.gov/nara/cfr/cfr-table-search.html>.

### DOE Directives

Security directives and related materials can be obtained from the DOE Directives online at <http://www.directives.doe.gov>. Applicable directives include:

DOE O 142.1, *Classified Visits Involving Foreign Nationals*, January 13, 2004

The Order establishes a program to facilitate, document, and assure accountability when approving a foreign national’s access to classified DOE programs and facilities.

DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, June 18, 2004

The Order cancels the following:

DOE Policy 142.1 and Notice 142.1, both titled and dated, *Unclassified Foreign Visits and Assignments*, July 14, 1999

Secretarial Memorandum, "Unclassified Foreign Visits and Assignments," July 14, 1999

Secretarial Memorandum, "Policy Exclusion for Unclassified Foreign National's Access to Department of Energy Facilities in Urgent or Emergency Medical Situations," April 10, 2001

Deputy Secretary Francis S. Blake's Memorandum, "Departmental Use of Foreign Access Central Tracing System, November 5, 2001

Deputy Secretary Kyle E. McSlarrow's Memorandum, "Departmental Use of Foreign Access Central Tracking System," November 5, 2001.

The Order establishes requirements and responsibilities for unclassified foreign visits by and assignments of foreign nationals to DOE facilities for unclassified activities.

International cooperation and collaboration is an important element in the effective planning and implementation of many DOE programs. DOE and its international partners benefit from the exchange of information that results from a managed process of unclassified visits and assignments by foreign nationals. These visits and assignments must be conducted in a manner consistent with national security policies, requirements, and objectives including export control laws and regulations.

DOE O 200.1, *Information Management Program*, September 30, 1996  
(see also DOE M 475.1-1A, *Identifying Classified Information*, February 26, 2001)

DOE M 200.1-1, *Telecommunications Security Manual*, March 1, 1997

DOE O 205.1, *Department of Energy Cyber Security Management Program*, March 21, 2003

DOE N 205.2, *Foreign National Access to DOE Cyber Systems*, November 1, 1999

This Notice gives requirements and conditions for foreign national access to DOE cyber systems. Cyber systems include computers, networks, and associated servers, as well as data storage, switching, display, and control devices. Basic tenants: 1) Access by foreign nationals to DOE cyber systems must be approved by a DOE official designated by the site manager or Lead Program Secretarial Officer (LSPO) or by a contractor official designated by senior contractor management; 2) Access by foreign nationals must be periodically audited consistent with the documented risk upon which the approval is based; 3) Nonresident foreign nationals from Sensitive Countries are not permitted access from other than a DOE or DOE contractor site to cyber systems containing UCNI or NNPI. DOE site managers/LPSOs and contractors/subcontractors are responsible for ensuring DOE networked systems containing UCNI or NNPI have protective measures to prevent unauthorized access.

DOE N 205.3, *Password Generation, Protection, and Use*, November 23, 1999, sets the minimum requirements for the generation, protection, and use of passwords to support authentication when accessing classified and unclassified DOE information systems.

DOE G 205.3-1, *Password Guide*, November 23, 1999, provides detailed guidance to supplement DOE N 205.3.

DOE N 205.7, *Extension of DOE Directives*, February 12, 2004, extends the following directives until August 12, 2004: DOE N 205.2 and DOE N 205.3

DOE N 205.8, *Cyber Security Requirements for Wireless Devices and Information Systems*, February 11, 2004

The Notice establishes DOE requirements and responsibilities for using wireless networks and devices within DOE and implements the requirements of DOE O 205.1, *Department of Energy Cyber Security Management Program*, March 21, 2003, including requirements for cyber resource protection, risk management, program evaluation, and cyber security plan development and maintenance.

DOE N 205.9, *Certification and Accreditation Process for Information Systems Including National Security Systems*, February 19, 2004

DOE N 205.10, *Cyber Security Requirements for Risk Management*, February 19, 2004

DOE N 205.11, *Security Requirements for Remote Access to DOE and Applicable Contractor Information Technology Systems*, February 19, 2004

DOE N 205.12, *Clearing, Sanitizing, and Destroying Information System Storage Media, Memory Devices, and Other Related Hardware*, February 19, 2004

DOE N 221.9, *Reporting Fraud, Waste, and Abuse*, August 29, 2003, notifies all employees of their duty to report allegations of fraud, waste, and abuse to the appropriate authorities, including the Office of Inspector General.

DOE O 231.1A, *Environment, Safety and Health Reporting*, June 3, 2004, establishes basic requirements and responsibilities for occurrence reporting.

DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information*, October 19, 2003

The Manual provides detailed requirements to supplement DOE O 231.1A. The information gathered is used for analysis of environmental protection, safeguards and security, and safety and health of workers and the public.

