SEC100
Annual Security Refresher Briefing

SAND2012-8571 P

Think.Assess.Protect: Keep us secure.

security.sandia.gov
security@sandia.gov

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

Welcome to the New and Improved SEC100

You spoke, we listened

During SEC2011, the Labs-wide Security Learning and Feedback Activity, which replaced SEC100 last year, we asked you for suggestions, comments, and any other input about Sandia's Security Program. We promised to adopt viable ideas that could improve security or make it less burdensome. Your feedback during that event proved what we had always assumed: you recognize the importance of good security, and you're eager to implement effective measures…you just need help doing so. And you made it clear that help should come in the form of clear guidance and useful tools, along with information that is relevant to the workplace of today.

But the goal is the same

The ultimate goal of this refresher briefing is to reinforce what you already know: each of us is responsible for protecting sensitive information and classified matter. You may not think of security as being that simple, but it is. Most security requirements, in one way or another, are about ensuring information and material are kept from those who don't have a need to know (NTK).

Let's Get Started

During this reinvented SEC100, we'll follow Sam Seriously through a typical work day at SNL. Unfortunately for Sam, he will experience situations that challenge his understanding of security requirements. But, like you, he knows his security responsibilities; thus, nothing he encounters can prevent him from ensuring secure operations. Your challenge is to help him make the right decisions.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 01: REPORTING MISTAKES

Meet Sam

Our story begins at 8:00 am on an average Tuesday morning. Sam is an engineer who works on the Super-Secret Ray Gun (SSRG) project. He's been working at SNL for 7 years, he has a Q clearance, and he works in a Limited Area. He loves his work and he knows the rules.

SEC100

Module 1: Reporting Mistakes

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 01: REPORTING MISTAKES

This morning, there's an important meeting about the SSRG project in the Limited Area conference room. Unfortunately, forgetful Sam didn't leave his BlackBerry behind at his desk. As the meeting progresses, another participant says something classified.

SEC100

WHAT SHOULD SAM DO?

Tell the meeting host that he has his phone with him. Since the phone was off, there isn't a need to report.

Go to page 5.

Remove the BlackBerry from the meeting, and call the Security Incident Management Program (SIMP) after the meeting.

Go to page 6.

Your Answer:

Tell the meeting host that he has his phone with him. Since the phone was off, there isn't a need to report.

Close, but Sam needs to do more...

Even though his phone was off, Sam still needed to report the incident. All communications devices must be removed from areas where classified processing or classified discussions are taking place, regardless of whether such devices are powered off. The new rules also say that removing the battery from a device is not an acceptable practice. Luckily the host knew this, and told Sam to report to SIMP.

Note: BlackBerry rules of use are changing. Look for official communications mid-October.

Go to page 7.

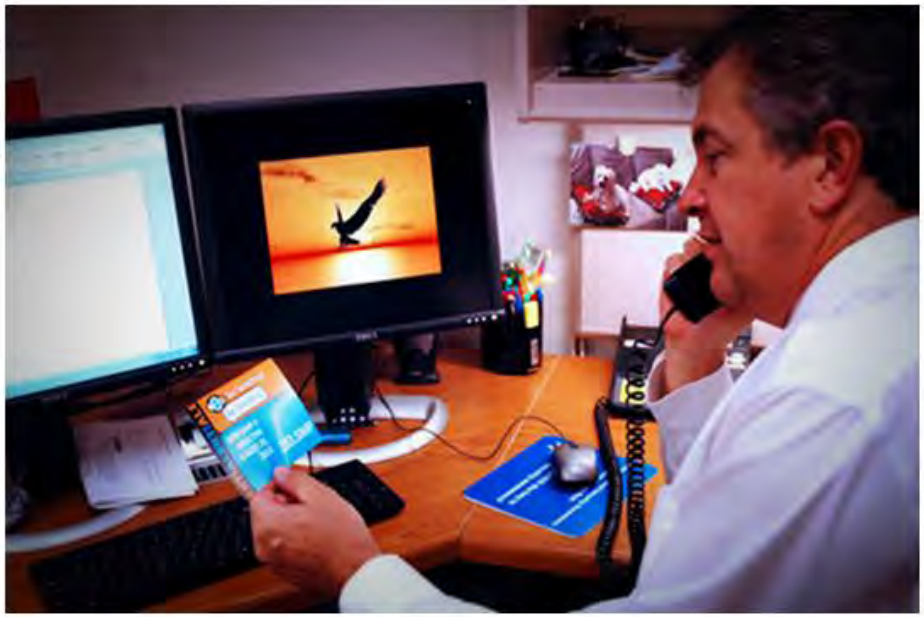
Your Answer:

