



# .SEC100 ANNUAL SECURITY REFRESHER BRIEFING.



# SEC100 Annual Security Refresher Briefing 2009

## Table of Contents

Introduction.....	3
Lessons Learned.....	3
10 CFR 824.....	4
Security Incidents.....	4
Business Rules.....	4
Completion Time.....	4
Objectives.....	5
Module 1: Reporting Requirements.....	5
Module 2: New Federal Credential/Badge Requirements.....	5
Module 3: Random Drug Testing.....	5
Module 4: Escorting and Hosting.....	5
Module 5: Foreign Interactions.....	5
Module 6: Personally Owned Electronic Devices.....	5
Module 7: Technical Surveillance Countermeasures.....	5
Module 8: Classified Videoconferencing.....	5
Module 9: Classification.....	5
Module 10: Classified Matter Protection & Control.....	5
How to Receive Credit.....	6
Resources.....	6
Contacts.....	6
Corporate Process Requirements (CPRs) and Manuals.....	6
Other Websites.....	6
Forms/Aids.....	7
Course Contacts.....	7
SEC100 Completion Record.....	8
Module 1: Reporting Requirements.....	9
Managers’ Reporting Requirements.....	11
Waste, Fraud, and Abuse.....	11
End of Module Question.....	11
Module 2: New Federal Credential.....	12
HSPD-12 Enrollment.....	12
End of Module Question.....	13
Module 3: Random Drug Testing.....	14
Drug Testing.....	14
Selection Notification.....	14
End of Module Question.....	15

Module 4: Escorting and Hosting .....	16
Escorting .....	16
Restrooms .....	16
Controlling Limited Area Access .....	16
Hosting Visitors .....	17
End of Module Question .....	17
Module 5: Foreign Interactions .....	18
Interacting with a Foreign National .....	18
Hosting a Foreign Visitor or Assignee .....	18
Foreign National Requests .....	19
End of Module Question .....	20
Module 6: Personally Owned Electronic Devices .....	21
Cell Phones .....	21
Other Devices .....	21
End of Module Question .....	22
Module 7: Technical Surveillance Countermeasures .....	23
Surveillance Awareness .....	23
Assessing Surveillance Vulnerabilities .....	23
End of Module Question .....	24
Module 8: Classified Videoconferencing .....	25
Classified Videoconferencing at SNL .....	25
End of Module Question .....	26
Module 9: Classification .....	27
Classification Practices .....	27
Determining Classification Issues .....	27
Classification Responsibilities .....	27
Review and Approval Process for Release of Information .....	28
Association and Compilation .....	28
Improperly Classified Documents .....	28
No Comment Policy .....	29
End of Module Question .....	29
Module 10: Classified Matter Protection and Control .....	30
Protecting Classified .....	30
End of Module Question .....	31
SEC100 Feedback Form .....	32

## Introduction

Why do I have to take SEC100?	DOE Manual 470.4-1, Section K, “Safeguards and Security Awareness Programs,” requires that all cleared individuals receive an annual security refresher briefing.
Why is SEC100 important?	An annual refresher briefing ensures that all Members of the Workforce (DOE/NNSA employees, contractors, and consultants) are aware of new security requirements and information. This briefing also provides the opportunity to review our security responsibilities.
How are topics for this briefing selected?	The Annual Security Refresher Briefing is designed to selectively reinforce the information provided in the Comprehensive Security Briefing (SEC150) and address current Safeguards and Security (S&S) issues that are specific to various facilities and organizations.
What happens if I delay taking the course?	<b>Failure to successfully complete this briefing by your due date will result in your DOE badge (automated access) being disabled until you have completed the course.</b>

SEC100 addresses the following security-related topics:

- Reporting Requirements
- New Federal Credential/Badge Requirements
- Random Drug Testing
- Escorting and Hosting
- Foreign Interactions
- Personally Owned Electronic Devices
- Technical Surveillance Countermeasures
- Classified Videoconferencing
- Classification
- Classified Matter Protection & Control

### **Lessons Learned**

Safeguards & Security (S&S) Lessons Learned Program was established to identify, analyze, and disseminate S&S lessons learned information. Lessons learned are experiences that—when discussed and disseminated—can be used to improve programs and help prevent similar mistakes. S&S lessons learned information is acquired primarily through root cause analysis of security incidents. However, lessons learned and best

practice information can also be acquired through other sources. If you know of a worthwhile lesson learned or best practice to share with Members of the Workforce, consult with your Sandia manager. For additional information about the S&S Lessons Learned Program, contact SNL/NM's [S&S Awareness Coordinator](#).

## **10 CFR 824**

Remember, security responsibilities are an ongoing role. Failing to follow security requirements may lead to a serious security breach, as well as significant fines to Sandia Corporation (per Title 10, *Code of Federal Regulations*, Part 824 [[10 CFR 824](#)] “Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations”).

Section 234B of 10 CFR 824 instructs that a contractor or subcontractor to DOE who violates any rule, regulation, or order relating to the security of Restricted Data, classified information, or sensitive information will be subject to a fine of up to \$100,000 per offense.

## **Security Incidents**

All security incidents must be immediately reported to the Security Incident Management Program (SIMP). In NM, use the OOPS process (311 from a Sandia phone, or (505)844-0311 from an outside line), or in CA, (925)294-3230.

## **Business Rules**

Sandia's Business Rules are continually revised to ensure that they remain current and in compliance with DOE directives, federal and state laws, and Sandia best management practices. When discrepancies or inconsistencies exist between the Business Rules and this briefing, the requirements cited in the Business Rules take precedence.

## **Completion Time**

Course completion time is estimated to be 30 minutes. However, course completion times vary greatly, depending upon familiarity with the content, reading speed, number of interruptions, and number of optional links accessed.

Charging A-290 for 30 minutes for course completion is authorized for Sandia employees.

*Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000*

## Objectives

### **Module 1: Reporting Requirements**

Upon completing this module you will be familiar with security-related information that Members of the Workforce are required to report.

### **Module 2: New Federal Credential/Badge Requirements**

Upon completing this module you will be able to identify security requirements for the use and protection of your new federal credential.

