SEC100

SEC100
Annual Security Refresher Briefing

2008

Table of Contents

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 refresher briefing.
Why is SEC100 important?	An annual refresher briefing ensures that all Members of the Workforce (employees, contractors, and consultants) are aware of new security information, as well as site-specific information that may affect local procedures. The ultimate goal is to help reduce security incidents at SNL.
What happens if I delay taking the course?	Failure to successfully complete this briefing by your due date will result in your DOE badge (automated access) being disabled until compliance has been accomplished.

Remember—Your security responsibilities are ongoing. Your actions or inactions could 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).

SEC100 addresses the following security-related topics:

- New Badge (Credential).
- Classification.
- Reporting Requirements.
- Security Incidents.
- Foreign Interactions.
- Foreign Travel.

Note: Sandia's Business Rules, including Corporate Process Requirements (CPRs), are continually revised to ensure that they remain current and in compliance with DOE directives, federal and state laws, and Sandia best-management practices. Thus, when discrepancies or inconsistencies exist between the Business Rules and this briefing, you must follow the requirements cited in the Business Rules.

OBJECTIVES

Module 1

Upon completing this module, you will be able to identify:

- The process for obtaining a replacement badge (a.k.a. federal credential).
- The different types of credentials.

Module 2

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

Module 3

Upon completing this module, you will be able to recognize what security-related information needs to be reported.

Module 4

Upon completing this module, you will recognize the security-related issues associated with cell phones, personal digital assistants (PDAs), and stolen badges.

Module 5

Upon completion of this module, you will be able to recognize:

- The definition of an uncleared foreign national.
- The requirements for interacting with uncleared foreign nationals.
- The function of SNL's Foreign Interactions Office (FIO).

Module 6

Upon completing this module, you will recognize:

- The requirement for obtaining pre-approval for official foreign travel.
- The requirement for reporting instances of unofficial foreign travel to a sensitive country.

HOW TO OBTAIN BRIEFING MATERIALS

This briefing is also available in pdf format in Web Fileshare accessible from the SEC100 course description. It is also available through the Sandia external website at the Contractor Toolcart (http://www.sandia.gov/FSO/briefings.htm). Those who complete the pdf version should send their Record of Completion to the Course Administrator, MS-1341, or fax (505) 284-6079.

Completion Time

Course completion time is estimated to be between 20-40 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 course completion is not authorized.

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 Travel Help Line
  - NM & CA: (505) 845-1300
- SNL/NM Clearance Office - (505) 844-5688
- SIMP Pager
  - NM: (505) 540-2382
  - CA: 888-932-9710
- Sandia Protective Force - (505) 844-3155

Glossary

Glossary of Security Terms

Corporate Process Requirements (CPRs) and Manuals

CPR300.4.3, *Employee Conduct and Corrective Discipline*

CPR400.2.10, Section 4.8, “Prohibited and Controlled Electronic Devices and Media”

CPR400.2.20, *Management of Information Throughout Its Life Cycle*

CPR400.3.1, *Technical Surveillance – Audio and Video Recording*

CPR 400.3.5, *Foreign Interactions*

CPR 400.3.7, Attachment B, “Reporting Personal Information”

CPR400.3.8, *Security-Related Roles and Responsibilities*

CPR400.3.11, *Access Controls*

CPR400.3.12, *Management of Classified Matter*

CPR400.3.13, *Foreign Travel*

CPR400.3.16, *Cellular Phones*

DOE Manual 470.4-1, Section K, "Safeguards and Security Awareness Programs"

DOE O 142.3, *Unclassified Foreign Visits and Assignments*

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

Classification Homepage

Classification Office's DC Access List

Corporate Investigations website

Contractor Toolcart

HSPD-12 website

Personnel Security Homepage

Technical Surveillance Countermeasures (TSCM) Homepage

Forms/Aids

SF 7643-FTR, First Time Foreign Traveler Request Information Form

SF 7643-RFT, Repeat Foreign Traveler Request Information Form

Foreign National Request (FNR) Security Plan (SP) Decision Tool Wizard

CONTACTS

For questions:	Contact:
Course Administrator	Margret Tibbetts, mrtibbe@sandia.gov, (505) 845-7776, MS-1341
Program Owner	Fran Armijo, fparmij@sandia.gov, (505) 284-2416, MS-1341

SYMBOLS

The caution symbol denotes key supplemental information.

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

MODULE 1: NEW BADGE (CREDENTIAL)

Objectives

Upon completing this module, you will be able to identify:

- The process for obtaining a replacement badge (a.k.a. credential).
- The different types of credentials.