Remove the BlackBerry from the meeting, and call the Security Incident Management Program (SIMP) after the meeting.

This is Sam's best option...

Even though his BlackBerry was off, Sam still needed to report the incident. All communications devices must be removed from areas where classified processing or classified discussions are taking place, regardless of whether such devices are powered off. The new rules also say that removing the battery from a device is not an acceptable practice.

Note: BlackBerry rules of use are changing. Look for official communications mid-October.



Go to page 7.

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

Summary

MODULE 01: REPORTING MISTAKES

The sooner an inquiry begins, the sooner measures can be taken to mitigate associated risks. In Sam's case, SIMP was able to determine that there had been no compromise of information.

When a meeting has the potential to become classified, the host should inform participants of this fact and remind them to remove their communications devices before the meeting starts. This would have mitigated the issue with Sam and his BlackBerry.

SEC100

Summary

Reporting isn't just a DOE expectation, and it's not about assigning blame. Rather, it's part of Sandia's commitment to secure operations. More importantly, accurate and timely reporting allows us to mitigate potential risks which include:

- Harm to national security
- Loss of America's technological and military superiority
- Damage to Sandia's reputation

Why is time frame important?

Timely reporting is important for several reasons:

- Sandia is obligated to report to DOE within specific time frames.
- The sooner something is reported, the sooner we can take steps to mitigate the situation.
- Reporting allows us to learn from mistakes and help others avoid doing the same thing.

How are incidents and infractions related?

Basically, an incident is the result of not following security requirements, which must be investigated. An infraction is the assignment of responsibility (not blame) for an incident—in other words, it identifies who was responsible for the incident.

Note: In some cases, a security incident may even be a violation of federal law (e.g., release of classified matter, whether intentional or not).

What happens if I get an infraction?

In general, if you are involved in an incident and report in a timely manner, it would not result in adverse consequences, such as the loss of ability to hold a clearance or employment—even if you are assigned an infraction. That said, however, federal law establishes potential consequences for malicious, intentional, or gross security violations, including imprisonment and monetary fines.

Understanding Prohibited and Controlled Articles

Prohibited articles are typically things that can hurt you—things like guns, fireworks, or illegal drugs. They are not allowed on Sandia-controlled premises

Controlled articles are a little more complicated. We typically think of them as "anything that can record or transmit."

All Sandia-owned items that meet the controlled articles criteria (see IM100.1.2, Manage Controlled Electronic Devices and Media) must be registered.

Module 2: Protecting Classified

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 02: PROTECTING CLASSIFIED INFORMATION

After the meeting, Sam goes to see Brad, an important member of his team, to talk about the SSRG project. Brad isn't at his workstation, but Sam notices that his lab notebook is sitting out. The lab notebook has a classified cover sheet, and Sam presumes that the contents of the notebook are classified. The workstation is in the Limited Area.

SEC100

WHAT SHOULD SAM DO?

Leave notebook in office, lock the door, and try to find Brad.

Go to page 12.

Give the lab notebook to Brad's Classified Administrative Specialist (CAS).

Go to page 13.

Your answer:

Leave notebook in office, lock the door, and try to find Brad.

Close, but Sam could have done more...

Shortly after leaving the locked office, Sam found Brad in the hallway. Turns out, he had only been gone for a few minutes. Together they reported the incident to SIMP immediately. Because of the timing, SIMP was able to make the determination that there had been no compromise. However, it would have been a better choice for Sam to keep the notebook with him until he could find Brad or give it to Brad's Classified Administrative Specialist (CAS). Both are better choices for protecting the information.