DOE N 251.54, *Extension of DOE Directives on Security*, July 8, 2003, extends DOE N 473.8, *Security Conditions*, until July 8, 2004

DOE N 251.57, *Extension of DOE Directives on Security*, April 28, 2004, extends the following directives until April 28, 2005: DOE O 470.1, *Safeguards and Security Program* and DOE O 471.2A, *Information Security Program*

DOE O 470.1, *Safeguards and Security Program*, September 28, 1995, with Change 1, June 26, 1996 has the following objectives:

To ensure appropriate levels of protection against unauthorized access; theft, diversion, loss of custody, or destruction of nuclear weapons, or weapons components; espionage; loss or theft of classified matter or government property; and other hostile acts that may cause unacceptable adverse impacts on national security or on the health and safety of DOE and contractor employees, the public, or the environment.

To deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of special nuclear materials.

To provide an integrated system of activities, systems, programs, facilities, and policies for the protection of classified information, nuclear materials, nuclear weapons, nuclear weapons components, and DOE and certain DOE contractor property and personnel as required by the Atomic Energy Act of 1954, as amended, other Federal statutes, Executive Orders, and other directives.

To use the Design Basis Threat, issued by the Director of Security, in the design and implementation of protection programs.

To provide levels of protection in a graded manner in accordance with the potential risks.

To establish safeguards and security programs comparable in effectiveness to other federally regulated programs with similar interests when such levels are consistent with DOE protective needs and national security interests.

To ensure effective planning of graded protection levels and prudent application of resources.

To ensure personnel receive training appropriate for their roles in support of the program and that persons given access authorization are aware of Safeguards and Security Program requirements.

To standardize safeguards and security equipment and systems to achieve operational and financial benefits.

DOE O 470.1, Attachment 1, *Contractor Requirements Documents*, September 28, 1995, establishes the DOE contractor requirements and responsibilities.

DOE M 470.1-1, *Safeguards and Security Awareness Program Manual*, October 2, 2002, establishes the responsibilities and requirements necessary to implement the requirements of DOE O 470.1, Ch. IV, *Safeguards and Security Awareness Program*.

DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, May 8, 2001.

DOE O 470.2B, *Independent Oversight and Performance Assurance Program*, October 31, 2002

The Order establishes requirements for the Independent Oversight and Performance Assurance Program, which provides DOE and contractor managers, Congress, and other stakeholders with an independent evaluation of the effectiveness of certain DOE programs, including Safeguards and Security.

DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, June 30, 2000 has the following objectives:

To prevent unauthorized dissemination of Unclassified Controlled Nuclear Information.

To ensure that the maximum amount of government information is publicly available.

DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Program*, June 30, 2000, with Change 1, October 23, 2001, provides detailed requirements to supplement the Order.

DOE O 471.2A, *Information Security Program*, April 27, 1997 has the following objectives:

To establish an Information Security Program for the protection and control of classified and sensitive information.

To ensure that individuals protect classified information and sensitive unclassified information to which they have access or custody.

To ensure that classified information is not released to the public until it has been formally and officially declassified by an appropriate declassification authority and its release is otherwise permitted by applicable law or regulation. Likewise, no sensitive unclassified information shall be released without review for applicable release restrictions.

To establish protection systems that require higher degrees of protection for each higher classification level (Confidential, Secret, Top Secret).

DOE M 471.2-1B, *Classified Matter Protection and Control Manual*, Ch III, Paragraphs 1 and 2, January 6, 1999, and DOE M 471.2-1C, *Classified Matter Protection and Control Manual*, April 17, 2001

These Manuals provide detailed requirements for the protection and control of classified matter and supplement DOE O 471.2A. In DOE M 471.2-1C: Chapter I provides a concise overview of protection and control planning considerations; Chapter II establishes control requirements for classified matter in-use, marking of classified matter,

accountability and control systems, reproduction, receipt and transmission, contract closeout or facility termination, and destruction; Chapter III provides physical protection requirements for classified matter in storage; and Chapter IV addresses loss, potential compromise, or unauthorized disclosure of classified information.

DOE M 471.2-2, *Classified Information Systems Security Manual*, August 3, 1999

The Manual provides requirements and implementation instructions for the graded protection of the confidentiality, integrity, and availability of information processed on all automated information systems used to collect, create, process, transmit, store, and disseminate classified information by, or on behalf of, the DOE.

DOE M 471.2-3A, *Special Access Program Policies, Responsibilities and Procedures*, July 11, 2002.

DOE M 471.2-4, *Technical Surveillance Countermeasures*, February 6, 2004

The Manual is “Official Use Only” and will not be distributed on the Internet. Contact your site/facility Security Office for information.