In Brief—All federal facilities, including SNL, are required to adopt a standardized federal credential by October 27, 2008. The federal credential will replace your DOE badge as a form of identification and access authorization.

WHO… **…will receive the new federal credential?**	Every Sandia employee, contractor, and consultant who has a security clearance will be required to have a federal credential, which will replace their current badge. All credentials will have start and end dates, and will be valid for 5 years. Contractor and consultant credentials will include expiration dates consistent with the lengths of their contracts.
WHY… **…do I need a federal credential?**	Homeland Security Presidential Directive 12 (HSPD-12), issued August 27, 2004, established a goal of eliminating the wide variations in the quality and security among forms of identification used to gain access to secure federal facilities where there is a potential for terrorist attacks. Subsequently, the National Institute of Standards and Technology (NIST) developed a standard for a "smart card" credential that will include secure, unique information about each credential holder. The security features that NIST established for the federal credential are: • Based on sound criteria to verify an individual's identity. • Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation. • Used for rapid electronic verification of personal identity. • Applicable to all government organizations and contractors. • Used to grant physical access to federally controlled facilities. • Used to grant logical (cyber) access to federally controlled information systems. This feature will be implemented at Sandia at a later date. • Not applicable to identification associated with national security systems. • Implemented in a manner that protects individual privacy.

WHAT…

…makes the credential "smart"?

Each credential contains the following components:

- Integrated circuit chip (ICC) that stores 64KB of data that includes:
  - Four Public Key Infrastructure (PKI) digital certificates (Personal Identity Verification [PIV] authentication, card authentication, digital signature, and encryption).
  - Two interoperable fingerprint templates.
  - Digital photo.
  - Cardholder Unique Identifier (CHUID), including organization affiliation, agency affiliation, department affiliation, and expiration date.
- Magnetic stripe.

WHAT…

…will the credential look like?

Your federal credential will also look different from your current DOE badge. **It will not have color coding to indicate clearance level.** Instead, colored stripes will indicate the type of individual, as follows:

- Federal Contractor (includes Sandia employees, contractors, and consultants)—green stripe.
- Foreign national—blue stripe.
- Federal employee—white (essentially no stripe because the background is also white).
- Additionally, first responders will have a separate red stripe on the bottom of their credentials.

Federal Contractor* - Green stripe	Foreign National - Blue stripe	Federal employee - White (no stripe)
		

*Employees, contractors and consultants

WHEN…

…will I receive my new credential?

By early CY2008, there will be four credentialing centers in Albuquerque, including two at the Innovation Parkway Office Complex (IPOC). Lawrence Livermore National Laboratory (LLNL) is planning to host two credentialing centers for the Livermore area. Other credentialing centers will be established throughout the United States, including Southern Nevada, where one or more will be located in the Las Vegas area. When the credentialing centers are operational, Sandia employees will be enrolled first, followed by cleared Sandia contractors and consultants.

When it is your turn to receive a federal credential:

1. You will be notified by e-mail to schedule an appointment online at a credentialing center.
2. During your first visit, you will be required to present two forms of identification (one of which must be a government-issued ID), and you will be fingerprinted.
3. Approximately 3 weeks later, you will be notified to return to the credentialing center to pick up your credential.
4. During the return visit, you will be required to show one form of photo ID, and you will have a new set of digital fingerprints compared to the index fingerprints taken at the time of enrollment.

HOW…

…will the new credential work?

- **Access to Sandia-controlled premises**—Eventually, badge-swipe readers at SNL will be replaced by new smart-card readers. Until then, you will swipe your new credential in the same way as your current DOE badge. When the badge readers have been replaced, you will touch your credential to a reader and enter your personal identification number (PIN) (where applicable) to unlock the door, gate, or turnstile. Certain protected, sensitive facilities may also require fingerprint identification (a.k.a. three-factor authentication).
- **Access to other federal facilities**—Access controls are established at each facility based on agency-specific requirements and/or local protection requirements. Where one of the new smart-card readers exists, you will gain access as described above. If the system recognizes you and verifies your credential as valid, you will be allowed access; otherwise you may need to be enrolled in the facility's access-control system. Regardless, your federal credential will be required.
- **Access to information system resources**—When logical access has been implemented at SNL, you will log on by inserting your federal credential into a smart-card reader, then enter your username and password as usual to access most applications (a.k.a. two-factor authentication).