Go to page 14.

Your Answer

Give the lab notebook to Brad's Classified Administrative Specialist (CAS).

This is Sam's best option.

Susan, Brad's CAS, is familiar with the sensitivities of Brad's project, and is trained to properly protect and store that type of classified information. Therefore, Brad can reasonably presume the notebook will be protected correctly. Together, Sam and Susan reported the incident. Since SIMP was able to determine that Brad had just left for a meeting moments before Sam arrived, they could reasonably assume there had been no compromise.

Go to page 14.

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

Summary

MODULE 02: PROTECTING CLASSIFIED INFORMATION

Just because Brad's lab notebook is related to the SSRG project and Sam has a Q clearance, that doesn't mean he has the appropriate Need to Know (NTK) for this particular information. Sam did the right thing by taking action immediately without examining the notebook.

SEC100

Additional Things to Know

What is classification?

Classification is the act or process by which information or documents or material are determined to require protection in the interest of national security under the Atomic Energy Act, 10 CFR 1045, or Executive Order 13526.

Identify and Protect Classified Information

It's easy to take measures to prevent issues.

- Consult a knowledgeable Derivative Classifier (DC) to have your documents reviewed, even if you only suspect that the documents may contain classified information.
- If you are working in a classified subject area, consult a knowledgeable DC to avoid associating or compiling unclassified information that may result in a classified document.
- If you believe that a document has received an incorrect classification determination, you may challenge the determination. The Classification Offices can help you resolve concerns, or they can consult DOE or NNSA for a formal determination.
- If you have a classified document or material that you believe can be declassified or downgraded, first consult with your DC who will work with a Derivative Declassifier (DD) in the Classification Office to "declassify" or "downgrade" the item. While DCs can derivatively classify or upgrade the classification level of information, only DDs can make determinations to declassify or downgrade classified information.

Avoid Security Incidents

It's also important to understand how to handle situations that involve the unintentional or unauthorized release of classified (or potentially classified) information:

- First, the release of classified, whether intentional or inadvertent, constitutes an incident.
- If you work in a classified subject area, it is your responsibility to be familiar with the associated classification *levels* (which indicate the sensitivity of classified matter) and *categories* (which indicate the types of classified matter) . To understand the sensitivities of the work being done, use the resources available, such as a knowledgeable DC, your manager, the Classification Office, your CAS, and the online Review and Approval Process.
- Accidental or unintentional release of classified information by others (e.g., Wiki Leaks) does not mean that the associated information has been declassified.
- DOE's "No Comment" policy requires that you neither confirm nor deny public statements concerning classified or potentially classified information.

Conducting Classified Meetings

Classified meeting owners are responsible for following applicable procedures, including:

- Announcing the necessary clearance level and NTK at the start of the meeting.
- Verifying that all participants have appropriate clearances and NTK. To verify a clearance prior to meeting, send the name to clearance-nm@sandia.gov.
- Verifying that the appropriate classification level is transmitted to participating (e.g., via videoconference) remote sites, electronically or by using a sign.
- Maintaining door control at all times.
- Terminating all classified conversations before using the phone.

Note: It is no longer acceptable to simply remove the battery from a Blackberry when discussing classified. Ensure you're familiar with the rules of use and other relevant guidance at SNL's Blackberry website.

Video Conferences

- Be knowledgable about video conference requirements. Each classified videoconference room may have a different set of requirements; therefore, it is important that the meeting owner follow all procedures on the Monitor Check Sheet.
- Some videoconference systems at SNL are designed and used to conduct classified videoconferences with networks other than the DOE classified networks. Contact the room owner or the Videoconference Help Desk for both NM and CA (505-845-2000, Option 1) for guidance.