### **Module 3: Random Drug Testing**

Upon completing this module you will be familiar with the random drug testing policy that applies to Members of the Workforce who hold Q- or L-level security clearances.

### **Module 4: Escorting and Hosting**

Upon completing this module you will be familiar with identifying the responsibilities associated with escorting and limited area access.

### **Module 5: Foreign Interactions**

Upon completing this module you will be able to identify security requirements for hosting uncleared foreign nationals.

### **Module 6: Personally Owned Electronic Devices**

Upon completing this module you will be able to recognize the security-related issues associated with cell phones, personal digital assistants (PDAs), and other personally owned electronic devices.

### **Module 7: Technical Surveillance Countermeasures**

Upon completing this module you should be able to identify precautions to take if you suspect or are aware of technical surveillance vulnerabilities.

### **Module 8: Classified Videoconferencing**

Upon completing this module you should understand your responsibilities for classified videoconferencing at SNL.

### **Module 9: Classification**

Upon completing this module you should be able to determine when to seek assistance from a Derivative Classifier (DC) or the Classification Office.

### **Module 10: Classified Matter Protection & Control**

Upon completing this module you should be familiar with Classified Matter Protection and Control (CMPC) practices.

## How to Receive Credit

To receive credit for SEC100:

- Read through the course material.
- Answer all the practice questions, and check your answers.
- Send SEC100 Completion Record to the Course Administrator, MS-1341, fax (505) 284-6079 for credit.

## Resources

### Contacts

- Badge Office
  - NM: (505) 284-3626
  - CA: (925) 294-2061
- Central Alarm Station (SNL/CA) - (925) 294-2300
- Corporate Investigators - (505) 845-9900
- Counterintelligence (CI) Hotline
  - NM: (505) 284-4760 or (505) 844-3834
  - CA: (925) 294-6614
- Foreign Visits and Assignments
  - NM: (505) 844-2697
  - CA: (925) 294-3042
- SIMP Pager
  - NM: (505) 540-2382
  - CA: (888) 932-9710
- SNL/NM Protective Force - (505) 844-3155

### Corporate Process Requirements (CPRs) and Manuals

- [CPR300.5.3](#), *Workplace Substance Abuse Prevention and Testing*
- [CPR400.2.10](#), *Using Information Technology (IT) Resources*
- [CPR400.3.1](#), *Technical Surveillance – Audio and Video Recording*
- [CPR400.3.5](#), *Foreign Interactions*
- [CPR400.3.7](#), *Reporting Personnel Security Information; Security Incidents; and Waste, Fraud, and Abuse*
- [CPR400.3.11](#), *Access Controls*
- [CPR400.3.12](#), *Management of Classified Matter*
- [CPR400.3.17](#), *Export/Import Controls and Compliance*
- [DOE Manual 470.4-1](#), Section K, “Safeguards and Security Awareness Programs”
- Title 10, *Code of Federal Regulations*, Part 824 ([10 CFR 824](#)), “Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations”

### Other Websites

- [Badge Office website](#)
- [California Site Operations Center 8500 Security homepage](#)
- [Classification Office’s DC Access List](#)

- [Corporate Investigations website](#)
- [Foreign Interactions website](#)
- [Laptops on Foreign Travel \(LOFT\) website](#)
- [Physical Security & Planning website](#)
- [Safeguards & Security homepage](#)
- [Technical Surveillance Countermeasures \(TSCM\) homepage](#)

**Forms/Aids**

- [Foreign National Request \(FNR\) Security Plan \(SP\) Decision Tool Wizard](#)

**Course Contacts**

For questions:	Contact:
Course Administrator	Margret Tibbetts, <a href="mailto:mrtibbe@sandia.gov">mrtibbe@sandia.gov</a> , (505) 845-7776, MS-1341
Program Owner	Fran Armijo, <a href="mailto:fparmij@sandia.gov">fparmij@sandia.gov</a> , (505) 284-2416, MS-1341



## SEC100 Completion Record

After reading all the modules in SEC100 Annual Security Refresher Briefing, fill in the form below and forward to the Course Administrator, MS-1341, fax number (505) 284-6079 in order to receive course credit

**I have read all the modules and answered all the practice questions in SEC100 Annual Security Refresher Briefing**

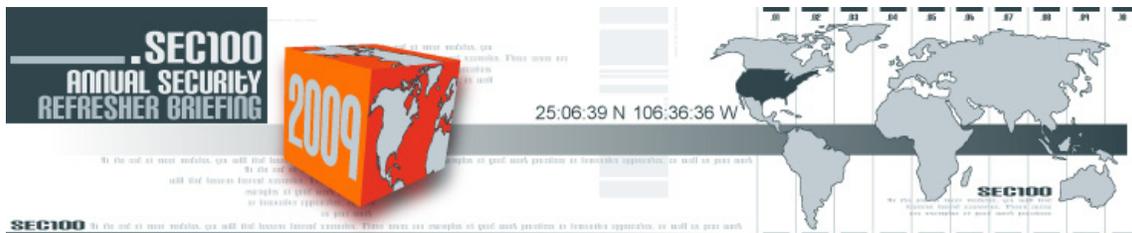
Print Full Name (Last, First, Middle Initial)	Last 4 digits of SSN
Org./Company Name	
Signature	Date

- Employee   
  Contractor   
  Consultant  
 Student   
  KMP

If you would like confirmation of your completion, provide either:

\_\_\_\_\_  
Email Address

\_\_\_\_\_  
Fax Number



## Module 1: Reporting Requirements

### Objectives:

Upon completing this module you will be familiar with security-related information that Members of the Workforce are required to report.

Maintaining your security clearance is essential to your job, and requires that you follow all reporting requirements.