- *A replacement credential will take 2 to 4 weeks to obtain.*
- *Until the new federal credential is fully implemented at SNL, you may be required to keep your current DOE badge as an alternate form of access authorization.*
- *Uncleared employees, contractors, consultants and visitors will not be issued the new credential at this time. They will continue to receive site-specific badges, which will be issued by Sandia Badge Offices rather than at a credentialing center.*

For more information about the re-badging initiative and the new federal credential, see the HSPD-12 website.

End of Module Questions

1. All cleared federal employees and contractors will be required to have a federal credential.

- ☐ **a)** True
- ☐ **b)** False

2. The goal for issuing the new federal credential is to eliminate wide variations in the quality and security of forms of identification used to gain access to secure federal facilities where there is potential for_____.

- ☐ **a)** Protests
- ☐ **b)** Military units
- ☐ **c)** Terrorist attacks
- ☐ **d)** Layered security

3. A cleared foreign national badge will be:

- ☐ **a)** White with red stripe
- ☐ **b)** White with blue stripe
- ☐ **c)** White with green stripe
- ☐ **d)** Layered security

Answers to end of module questions

1. a) True

2. c) Terrorist attacks

3. b) White with blue stripe

MODULE 2: CLASSIFICATION

Objectives

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

In Brief— 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.

Classification is the identification of information that needs to be protected in the interest of national security. Through classification, SNL 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).

WHO… **…determines 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 trained by the Classification Office.
WHAT... **...are my responsibilities?**	You are responsible for ensuring that all documents: • Are protected at the highest **potential** classification level. • Receive a classification review when the: o Documents contain information in a classified subject. o Document is suspected of containing 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.

WHEN…

…do I need DC assistance?

Always 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 for guidance. Contact the Classification Office to discuss any clarification issues that the DC cannot provide.

Sandia Review and Approval for Release of Information Process

- 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.
- All technical information and some military programmatic/cost/tactics information that is not publicly available/public domain is export controlled information (ECI). 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.

Issues of Specific Concern When Handling Information That Might Be Classified

WHAT...

...is association or compilation?

An issue of continuing concern at SNL is *classification association* or *compilation*. 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 elaboration.

WHAT...

...if a document is improperly classified?

A DC can make a determination to upgrade a document. Downgrading or declassification require both a DC and a Derivative Declassifier; upgrades to TS determinations can only be made by a Classification Officer at Sandia. At SNL, only the Classification Office's Classification Officer and some Classification Analysts are authorized Derivative Declassifiers.

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

HOW… **…do I challenge the classification?**	To challenge 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.
WHEN… **…does "No-Comment Policy" apply?**	Inquiries on inadvertent release of classified requires a "no comment" response from you. Inadvertent release of classified information does not declassify information. Refer inquiries about classified information to Media Relations. 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.

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

See CPR400.2.20, *Management of Information Throughout Its Life Cycle*, for additional classification information.

For specific guidance, consult the appropriate Classification Office:
NM – (505) 844-2490
CA – (925) 294-2202

End of Module Questions

1. Who should be consulted before you work on a new project in a classified subject area?

- ☐ **a)** Classified Material Specialist
- ☐ **b)** Computer Security Representative
- ☐ **c)** Derivative Classifier
- ☐ **d)** Classified Administrative Specialist

2. The declassification process requires two individuals, one of whom must be a Derivative Declassifier.

- ☐ **a)** True
- ☐ **b)** False

Answers to end of module questions

1. c) Derivative Classifier

2. a) True

MODULE 3: REPORTING REQUIREMENTS

Objectives

Upon completing this module, you will be able to recognize what security-related information needs to be reported.

In Brief— When you completed your original Questionnaire for National Security Positions (QNSP) (SF86)—and when you requested renewal of your clearance, if applicable—you were made aware of your responsibility to report certain personal information. Those reporting responsibilities are ongoing.

Below is a summary of reporting requirements. For a complete list of reporting requirements including contacts refer to the reporting requirements matrix on the SRN or the contractor website on the SON.

When	What
Immediately	• If you are approached or contacted by any individual seeking unauthorized access to classified matter or special nuclear material (SNM). • Report **all** substantive contacts with **any** foreign national. o Report each foreign national one time. o Report every time you have a face-to-face meeting with a foreign national where SNL business is conducted. **Note:** In addition to reporting the fact that you have a relationship with a sensitive foreign national, you must also report each individual communication with that person. • If you are employed by, represent, or have other business-related associations with a non-sensitive foreign or foreign-owned interest or foreign national. • If you no longer require your clearance.