Module 3: OPSEC and Unclassified Controlled Information (UCI)

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 03: OPSEC AND PROTECTING UNCLASSIFIED CONTROLLED INFORMATION (UCI)

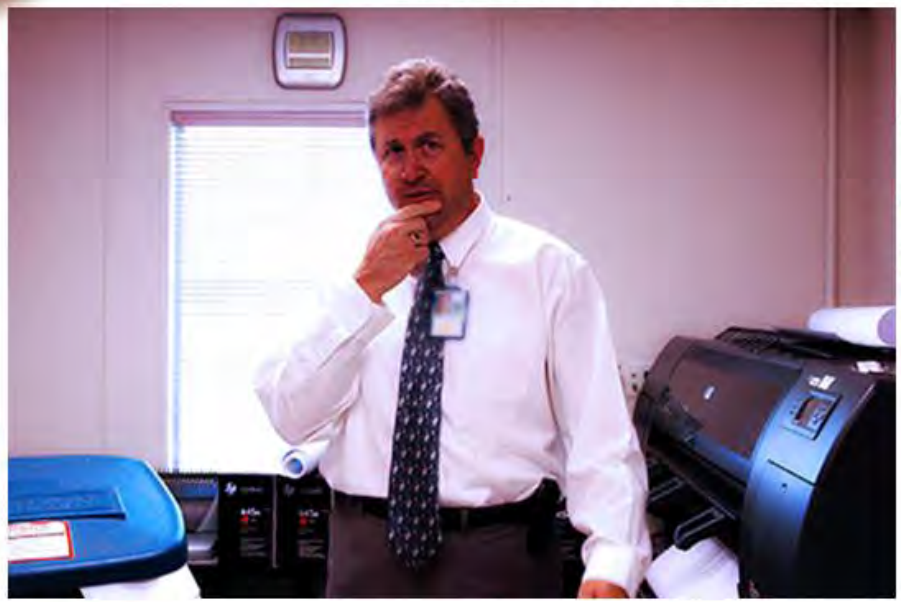
A program similar to the SSRG project just lost some valuable, unclassified information to a competitor, which cost them the contract. Sam thinks that his project might have some of the same vulnerabilities. The SSRG is inside a Limited Area, and everyone in Sam's office area has a Need to Know (NTK) regarding SSRG information. They have an open work environment, and information is frequently left on printers and copiers.

Sam remembers the catchphrase "**THINK. ASSESS. PROTECT.**" and decides to apply it to his workspace.

SEC100

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 03: OPSEC AND PROTECTING UNCLASSIFIED CONTROLLED INFORMATION (UCI)



THINK About the Threat

What does Sam need to protect?

- Information that could cause harm to the nation if lost/compromised.
- Information that could give someone a competitive advantage.

SEC100

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 03: OPSEC AND PROTECTING UNCLASSIFIED CONTROLLED INFORMATION (UCI)

ASSESS the Vulnerabilites

What actions can Sam take to reduce the risks?

- Don't leave information on copiers.
- Keep sensitive information out of recycle bins/trash.
- Don't leave computers unlocked.
- Apply NTK to both information and controlled-access areas.

SEC100

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 03: OPSEC AND PROTECTING UNCLASSIFIED CONTROLLED INFORMATION (UCI)

PROTECT Against Risks

How can Sam mitigate the risks?

- Mark information correctly to help ensure it is easily recognized as needing protection.
- Secure information when not in use.
- Lock doors.
- Check recycle bins periodically for unclassified controlled information (UCI).

SEC100

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

Summary

MODULE 03: OPSEC AND PROTECTING UNCLASSIFIED CONTROLLED INFORMATION (UCI)

The most important thing to consider in all circumstances is the risk of inadvertent release of information. This particular vulnerability is especially difficult because individuals may not even be aware that information has been compromised.

Also, keep this in mind: Even though individual pieces of information may be unclassified, certain elements of that information can be combined to reveal classified information and threaten national security.

SEC100

Additional Things to Know

Operations Security (OPSEC) is a five-step, analytical, information security process that is used primarily to protect mission operations by affording sensible security to information. If you review the OPSEC process, it can seem daunting, but you practice OPSEC in your personal life every day.