DOE O 471.3, *Identifying and Protecting Official Use Only Information*, April 9, 2003

DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, April 9, 2003

DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, April 9, 2003

DOE O 471.4, *Incidents of Security Concern*, March 17, 2004 cancels: DOE N 471.3, *Reporting Incidents of Security Concern*, April 13, 2001, Chapter VII of DOE O 470.1, and Chapter IV of DOE M 471.2-1B.

The Order has requirements for the timely identification and notification of, response to, inquiry into, reporting of, and closure actions for incidents of security concern.

DOE O 472.1C, *Personnel Security Activities*, March 25, 2003

The Order establishes the overall objectives, requirements, and responsibilities for implementation and operation of the Personnel Security Program.

DOE M 472.1-1B, *Personnel Security Program Manual*, July 12, 2001

The Manual provides detailed requirements and procedures to supplement the Order and is intended for use by DOE employees responsible for personnel security activities.

DOE O 473.1, *Physical Protection Program*, December 23, 2002

DOE M 473.1-1, *Physical Protection Program*, December 23, 2002

DOE O 473.2, *Protective Force Program*, June 30, 2000, establishes requirements and responsibilities for the management and operation of the DOE Protective Force Program.

DOE M 473.2-2, *Protective Force Program Manual*, June 30, 2000, with Change 1, December 20, 2001, provides detailed requirements to supplement the Order.

DOE G 473.2-1, *Guide for Establishment of a Contingency Protective Force*, March 27, 2003.

DOE N 473.8, *Security Conditions*, August 7, 2002, ensures that DOE uniformly meets the protection requirements specified in Presidential Decision Directive 39, "U.S. Policy on Counterterrorism (U)."

DOE O 474.1A, *Control and Accountability of Nuclear Materials*, November 20, 2000

The Order establishes DOE requirements, including those for the National Nuclear Security Administration, for nuclear material control and accountability (MC&A) for DOE-owned and -leased facilities and DOE-owned nuclear materials at other facilities that are exempt from licensing by the Nuclear Regulatory Commission (NRC).

DOE M 474.1-1B, *Manual for Control and Accountability of Nuclear Materials*, June 13, 2003

The Manual prescribes the requirements and procedures for nuclear material control and accountability for the DOE, including the NNSA.

DOE M 475.1-1A, *Identifying Classified Information*, February 26, 2001.

The Manual provides requirements for managing the Department's classification and declassification program, including details for classifying and declassifying information, documents, and material. It also supplements DOE O 200.1, *Information Management Program*.

DOE O 551.1B, *Official Foreign Travel*, August 19, 2003

The Order establishes the DOE and NNSA requirements and responsibilities governing official foreign travel by Federal and contractor employees.

## SAMPLE NEWSLETTER



December 2000  
Number 9

# OPERATIONS SECURITY (OPSEC)

### What Is It?

Operations Security (OPSEC) is a national security program designed to prevent terrorists, foreign agents, criminals, and other adversaries from obtaining sensitive or unclassified information which, when compiled, may lead them to classified information about our programs or activities.

### What Is The Risk?

Because we live in a free and open society, where information on almost everything is readily accessible, many of us tend to be unaware of the dangers of openly discussing sensitive subjects or passing on information that we think may be helpful or interesting to a "friend." We need to be aware that the disclosure of such information could be harmful to the national security. Highly valuable collection targets include:

- \* Security Systems
- \* Financial Plans
- \* Computer Systems
- \* Strategic Plans
- \* Staffing Information
- \* Budget Documents
- \* Construction Plans
- \* Materials Control & Accountability
- \* Procurement Documents
- \* Construction Drawings & Specifications
- \* Defense Production Information
- \* Energy R&D Technologies
- \* Environmental Documents
- \* Uranium Enrichment Operations

### Why Is OPSEC Important?

The advantage goes to the nation that acquires the most information about a known or potential adversary's defense programs, plans, weapons, scientific research, and, especially now, technical developments. The loser is the government that pays for research and development only to have it lost or compromised due to poor OPSEC.

### What Does It Cost?

Good OPSEC costs very little, and often, nothing. It is usually just using common sense.

**What Can You Do?**

The answer is contained in the simple phrase “need-to-know.” Before you speak to anyone about a sensitive subject, ask yourself, “Does this person have a need-to-know?” When you write a contract or other document dealing with a sensitive or classified subject, include only those facts/figures that are absolutely necessary. Limit access to classified or sensitive information; properly store classified documents in approved containers; and, follow document accountability and distribution procedures. The most important safeguard is to BEWARE. Think before you speak in front of people. Be sure others have a definite need-to-know. When you leave your workplace, ask yourself, “Is it secure?” BEWARE of those who ask too many questions about your work or other projects. These may be attempts to collect intelligence. Remember, YOU are the front line of defense.

**Where Can You Get More Information?**

Contact [NAME], OPSEC Program Manager, at [PHONE] or [NAME], Security Awareness Coordinator, at [PHONE]