Orally within 2 working days **AND** **In writing within the next 3 working days**	If you are arrested or are subject to criminal charges, or if you are detained by any law-enforcement authority for violations of the law within or outside of the United States. Traffic violations of $250 or less need not be reported unless they are drug or alcohol related. • If you file for bankruptcy. • If you have your wages garnished. • If you are a U.S. citizen who changes citizenship or acquire dual citizenship. • If you are a foreign citizen who changes citizenship. • If you change your name. • If you are hospitalized for a mental illness. • If you are treated for drug or alcohol abuse.
Within 45 days	• If you enter into a marriage or cohabitation in a spouse-like relationship.

When in doubt as to whom to report information, call (505) 845-9900 in New Mexico, (925) 294-1358 in California.

See the following for additional guidance:

- CPR 400.3.7, Attachment B, "Reporting Personal Information"
- Corporate Investigations website
- Contractor Toolcart

End of Module Question

1. **A traffic violation of $250 or less which is drug or alcohol related must be reported orally within 2 days.**

   ☐ **a)** True

   ☐ **b)** False

2. **You must immediately report if you are approached or contacted by any individual seeking unauthorized access to classified matter or Special Nuclear Material (SNM).**

   ☐ **a)** True

   ☐ **b)** False

3. **Marriage or cohabitation with a person in a spouse-like relationship must be reported within 45 days.**

   ☐ **a)** True

   ☐ **b)** False

Answers to end of module questions

1. a) True

2. a) True

3. a) True

MODULE 4: SECURITY INCIDENTS – CELL PHONES, PDAS, AND STOLEN BADGES

Objectives

Upon completing this module, you will recognize the security-related issues associated with cell phones, personal digital assistants (PDAs), and stolen badges.

In Brief— Your security responsibilities are ongoing. Your actions or inactions could 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*).

Each year, this Annual Security Refresher Briefing reminds you about the need to avoid taking cell phones into limited or more restricted areas. The main reason for this is because cell phones—even when turned off—may function as a listening and/or recording devices. As the result of rapidly changing technology, however, cell phones now have capabilities (e.g., cameras and MP3 recording features) that make them even more of a security threat.

Unfortunately, cell phone-related security incidents continue to be a problem.

Year	Cell Phone Incidents
2005	273
2006	233
2007	277

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, until it rings during a meeting.

WHAT…

…type of cell phones are not permitted?

- Personal cell phones are not permitted within limited or more restricted areas unless an authorized exception has been granted by Technical Surveillance Countermeasures (TSCM) personnel.

Note: While cell phones are permitted in property protection areas (PPAs) some managers of PPAs have chosen to disallow cell phones in their facilities.

- Cell phones owned by other U.S. government agencies are not allowed in SNL limited or more restricted areas unless a prior exception has been obtained from TSCM.

WHY…

…are PDAs a security concern?

Personal Digital Assistants (PDAs)—Today's PDAs come equipped with recording and/or transmission features (e.g., Bluetooth, WiFi), and present a security risk. You are responsible for ensuring that the WiFi/Bluetooth features are always disabled. Learn how to disable those features on your Sandia-issued PDA. Consult the Corporate Computing Help Desk (CCHD, 845-2243) for assistance. Also, remember to use the Preferred Systems Query when ordering a PDA.

HOW…

…can I avoid prohibited article-related incidents?

To avoid unintentional security incidents:

- Develop a positive routine of always stopping to check for prohibited items when you arrive at a security area boundary.
- Condition yourself to make some sort of mental connection between your badge—the item you must always have—and items that are prohibited.
- At your next staff meeting, share ideas for reminding individuals not to take cell phones into limited or more restricted areas.
- As you enter a limited area, turn to the person entering behind you and ask if he or she has any prohibited items.
- Utilize the cell phone lock boxes at limited area entry points.
- If you are arranging a visit to SNL, ask your visitor if he or she is planning to bring a cell phone, PDAs, or other prohibited items, and inform him or her about SNL's restrictions on such items.

WHY…

…shouldn't I leave my badge in my vehicle...

In New Mexico, 144 badges were stolen from vehicles between January 2005 and October 2007. Your badge could be used to gain unauthorized access to SNL and other DOE-related facilities and could result in the compromise of national security. You are responsible and accountable for safeguarding and providing the appropriate level of security for your Sandia-issued security badge. Keep your badge in a safe, secure place that is not readily visible to others.