Here are two everyday examples:

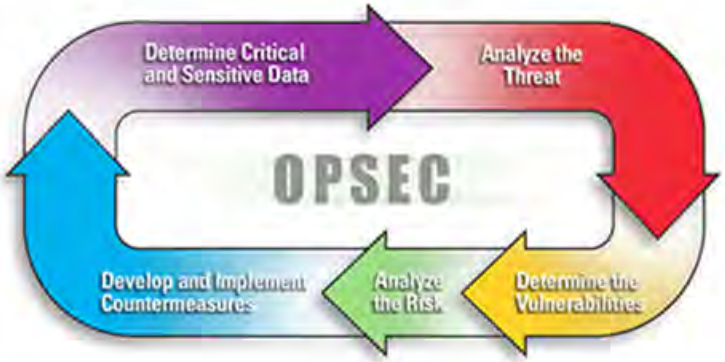
1. When you ***leave for work***, do you check to make sure your doors and windows are locked? Do you make sure the paper is taken in that morning, and do you have lights that are on timers?
2. When you ***go on vacation***, do you leave lights on, have neighbors pick up your mail, or leave a car in the driveway? All of these things provide the appearance of normalcy while you are away on a trip.

Again, these are all protection measures, or mitigations that you put in place because you have:

1. Determined what you need to protect and who you think your biggest threats are.
2. Assessed where you may be vulnerable and determined what risks are present.

The OPSEC Five-Step Process

1. **Determine critical and sensitive data.** *What do you want to protect? What information is critical to your organization? If you don't know what to protect, how do you know you are protecting it?*
2. **Analyze the threat.** *Who wants your information? If you don't know the threat, how do you know what to protect?*
3. **Determine the vulnerabilities.** *How can adversaries get your information? How would you get the information if you were the adversary?*
4. **Analyze the risks.** *What are the consequences of your critical or sensitive information being lost or stolen? Would undesirable attention be drawn to DOE/NNSA or SNL? Could it lead to legal action?*



5. **Implement countermeasures.** *What measures can you take to protect your information? Develop a plan to address identified vulnerabilities.*

Types of unclassified information that must be protected

The preferred term for sensitive unclassified information is Unclassified Controlled Information (UCI), although it is sometimes called Sensitive Unclassified Information (SUI) or Unclassified Protected Information (UPI). There are several different types of UCI, as illustrated in the accompanying diagram. For each type, there are different marking and handling requirements, which are specified in corporate procedure IM100.2.5, *Identify and Protect Unclassified Information*.

Sandia Proprietary and Government-Owned Information

The two primary types of UCI at SNL are Sandia Proprietary (Sandia-owned information) and Government-owned information. Each type has several different designations:

Sandia Proprietary	Government-owned

• Attorney-Client/Attorney Work Product Privileged Information
• Cooperative Research and Development Agreement (CRADA) Information
• Patent
Caution
• Employment-related Records
• Sandia financial information
• License agreement
	• Official Use Only (OUO)
	  ○ Export Controlled Information (ECI)
	  ○ Privacy Act (PA) Information
	  ○ Applied Technology (AT)
	• Naval Nuclear Propulsion Information (U-NNPI)
	• Safeguards Information (SGI)
	• Unclassified Controlled Nuclear Information (UCNI)

*Personally Identifiable Information (PII) *Third Party Proprietary	
**Can fall under either Sandia Proprietary or Government-Owned Information*	

The UCI Flowchart will aid you in identifying the various types of unclassified information with which you may be working.

Unclassified Controlled Nuclear Information (UCNI)

Another type of UCI that is common at SNL is UCNI. This is certain unclassified information about nuclear facilities and nuclear weapons that must be controlled because its unauthorized release could have a significant adverse effect on the national security or public health and safety. UCNI is information in at least one of the following subject areas:

- Design of production or utilization facilities
- Security measures (e.g., security plans, procedures, equipment) for the physical protection of production or utilization facilities or nuclear material
- The design, manufacture, or utilization of nuclear weapons or components that were once classified as Restricted Data, as defined in Section 11y of the Atomic Energy Act

If you believe your information meets the criteria in one of the UCNI subject areas, you must consult an UCNI Reviewing Official (UCNI RO) about the sensitive information with which you are working. Only an UCNI RO can determine, based on guidance, if information actually contains UCNI.