If You...	You Must Report...	To...
<p>Are <b>arrested</b>, have <b>criminal charges</b> brought against you (including charges that are dismissed), or you are <b>detained</b> by federal, state, or other law-enforcement authorities for violations of the law, within or outside of the United States</p> <p><b>Note:</b> Traffic violations in which a fine of \$250 or less was imposed do not have to be reported unless the traffic violation is alcohol- or drug-related</p>	<p>Orally, within 2 working days of occurrence</p> <p>In writing, within the following 3 working days</p>	<p>NM – Corporate Investigations</p> <p>CA – Clearance Processing</p>
<p>File for <b>bankruptcy</b>, regardless of whether it is for personal or business-related reasons</p>	<p>Orally, within 2 working days of occurrence</p> <p>In writing, within the following 3 working days</p>	<p>NM – Corporate Investigations</p> <p>CA – Clearance Processing</p>
<p>Have your <b>wages garnished</b> for any reason</p>	<p>Orally, within 2 working days of occurrence</p> <p>In writing within the following 3 working days</p>	<p>NM – Corporate Investigations</p> <p>CA – Clearance Processing</p>
<p><b>Change your name</b></p>	<p>In writing (<a href="#">SF 2730-NCB, Name Change Request for Badge Office and Staffing</a>), 2 days after the occurrence</p>	<p>NM &amp; CA – Personnel Security</p>

If You...	You Must Report...	To...
<b>Marry or cohabitate</b> in a spouse-like relationship	In writing ( <a href="#">DOE F 5631.34</a> , <i>Data Report on Spouse/Cohabitant</i> ), within 45 working days of marriage or cohabitation	NM – Personnel Security CA – Clearance Office
Are approached or contacted by any individual seeking unauthorized <b>access to classified information or matter</b> , or special nuclear material (SNM)	Immediately	NM – Counterintelligence, Corporate Investigations, or SIMP CA – Counterintelligence, Security, or SIMP
Have substantive contacts with <b>foreign nationals</b> (excluding family members)	Immediately	NM – Counterintelligence or Corporate Investigations CA – Counterintelligence
Are <b>hospitalized</b> for a <b>mental illness</b> or for treatment of <b>alcohol or drug abuse</b>	Orally, within 2 working days of occurrence In writing, within the following 3 working days	NM – Corporate Investigations CA – Clearance Office
Are employed by, represent, or have any other <b>business-related</b> association with a <b>foreign</b> or <b>foreign-owned interest</b> , or <b>foreign national</b>	Immediately	NM – Corporate Investigations CA – Counterintelligence
Have business-related foreign <b>travel</b> to sensitive or non-sensitive countries, or have personal foreign travel to sensitive countries	37 days before trip Prior to travel, or as soon as practical	NM & CA – International Travel
No longer require your clearance, terminate your employment, are on extended leave of 90 consecutive working days, or your access authorization is no longer required for 90 consecutive working days	Immediately – both orally and with completed <a href="#">DOE F 5631.29</a> , <i>Security Termination Statement, and Badge</i>	NM – Counterintelligence, Corporate Investigations, or SIMP CA – Counterintelligence, Security, or SIMP

You are not precluded from reporting derogatory information directly to the DOE Personnel Security Department. However, as the sponsor of your clearance, you are still required to report these items to the SNL organizations listed above. For phone numbers or additional information, refer to the [Reporting Requirements](#) matrix on the Sandia Restricted Network, or the [Contractor Toolcart](#) on Sandia's external network.

## **Managers' Reporting Requirements**

All managers aware of a Member of the Workforce's hospitalization for a mental illness or other condition (e.g., substance or alcohol abuse) that may significantly affect that individual's judgment or reliability, must provide notification of the individual's condition to the appropriate group (Corporate Investigations in NM or the Clearance Office in CA). Such a condition may affect the individual's ability to keep an access authorization. Verbal notification must be made to the appropriate parties within 8 working hours, and written confirmation within the next 10 working days.

## **Waste, Fraud, and Abuse**

Members of the Workforce have a duty to report to an appropriate authority any allegations of fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement relating to DOE programs, operations, facilities, contracts, or information technology systems. Examples of violations to be reported include, but are not limited to, allegations of false statements, false claims, bribery, kickbacks, fraud (including timecard fraud), DOE environment, safety, and health (ES&H) violations, theft, computer crimes, mischarging, conflicts of interest, and conspiracy to commit any of these acts. Incidents or information may be reported to Corporate Investigations or directly the Office of the Inspector General.

## **End of Module Question**

Jeremy has received a traffic ticket, and he's evaluating whether or not he has to report it. Under what circumstances would Jeremy be required to report the traffic ticket?

- a) If the ticket was over \$250.00.
- b) If drugs or alcohol were involved.
- c) If the ticket was received while commuting to or from SNL.
- d) Either a or b.

---

**Answer:** d) Either a or b.



## Module 2: New Federal Credential

### Objective:

Upon completing this module you will be able to identify security requirements for the use and protection of your new federal credential.

### HSPD-12 Enrollment

Sandia began fully implementing the Homeland Security Presidential Directive 12 (HSPD-12) enrollment process in August 2008.

The new federal credential presents some new challenges and responsibilities. For instance, your new credential comes with its own unique card holder. You should care for and protect your new credential by following these requirements:

- Do not mark on, punch holes in, or bend your credential. If the credential is altered, it will be considered defacing federal property. If the protective plastic covering peels away, it will also void the credential.
- Do not scratch the magnetic strip on your credential.
- Avoid leaving your credential in areas subject to excessive heat (e.g., clothes dryer) or in direct sunlight (e.g., car dashboards) since these could cause the credential to warp.
- Do not subject the credential to magnetic fields (e.g., stereo equipment, magnets, or other magnetic-strip cards).



The following should be kept in mind about the card holder that is issued with the new credential:

- For the protection of the credential, it must be kept in the front slot of the card holder when it is not in use.
- The card holder may not be replaced with another type of card holder. The card holder you are issued is General Services Administration (GSA) approved and is designed to prevent damage and degradation of the laminates on the credential. It has electromagnetically-opaque film that provides an additional layer of protection against unauthorized or unknown access.

- The credential must be removed completely from the card holder when showing the credential to a guard at the Kirtland Air Force Base gate or a Protective Force officer at the California site gates or New Mexico limited areas.