- *Failure to properly protect your badge may result in a security infraction and disciplinary action.*
- *Replacement for the new federal credential will take 2 to 4 weeks to obtain.*

See the following for additional information:

CPR400.2.10, Section 4.8, "Prohibited and Controlled Electronic Devices and Media"

CPR400.3.16, *Cellular Phones*

End of Module Questions

1. **Your security responsibilities are ongoing. Your actions or inactions could lead to a serious security breach, as well as significant fines to Sandia Corporation.**

   ☐ **a)** True

   ☐ **b)** False

2. **Most cell phone incidents occur because _____**

   ☐ **a)** Sandia does not provide enough cell phone boxes.

   ☐ **b)** The responsible individual has intentionally taken his or her cell phone into a limited area.

   ☐ **c)** The responsible individual has deviated from his normal routine.

3. **PDAs present a security risk because they come equipped with recording and/or transmission features (e.g., Bluetooth, WiFi).**

   ☐ **a)** True

   ☐ **b)** False

4. **Failure to properly protect your badge may result in a security infraction and disciplinary action.**

   ☐ **a)** True

   ☐ **b)** False

Answers to end of module questions

1. a) True

2. c) The responsible individual has deviated from his normal routine.

3. a) True

4. a) True

MODULE 5: FOREIGN INTERACTIONS

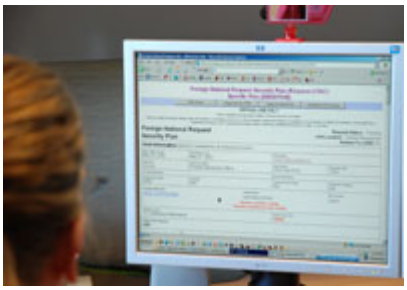
Objectives

Upon completion of this module, you will be able to recognize:

- The definition of an uncleared foreign national.
- The requirements for interacting with uncleared foreign nationals.
- The function of SNL's Foreign Interactions Office (FIO).

In Brief— Interaction with uncleared foreign nationals is an essential part of DOE's commitment to international collaboration in unclassified research projects. In many cases, technology development can be accomplished more efficiently and economically through cooperation among countries involved in the same research. It is everyone's responsibility to ensure that foreign nationals do not gain access to DOE information, programs, technologies, and Sandia sites, without prior approval.

WHO... **...is considered a Foreign National?**	Per DOE O 142.3, *Unclassified Foreign Visits and Assignments*, a foreign national is a person who was born outside the jurisdiction of the United States, is a citizen of a foreign government, and has not been naturalized under U.S. law.
HOW… **…can I tell if I'm interacting with a foreign national?**	Before any visit or substantive business discussions take place, due diligence requires that you ask the person involved if he or she is a U.S. citizen. If you are still uncertain, based on the reply, assume that the answer is "no" and act accordingly until the person's status can be determined. The FIO has created a Foreign National Request (FNR) Security Plan (SP) Decision Tool Wizard to help customers determine if their interaction with a foreign national requires an FNR SP and, if required, the type of FNR SP to process.  *Uncleared foreign national employees, visitors, or contractors are issued a red, uncleared badge by the appropriate Badge Office.* If a visitor arrives at SNL and you discover that he or she is a foreign national and has not completed the FNR SP approval process, do the following immediately: • Escort the foreign national from the premises. • Follow the OOPS process by immediately reporting the incident to your manager and to the Security Incident Management Program (SIMP).

WHERE… **…do I learn my responsibilities regarding foreign interactions?**	If you host or escort a foreign national, you are required to annually complete EC100, *Export Control Awareness Training*, and FCPA100, *Foreign Corrupt Practices Act*. If you have any interactions with foreign nationals, consult the course description for these courses.
WHO… **…manages the approval process for access by uncleared foreign nationals?**	SNL's FIO manages the approval process for unclassified foreign national access to DOE information, programs, and technologies and SNL sites through the FNR SP process. **Note:** DOE requires that all foreign national access be tracked and documented. The FIO tracks and documents approval decisions regarding all uncleared foreign national access via the electronic FNR SP. 
WHAT… **…has to happen to allow access by an uncleared foreign national?**	It is everyone's responsibility to ensure that foreign nationals do **not** gain access to DOE information, programs, technologies, and SNL sites, without prior approval via the FNR SP process. Failure to acquire the necessary approval before allowing foreign national access may result in a security incident or infraction. Time requirements associated with FNR SP submittal are based on the "sensitivity" of the foreign national and the nature of the access. See CPR400.3.5, *Foreign Interactions*, for FNR SP submittal criteria.
WHAT… **…information is on an FNR SP?**	The following information is documented via an FNR SP: • Approved access dates. • 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.