Module 4: Badges

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 04: BADGES

Sam returns from a long lunch at home, only to discover that he doesn't have his badge (actually, his HSPD-12 federal credential). Since he lives several miles away, it will take even more time away from work to go back for the badge.

SEC100

WHAT SHOULD SAM DO?

Go to the Badge Office (SNL/NM) or Visitor Control (SNL/CA) and report the "forgotten" badge.

Go to page 28.

Go home and retrieve the badge.

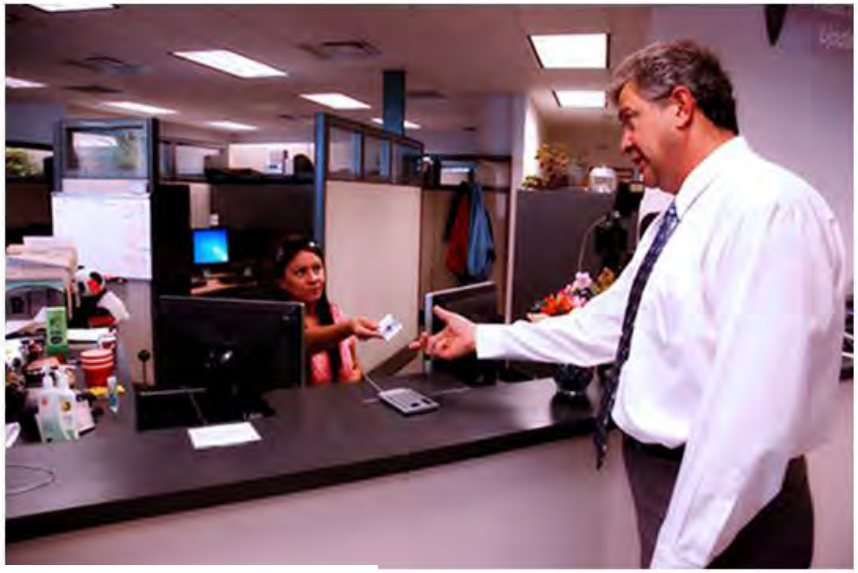
Go to page 29.

Your Answer:

Go to the Badge Office (SNL/NM) or Visitor Control (SNL/CA) and report the "forgotten" badge.

Close, but Sam should think twice...

The Badge Office will issue Sam a Local Site-Specific Only (LSSO) badge that he can use for the day. However, this will initiate an escalation process that includes notification to Sam's manager, followed by a discussion with his manager about proper handling and protection of badges. And, if Sam forgets his badge again, or it is stolen or lost within 365 days, the escalation process will involve higher levels of management and more counseling. Sam's best course of action is to go home and retrieve his badge.



Go to page 30.

Your Answer:

Go home and retrieve the badge.

This is Sam's best option...

If he had reported the "forgotten" badge to the Badge Office, he would have been issued a temporary Local Site-Specific Only (LSSO) badge. The same would occur if the badge had been lost or stolen. Sam's lucky.

Note: The Badge Office allows a one-time exemption per 365-day period for a lost, stolen, or forgotten badge before an escalation process begins. That process would involve notification to Sam's manager, followed by a discussion with his manager about proper handling and protection of badges. If there are more occurrences of a lost, stolen, or forgotten badge, the escalation process would then involve higher levels of management and more counseling

Go to page 30.

close

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

Summary

MODULE 04: BADGES

Badges need to be treated with the same care that you treat the keys to your home: there's valuable information to be protected. You are responsible for protecting your badge as government property. Failure to do so may result in disciplinary action and other consequences, beyond the escalation process mentioned in the preceding scenario.

Because badges are government property, failure to return them may result in the initiation of a federal investigation for theft.

SEC100

Additional Things to Know

Your Badge-Related Responsibilities

- When on Sandia-controlled premises, wear your badge conspicuously, photo side out, in a location above the waist and on the front of your body.