The following standard requirements also apply to the new credential:

- A badge or credential may be used as identification only for official government-use purposes.
- Members of the Workforce should not wear their badges/credentials outside of a government facility.
- The credential/badge must be protected from loss or theft.
- You are required to have your credential with you at all times while at work. If you forget your credential, it is highly recommended that you go home and retrieve it. Otherwise, you must follow the steps regarding a lost/stolen/forgotten badge listed in [CPR400.3.11](#), Attachment A, “Access Controls,” and your failure to protect your credential will be recorded and reported to DOE.
- Replace your badge when it is damaged or when your name or picture becomes unrecognizable.

While the new credential is accepted at other government facilities, you must still go through the same enrollment procedures at other facilities as you did with your previous badge.

For more details about your credential, including your responsibilities and privacy rights, read the “About the USAccess Credential Guide” on the [USAccess Program website](#).

### ***End of Module Question***

Jake has just received his new credential and is being given instructions by Badge Office personnel on use of his new credential. In the instructions Jake is being given, he is told that when entering through a manned gate, including a Kirtland Air Force Base gate, he must remove the badge from its holder and present the badge to the officer at the gate.

Does Jake have options?

- a) Yes, he can punch a hole in the badge and place it on a lanyard.
- b) Yes, he can obtain an easier to read-through card holder for his new credential.
- c) No, he is required to comply and remove his credential from the holder provided by the Badge Office.
- d) None of the above.

---

**Answer:** c) No, he is required to comply and remove his credential from the holder provided by the Badge Office.



## Module 3: Random Drug Testing

### Objective:

Upon completing this module you will become familiar with the random drug testing policy that applies to Members of the Workforce who hold Q- or L-level security clearances.

### Drug Testing

Effective October 13, 2008, Sandia implemented a random drug testing policy for all Q- and L-cleared Members of the Workforce. This policy is the result of a DOE decision to require random drug testing for all positions at sites that require access authorization.

Thirty percent of Sandia's cleared population will be randomly tested each year. Selection for a random drug test does not reduce the chances of being selected again in any future random selection for drug testing.

Additional drug and/or alcohol testing will be conducted if there is reasonable suspicion or as a result of an accident or incident on Sandia property.



### Selection Notification

If selected, an individual will receive verbal notification during operational hours. The notified Member of the Workforce must then report to a designated testing site within the same workday that the notification was given. Out-of-town clearance holders will have 24 hours to report to a designated collection site. If the call up administrator does not physically speak to the randomly selected individual, the individual's name will go back into the testing pool for future selection.

A confirmed, positive drug test will immediately result in the worker's badge being confiscated and the person being removed from his or her duties. Additional disciplinary actions, including termination, could follow. Contractors who test positive will be removed from their performance on the Sandia contract.

Failure to report to an approved clinic the day of the notification, or refusal to provide a sample, will result in measures equal to those for a positive drug test result.

For additional information on this new policy, refer to the "[Random Drug Testing at Sandia](#)" web page, or the external [Contractor Toolcart](#).

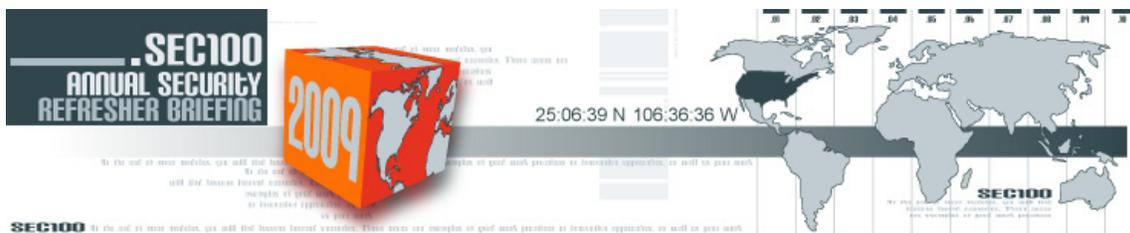
### **End of Module Question**

Jane, a Q-cleared employee, is randomly selected to take a drug test. She receives a call telling her where and when to report for the test. Jane had planned to spend the day preparing for an upcoming conference. Additionally, because she'd taken the bus to work, Jane doesn't have access to her personal vehicle, and the drug testing center is located off site. What should she do?

- a) Call back, reporting that she's ill and has to go home.
- b) Ask her manager to explain to Healthcare & Support Services that Jane is too busy to be tested today.
- c) Ask testing center personnel whether someone else can take her slot.
- d) Report for her drug test as scheduled.

---

**Answer:** d) Report for her drug test as scheduled.



## Module 4: Escorting and Hosting

### Objective:

Upon completing this module you will be familiar with identifying the responsibilities associated with escorting and limited area access.

### Escorting

Access to limited or more restricted areas can be controlled by doors, bypass gates, or turnstiles. When you escort someone into one on these areas, you will incur certain responsibilities and risks.

“Escorting” is the practice of accepting responsibility for an uncleared individual while that person is inside a limited, or more restricted, area. This practice requires maintaining **verbal and visual control** of the uncleared person at all times while he/she is within the restricted area. It is also your responsibility to ensure that:

- The individual does not have any [prohibited or controlled items](#).
- The individual does not have access to classified information.
- The individual does not have access to unclassified information for which he or she does not have a need to know (NTK).
- Individuals with whom you have contact are informed that the person you are escorting is uncleared (announce the visitor’s presence).
- Signs are posted that remind everyone that an uncleared person is in the area.
- If escorting responsibilities are transferred, the new escort is properly cleared, and is aware of, and willing to assume, responsibility for the individual.
- A visitor’s badge is retained by the host at the end of the visit.

If you come upon an unescorted, uncleared individual in a limited area, you should immediately take over escort responsibilities and report the incident.

### Restrooms

Escorts do not need to accompany a visitor into the restroom unless the restroom has more than one exit or any windows. In cases where the restroom does not have more than one exit or any windows, the escort should announce there is an uncleared visitor. This duty may be delegated in cases of visitors of the opposite sex.

### Controlling Limited Area Access

While we may be accustomed to associating turnstiles with access control, we sometimes forget that attention must also be given to access controls when using doors and bypass gates. Don’t assume that the door or gate has closed firmly behind you. Good security

practices include watching behind you to verify that no one follows you through the door or access gate to a limited area, and ensuring that the door or gate closes firmly behind you.