If you host an uncleared foreign national, you are responsible for adhering to the rules and requirements listed in the FNR SP. Hosts of uncleared foreign nationals are to conduct the foreign nationals' access in a manner that is beneficial to DOE and Sandia, ensuring that vital interests are not compromised during the interaction.

See CPR 400.3.5, *Foreign Interactions*, for additional information. See the International and Special Programs Department website for information about hosting cleared foreign nationals, including access to classified matter.

End of Module Questions

1. A foreign national is any person who was born outside the jurisdiction of the United States, is a citizen of a foreign government and has not been naturalized under U.S. law.

- ☐ **a)** True
- ☐ **b)** False

2. What electronic document is to be completed allowing access by an uncleared foreign national to unclassified DOE information, programs, and technologies or SNL sites?

- ☐ **a)** Foreign National Request (FNR) Security Plan (SP)
- ☐ **b)** Foreign Travel Request (FTR)
- ☐ **c)** Official Move Request (OMR)
- ☐ **d)** None of the above

Answers to end of module questions

1. a) True

2. a) Foreign National Request (FNR) Security Plan (SP)

MODULE 6: FOREIGN TRAVEL

Objectives

Upon completing this module, you will recognize:

- The requirement for obtaining pre-approval for official foreign travel.
- The requirement for reporting instances of unofficial foreign travel to a sensitive country.

In Brief— DOE requires Members of the Workforce (employees, contractors, and consultants) to obtain prior approval from SNL management and DOE for **all** official foreign travel (including travel to Canada and Mexico).

Official foreign travel includes travel funded from any source, including DOE, Reimbursable, Work-for-Others (WFO), Program Development, Indirect, and Center Support.

WHAT…

…are the requirements associated with official foreign travel?

If you are planning official travel to a foreign country, you are required to complete SF 7643-FTR, *First Time Foreign Traveler Request Information Form*, or SF 7643-RFT, Repeat *Foreign Traveler Request Information Form*. The completed form should be e-mailed to fortravel@sandia.gov or faxed to (505) 284-5030.

The deadlines for submitting official foreign travel trip requests to the Foreign Travel Office are as follows:

- Sensitive official foreign travel—52 calendar days prior to departure date.
- Non-sensitive official foreign travel—37 calendar days prior to departure date.

Note: There are many restrictions on laptops and other electronic equipment you may take on foreign travel because of the heightened risks associated with using them in a foreign country. Consult the Laptops on Foreign Travel (LOFT) homepage to review those restrictions and for assistance information.

WHAT…

…are the requirements associated with personal foreign travel?

Members of the Workforce (regardless of whether they hold a DOE clearance) must report all personal foreign travel to **sensitive countries**. Report such travel via the corporate Travel Information System prior to departure or as soon as is practical, in emergency cases.

Note: You should maintain documentation for all personal travel to non-sensitive countries for future reference during clearance reinvestigations.

Always exercise caution when sharing information with anyone to ensure that you do not inadvertently disclose sensitive, unclassified information.

See the following for additional information:

- CPR400.3.13, *Foreign Travel*
- CPR400.3.1, *Technical Surveillance – Audio and Video Recording*
- Foreign Travel Help Line: (505)844-1300

End of Module Questions

1. Unofficial travel to a sensitive country must be reported _____

- ☐ **a)** Doesn't matter
- ☐ **b)** 37 calendar days prior to departure
- ☐ **c)** 52 calendar days prior to departure
- ☐ **d)** Prior to departure or as soon as practical

2. Official travel to a sensitive country must be reported____.

- ☐ **a)** Doesn't matter
- ☐ **b)** 37 calendar days prior to departure
- ☐ **c)** 52 calendar days prior to departure
- ☐ **d)** Prior to departure or as soon as practical

3. Official travel to a non-sensitive country must be reported____.

- ☐ **a)** Doesn't matter
- ☐ **b)** 37 calendar days prior to departure
- ☐ **c)** 52 calendar days prior to departure
- ☐ **d)** Prior to departure or as soon as practical

Answers to end of module questions

1. d) Prior to departure or as soon as practical

2. c) 52 calendar days prior to departure

3. b) 37 calendar days prior to departure

SEC100 FEEDBACK FORM

Customer feedback is important to us. Please complete the evaluation form below and forward it to Course Administrator, MS1341, fax number 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?

  _____

  _____

  _____

  _____