## **Hosting Visitors**

“Hosting” is the practice of accepting responsibility for a cleared or uncleared visitor at SNL. It is your responsibility as a host to ensure that:

- Visitors have official business to include a programmatic NTK at SNL.
- Unescorted visitors surrender their badges at the conclusions of visits and that badges are returned to the appropriate Badge Office in one of the following manners:
  - The host or escort takes possession of the badge and ensures that it is returned to the appropriate Badge Office.
  - The badge is placed in the “badge box” located at 1611 Innovation Parkway (SNL Badge Office).
  - The badge is returned to the Badge Office via intra-office mail, in an Official Use Only (OUO) envelope.
- If a visitor badge is not retrievable, submit [SF 2730-LSB](#), *SNL Lost/Stolen Badge Report*, to the appropriate Badge Office.

For more information on access to limited areas, or escorting, refer to [CPR400.3.11](#), *Access Controls*.

## **End of Module Question**

Mark is escorting an uncleared contractor to his office, which is within the limited area. After arriving to his office, Mark offers the visitor a cup of coffee. Mark leaves to get the coffee, closing the office door behind him. Jeff, a cleared individual, is scheduled to meet with Mark and his visitor. Jeff knocks on the door, enters, and finds the uncleared individual alone. What should Jeff do?

- a) Close the door and forget about the incident.
- b) Go find Mark.
- c) Take over escorting responsibilities and report the incident.
- d) None of the above.

---

**Answer:** c) Take over escorting responsibilities and report the incident.



## Module 5: Foreign Interactions

### Objective:

Upon completing this module you will be able to identify security requirements for hosting uncleared foreign nationals.

### *Interacting with a Foreign National*

DOE encourages international collaborations and allows access by foreign national visitors and assignees to its unclassified information, programs, and technologies. However, to ensure that such access does not pose a risk to national security, Sandia protects those assets by monitoring and controlling interactions between Members of the Workforce and foreign nationals.

Before any substantive business discussion or a visit takes place, you must determine if the person involved is a U.S. citizen or not. This can be accomplished simply by asking the individual. If you are still uncertain based on the reply, assume that he or she is not a citizen, and protect access accordingly until that person's status can be determined.

Foreign nationals are classified as either "visitors" or "assignees." Visitors are foreign nationals who are authorized to be at SNL for 30 days or less. Assignees are those foreign nationals who are authorized to access SNL for 31 days or more

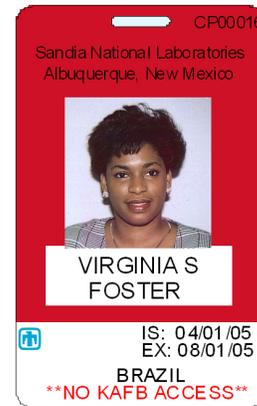
### Hosting a Foreign Visitor or Assignee

To host a foreign national visit, the responsible party must be an employee of Sandia or the Sandia Site Office (SSO), a U.S. citizen, be Q- or L-cleared, possess a DOE-approved badge, and have current completion of Foreign Corrupt Practices Act training (FCPA100) and Export Control Awareness Training (EC100) recorded in his or her TEDS training notebook as required courses.

Before hosting a foreign visitor or assignee:

- Ensure that the benefit of the visit to Sandia outweighs the potential risks.
- Identify any unclassified areas of your work that may be sensitive or might shed light on other work that is classified.
- Assess whether discussions of selected unclassified information with foreign nationals could divulge any proprietary details related to cooperative research or other collaborative work.

Be diligent when checking the security badges of uncleared foreign nationals. Site-specific badges worn by uncleared foreign national visitors and assignees have a red background and an expiration date. Foreign national employees will have a red badge without an expiration date.



## Foreign National Requests

As a host, it is your responsibility to ensure that foreign nationals do not gain access to DOE or Sandia information, programs, technologies, or sites without prior approval via the Foreign National Request (FNR) Security Plan (SP) process.

To determine if you need to submit a FNR SP or report a relationship to Counterintelligence (for yourself or someone else) use the [Foreign National Interaction System](#) wizard. Failure to obtain the necessary approvals before allowing access to a foreign national may result in a security incident, and potentially a security infraction.

Hosts of unclassified visits that involve uncleared foreign nationals must:

- Ensure that completed FNR SPs are submitted within the established time periods listed in [CPR400.3.5](#), *Foreign Interactions*.
- Document the foreign national's lawful status information (passport, visa, or other U.S. Citizenship and Immigration Services information) on FNR SPs for access to DOE and Sandia information, technologies, programs, or sites.
- Complete the Host Certification and the Host Risk Assessment documentation via the FNR SP application.
- Complete the Off-Site Host Briefing on an as-needed basis for non-SNL site access. (Foreign Interactions Office personnel will assist in determining when the briefing is needed and will administer the briefing in such cases.)
- Complete the Host Close-Out documentation via the FNR SP application within 10 calendar days of the conclusion of the foreign national's visit.
- Comply with all requirements as listed in [CPR400.3.5](#), *Foreign Interactions*.

The following information must be documented in an FNR SP:

- Approved access times.
- Individuals who are approved to host, co-host, or escort a foreign national.
- Approved buildings and rooms that the foreign national may access.
- Approved purpose of access, including subject matter and technical scope.
- Approved access to SNL information system resources.

For more information on your responsibilities when interacting with foreign nationals, refer to:

- [CPR400.3.5](#), *Foreign Interactions*
- [CPR400.3.11](#), *Access Control*
- [CPR400.3.17](#), *Export/Import Controls and Compliance*

**End of Module Question**

Jeff has just escorted a foreign national through a limited area in order to reach a property protection area. Samantha, the individual who prepared the Foreign National Request for Jeff, tells him that the foreign national was not authorized to enter the limited area. What did Samantha mean?

- a) A manager needed to authorize the shortcut.
- b) They accessed an area that wasn't authorized on the Foreign National Request (FNR) Security Plan (SP).
- c) Samantha should have accompanied them.
- d) The Badge Office needed to prepare an additional badge for the area.

---

**Answer:** b) They accessed an area that wasn't authorized on the Foreign National Request (FNR) Security Plan (SP).



## Module 6: Personally Owned Electronic Devices

### Objective:

Upon completing this module you will be able to recognize the security-related issues associated with cell phones, personal digital assistants (PDAs), and other personally owned electronic devices.

### Cell Phones

This year, as in past years, failure to keep personal cell phones out of the limited areas makes up the majority—approximately 60 percent—of Sandia's security incidents. Cell phones are classified as controlled articles because cell phones, even when turned off, may function as a listening or recording device. As a result of rapidly changing technology, cell phones now pose an even greater security threat because of built-in features such as cameras and recording capabilities.

You should establish a cell phone reminder for yourself, such as putting a chip clip on your lanyard, setting an alarm on your phone, developing an association between your badge and cell phone (when you put one on, take the other off), or whatever it takes to ensure that your cell phone is never taken into a limited area.

The majority of cell phone incidents occur because the individual has done something that deviates from his or her normal routine. For example:

- When the weather changes, a person may accidentally place his cell phone in his jacket pocket after making a call. Then, upon entering a limited area, he checks his belt (where he normally clips his phone), but forgets that his phone is in his jacket pocket.
- During a weekend trip, an employee places her cell phone in her purse. Upon returning to work on Monday, she is unaware that the phone is in her purse.

### Other Devices

Although cell phones receive the most attention, remember that there are also other personal electronic items, such as but not limited to, cameras, iPods and MP3 players, Blackberrys, Bluetooth devices, digital picture frames, and digital key chains that should also be kept out of limited areas.

For incidents involving controlled articles (cellular phones and other personal electronic devices), the responsible person will not be issued a security infraction if:

- The event is self-reported immediately to SIMP by the individual directly or by a person on his/her behalf.
- Potential for compromise of classified or unclassified controlled information can be ruled out. This is much easier to determine if the device was not used or connected to a computing system.
- The device did not enter a classified meeting, vault-type room, Special Access Program, or Sensitive Compartmented Information Facility (SCIF).
- The responsible individual holds a security access authorization (clearance).
- The responsible individual has not had a security incident within the preceding 12 months.

### **End of Module Question**

Susan is arriving at work when she receives a call from her husband. Susan removes her phone from her vehicle's console, talks to her husband, and absent-mindedly places the phone in her coat jacket instead of returning the phone to her the console.

What could Susan have done to prevent this incident from occurring?

- a) Place a reminder on her cell phone (e.g., a reminder clip on her lanyard).
- b) Arrange a time with her husband to call each other so she will anticipate the call.
- c) Put the cell phone on "silent" so it won't disturb her coworkers if it rings.
- d) None of the above.

---

**Answer:** a) Place a reminder on her cell phone (e.g., a reminder clip on her lanyard).



## Module 7: Technical Surveillance Countermeasures

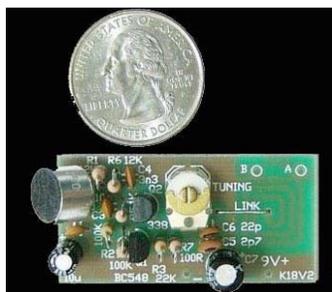
### Objective:

Upon completing this module you should be able to identify precautions to take if you suspect or are aware of technical surveillance vulnerabilities.

### **Surveillance Awareness**

Information about Sandia policy decisions and advances in Sandia technology is highly desirable to many foreign governments. The loss of such information could dangerously affect the financial welfare and security of our country. Eavesdropping devices are becoming easier to use and more sophisticated.

The Technical Surveillance Countermeasures (TSCM) Program is designed to detect, deter, isolate, and nullify technical surveillance penetrations and technical security hazards. TSCM technicians use several techniques and a variety of electronic and electrical equipment to detect illegal devices, more commonly known as “bugs,” designed to listen and/or transmit information.



### **Assessing Surveillance Vulnerabilities**

Maintain an awareness of your surroundings, especially to any changes to clocks, computers, or office furniture.

In the event that you suspect or become aware of a technical surveillance penetration, take the following steps:

1. Stop all classified discussions while maintaining other normal activities in the area.
2. Protect the area so that the suspected device cannot be removed.
3. Immediately report the incident to your manager and the TSCM Team, but do so away from the area where the threat is believed to be. Keep the following in mind:
  - Requests for TSCM services are classified as Secret/National Security Information (S/NSI) and must be arranged by a secure means (in person, classified hard-copy correspondence, or secure communications methods).
  - If reporting cannot be done by a secure means, simply state that you need to talk to a member of the TSCM Team immediately.

If you are on travel to a foreign country and suspect that your equipment has been tampered with during your stay, you must contact the TSCM Team upon your return. Do not take the equipment into any limited areas.

Upon returning from travel to a sensitive country with Sandia electronic equipment (e.g., laptops, personal digital assistants [PDAs], government-issued cell phone), you must notify the TSCM Team, and submit your equipment for inspection.

Remember, if you travel to a foreign country on Sandia-related business and fail to receive pre-approval, your trip will not be paid for by Sandia.

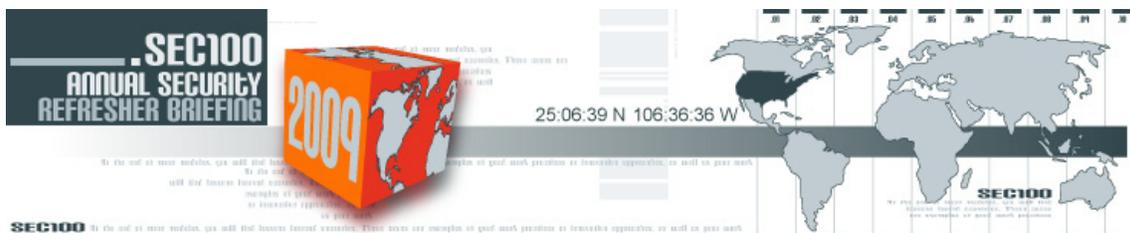
### ***End of Module Question***

John has just returned to work from a business trip to Europe. He is asked by his coworker, Jim, about his trip, and John tells him that he suspected his hotel room had been entered, and his laptop potentially used. Jim asks John what he's going to do about his suspicions. What should John do?

- a) Stop worrying; it's probably only his imagination.
- b) Report his suspicions about the incident to Technical Surveillance Countermeasures (TSCM).
- c) Refuse to travel to Europe in the future.
- d) Destroy his laptop.

---

**Answer:** b) Report his suspicions about the incident to Technical Surveillance Countermeasures (TSCM).



## Module 8: Classified Videoconferencing

### Objective:

Upon completing this module you should understand your responsibilities for classified videoconferencing at SNL.

### **Classified Videoconferencing at SNL**

The classified videoconference units located throughout SNL are for information up to Secret Restricted Data, Sigma 1 through 13, and Sigma 15. Classified secure IP (Internet Protocol) videoconferences may not include any information at the Sigma 14 level in any secure IP-classified videoconference room in California or New Mexico. Classified videoconferences with DOE/HQ Common Secure Videoconferencing Network (CSVN) do not allow Sigma 14 or Sigma 15.

The classified videoconference meeting owner is responsible for:

- Following established operational procedures as documented in the room binder.
- Signing and completing the functions documented on the Monitor Check Sheet.
- Completing the *Secure Videoconferencing Conference Log*.
- Verifying and enforcing need to know (NTK).

Other precautions that should be taken prior, during and after a classified videoconference include the following:

- Announce the clearance level and NTK requirements at the start of the meeting.
- Verify clearances and NTK of all participants.
- Be sure everyone has signed the *Secure Videoconferencing Conference Log*.
- Verify that the appropriate classification level is being transmitted to the remote site through the use of a sign or electronically.
- Maintain door control at all times.
- Terminate all classified conversations before using the room phone.

At the conclusion of a meeting:

- Terminate the call.
- Ensure you have logged off the room's computer.
- Shutdown the system as documented on the Monitor Check Sheet.
- Log the end time on the *Secure Videoconferencing Conference Log*.
- Verify that all classified material has been picked up and removed from the room.

- Close the door when you exit.

Each classified videoconference room may have a different set of requirements; therefore, it is important that the meeting owner follows all procedures on the Monitor Check Sheet. Both the Monitor Check Sheets and *Secure Videoconferencing Conference Logs* are audited regularly and must be completely filled out and signed. Incomplete logs could result in a security infraction.

A sample Monitor Check List form can be found at:  
[http://son.ca.sandia.gov/vact/vact\\_docs/monitor.doc](http://son.ca.sandia.gov/vact/vact_docs/monitor.doc).

A sample Secure Videoconferencing Log form can be found at:  
[http://son.ca.sandia.gov/vact/vact\\_docs/log.doc](http://son.ca.sandia.gov/vact/vact_docs/log.doc).

For more information, refer to “Videoconferencing” in [CPR400.2.10](#), *Using Information Technology (IT) Resources*.

### **End of Module Question**

Mark has just hosted a videoconference, taking the following steps:

- Verified clearances and the need to know of all participants.
- Verified that the appropriate classification level is being transmitted to the remote site electronically or through the use of a sign.
- Maintained door control at all times.
- Terminated all classified conversations before using the room phone.

At the conclusion of a meeting, Mark performs the following steps:

- Terminated the call.
- Ensured he was logged off the room’s computer.
- Shut down the system.
- Verified that all classified material had been picked up and removed from the room.
- Closed the door when he exited.

What did Mark fail to do?

- a) Failed to maintain door control at all times.
- b) Failed to terminate the call.
- c) Failed to complete required documentation of the event.
- d) Failed to verify clearances and need to know of all participants.

---

**Answer:** c) Failed to complete required documentation of the event.



## Module 9: Classification

### Objective:

Upon completing this module you should be able to determine when to seek assistance from a Derivative Classifier (DC) or the Classification Office.

### Classification Practices

Classification is the identification of information that needs to be protected in the interest of national security. Through classification, Sandia safeguards important information, thus preventing its compromise (i.e., restricting its availability to adversaries, yet allowing its use by individuals who have the appropriate clearance and need to know [NTK]).

You are required to protect classified information/material throughout its life cycle. A DC or Classification Office staff member will help you determine whether your information/material is classified.

### Determining Classification Issues

Per DOE policy, classification decisions are made by individuals who are knowledgeable in their technical fields and trained to recognize classification issues. These individuals are known as DCs and, at SNL, are authorized and trained by the Classification Office.

### Classification Responsibilities

You are responsible for ensuring that all documents are protected at the highest potential classification level and category. You should also ensure a classification review of a document within 180 days of its creation and prior to its release outside the organization when the document:

- Contains information in a classified subject area.
- Is suspected to contain classified information.

Managers are responsible for ensuring that:

- Personnel under their supervision receive briefings that explain the information with which they work has the potential to be classified.
- If a staff member who is no longer authorized to access classified information in a classified subject area subsequently creates a new document in that area, the document must be reviewed by a DC.

Consult a DC before beginning work on a project in a classified subject area and as the project progresses. Inform the DC about the project's scope, the internal and external organizations involved, and any associated classification concerns.

To find a DC, see the Classification Office's DC Access List. If you don't have access to the Sandia Restricted Network (SRN), call the Classification Office (505-844-5572 in NM, or 925-294-2202 in CA) for guidance.

### ***Review and Approval Process for Release of Information***

Sandia (SAND) reports, information to the public, or any information having a wide distribution must go through a formal Review and Approval for Release of Information process. Any sensitive unclassified information should be properly marked as official use only (OUO). Technical information and some military programmatic information that is not intended for public release should be export controlled and appropriately marked. Under certain conditions, foreign nationals may have export-controlled information. Contact Export Control for guidance if you anticipate disclosing technical information to a foreign national.

To obtain services your DC cannot provide, such as the need for an Unclassified Controlled Nuclear Information (UCNI) Reviewing Official or to discuss classification issues in the absence of your DC, contact the Classification Office or check the Classification website.

### ***Association and Compilation***

Classification association, or compilation, are concerns at SNL. This is a particularly critical issue with e-mail correspondence. When certain bits of information are combined, they often reveal information of greater sensitivity than any of the individual bits taken separately. You must take care to avoid associating or compiling information that may result in the creation of classified information. Consult a DC to avoid potential classification problems due to association or compilation. Always consult a DC to avoid associating or combining unclassified information that can become classified through association or compilation.

### ***Improperly Classified Documents***

A DC's determination may be misclassified. To downgrade the level of a document requires a Classification Analyst (CA) in the Classification Office. If a complete declassification is needed, a Derivative Declassifier (DD) must also be involved. CAs are trained and certified by DOE as DDs.

If you want to formally challenge your DC's determination, you may contact the Classification Office for assistance. When challenging the classification status of a document or material, you may appeal to the applicable program DC. The DC must reply to your request within 15 days. If the problem is not resolved to your satisfaction, contact the Classification Office to assist you in appealing your request.

A DC can make a determination to upgrade a document. Downgrading or declassifying requires both a DC and a DD. Only CAs are trained and authorized as DDs by DOE.

Upgrades to Top Secret (TS) determinations can be made only by a Classification Officer and DCs authorized at the TS level.

Documents containing only National Security Information (NSI) are scheduled for declassification on the occurrence of an event or date, unless specifically exempted. However, a DD's review is required prior to the actual declassification and remarking of the document.

### **No Comment Policy**

Confirmation, denial, or extension of public statements concerning classified information is prohibited. This "No Comment Policy" is intended to avoid giving credence to information in the public domain that may be of doubtful authority that could erode the protection of related classified information. Accidental release does not mean that a document or material has been declassified.

Inquiries on inadvertent or unauthorized releases of classified matter require a "no comment" response from you. Inadvertent release of classified information does not declassify information. At SNL, refer media inquiries to Media Relations and Communications (505-844-4902 in NM, or 925-294-2447 in CA).

Remember, you are required to protect information/material that you suspect might be classified even before acquiring classification determination from a DC.

### **End of Module Question**

Doug, a Sandia employee, is working on a classified project with a contractor, Brian. As you observed, Brian asked Doug to send him a list of unclassified titles of the classified procedures they would be working on. Doug, assuming that this was a routine administrative task, pulled the documents from the safe, and e-mailed the titles to Brian. Doug copied his manager on his e-mail to Brian. When his manager opened the e-mail, he realized that combining the unclassified titles resulted in a classified e-mail. What should Doug have done to prevent this incident from occurring?

- a) Given Brian the information by phone.
- b) Placed the information on a sheet of paper and handed the information to Brian.
- c) Sought guidance from his Derivative Classifier.
- d) Not included his manager on the e-mail distribution.

---

**Answer:** c) Sought guidance from his Derivative Classifier.



## Module 10: Classified Matter Protection and Control

### Objective:

Upon completing this module you should be familiar with Classified Matter Protection and Control (CMPC) practices.

### **Protecting Classified**

All classified matter must be protected from unauthorized disclosure. Proper storage of classified matter is an area of particular concern. Putting a classified document in your desk, in a cabinet, in a locked room, or any other similar types of methods does not qualify as proper storage. **Classified matter must be stored only in an approved GSA safe, a certified vault, a certified vault-type room (VTR), or by other storage methods specifically approved by Physical Security and/or CMPC Programs.**

Many requirements for protecting classified matter exist in addition to storage. Here are some additional requirements for protecting classified matter:

- All work involving classified information must be performed in approved security areas (limited areas or above).
- Classified discussions must not be held in hallways, break rooms, rest rooms, or other areas where access cannot be adequately controlled or the discussion may be heard by individuals without need to know (NTK).
- When discussing classified or when giving a formal presentation, clearly indicate to your listener(s) what information is classified and at what level, category or caveat.
- Classified discussions must be held in approved areas, ensuring that those without a NTK do not overhear the conversation.
- Classified matter must never be left unattended.
- Classified processing must be done only on computers approved for processing classified.
- Technical presentations for formal classified meetings must go through the [Review and Approval](#) process.
- When giving a presentation at a formal classified meeting, do not exceed your approved discussion topic area.



- When using a classified conference room, ensure all audio/visual equipment is placed in an inactive (secure) mode if it will not be used.

To prevent unauthorized disclosure, classified matter has specific requirements for the following:

- Generating
- Marking
- Physical protection
- Storage
- Reproduction
- Accountability
- Transmission (including hand-carrying)
- Destruction
- Incident reporting
- Emergency procedures

For additional information on protecting classified matter, refer to [CPR400.3.12](#), *Management of Classified Matter*.

### ***End of Module Question***

Jake is working with classified documents. He receives a call from his wife, reminding him that he has to pick up his son from his evening soccer practice. Jake piles the documents on his desk together and places all of them, including the classified, in a locked desk drawer. Did Jake properly store the classified?

- a) Yes, classified is safe and properly protected in a desk.
- b) No, he should store classified matter in a locked cabinet instead.
- c) No, classified matter should be stored by an approved method, such as a GSA-approved safe or a certified vault/vault-type room.
- d) No, he should have taken the document with him.

---

**Answer:** c) No, classified matter should be stored by an approved method, such as a GSA-approved safe or a certified vault/vault-type room.

## SEC100 Feedback Form

Customer feedback is important to us. Please complete the evaluation form below and forward it to Course Administrator, MS1341, fax number (505) 284-6079.

Rate on a scale of 1- 5 (with 1= poor and 5 =excellent):

The ease of using of this learning tool and/or test? 1 2 3 4 5

The organization of information presented? 1 2 3 4 5

The amount of information presented? 1 2 3 4 5

The usefulness of the information presented? 1 2 3 4 5

Your level of knowledge related to this topic BEFORE using this learning tool and/or test?

1 2 3 4 5

Your level of knowledge related to this topic AFTER using this learning tool and/or test?

1 2 3 4 5

The overall quality of this learning tool and/or test? 1 2 3 4 5

Fill in the blanks:

What was most valuable about this learning tool or test?

---

---

---

---

What information needs to be corrected, inserted, removed, or updated?

---

---

---

---

What could be done to improve or enhance this learning tool or test?

---

---

---

---