  Note:

  - During construction activities in which the badge may compromise safety, the badge may be worn in an armband badge holder.
  - During operations where it is not prudent to display your badge, it is acceptable to remove and/or cover the badge as needed to protect the safety of personnel/equipment and protect the badge from damage. However, badges must be readily accessible in the immediate area and produced upon challenge.
- Maintain your badge in good condition.
- If your facial appearance changes significantly, request a new badge with a new photo from the appropriate Badge Office.
- Obtain a new badge when wear and tear (e.g., from repeated swipes at entry control points) causes any part of the photo or writing to become obscured.
- Remove your badge when wearing it is not required (e.g., when offsite).
- Do **not** use your badge as a means of identification for unofficial purposes (e.g., cashing checks).
- Do **not** allow your badge to be photocopied, reproduced, or photographed at close range.
- Do **not** leave your badge unattended in a non-secure environment (e.g., within a non-secure building or vehicle.)

  Note: Leaving your badge in a locked secure area is acceptable and does not violate the requirement to protect your badge. A locked home or a locked vehicle provides acceptable protection if your badge is not in plain view.

- Protect your PIN as follows:
  - Do **not** share your PIN.
  - Keep your PIN in a locked drawer or office.
  - If compromised, change your PIN.
- Surrender your badge for destruction when any of the following circumstances occur:
  - Badge is no longer valid.
  - Badge is no longer required.
  - Upon request by a supervisor or security official (e.g., Protective Force personnel).

Module 5: Interacting with Foreign Nationals

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 05: INTERACTING WITH FOREIGN NATIONALS

The SSRG project involves Cooperative Research and Development Agreements (CRADAs), which will necessitate frequent interaction with Foreign Nationals (FNs). One of those FNs, Wesley, has just arrived to work on a 3-month assignment at SNL. His regular escort, Linda, has to go to a meeting and, because they're in the Limited Area, she needs to transfer escort responsibilities to Sam.

SEC100

WHAT SHOULD SAM DO?

Accept responsibility. Sam has escorted plenty of uncleared personnel, and he himself was escorted for several months when he first came to SNL.

Go to page 34.

Decline to do so.

Go to page 35.

Your Answer:

Accept responsibility. Sam has escorted plenty of uncleared personnel, and he himself was escorted for several months when he first came to SNL.

Sam almost got in hot water...

Luckily for Sam, a coworker who met all of these criteria saw the exchange and stepped in. Otherwise, Sam would be making another phone call.

Sam forgot that the general escorting responsibilities do not fully address this escorting issue. There are significant additional rules associated with escorting FNs. He should have consulted ISS100.4.1, *Control Access by Foreign Nationals to Unclassified DOE Information, Programs, and Technologies, and SNL Sites*. If he had, he would know that he must be listed as an escort on the Foreign National Request Security Plan (FNR SP) and be aware of exactly what areas/facilities Wesley is allowed to visit.

Plus, Sam can only accept the responsibility if he:

- Is a U.S. citizen.
- Has a DOE-approved badge.
- Is a Sandia employee, contractor, or SSO employee.
- Has the appropriate clearance for the areas into which he will escort Wesley.
- Has completed FCPA100, *Foreign Corrupt Practices Act Training*, and EC100, *Export Control Awareness Training*.

Go to page 36.

Your Answer:

Decline to do so.

This is Sam's best option...

Luckily, Sam knew that there are special rules for escorting FNs. Sam is familiar with ISS100.4.1, *Control Access by Foreign Nationals to Unclassified DOE Information, Programs, and Technologies, and SNL Sites*, which says that he must be listed as an escort on the Foreign National Request Security Plan (FNR SP) and be aware of exactly what areas/facilities Wesley is allowed to visit.

Plus, Sam can only accept the responsibility if he:

- Is a U.S. citizen.
- Has a DOE-approved badge.
- Is a Sandia employee, contractor, or SSO employee.
- Has the appropriate clearance for the areas into which he will escort Wesley.
- Has completed FCPA100, *Foreign Corrupt Practices Act Training*, and EC100, *Export Control Awareness Training*.

Go to page 36.

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 05: INTERACTING WITH FOREIGN NATIONALS

Summary

Don't assume that you're required to escort—you may always decline to engage in any security-related activity if you're not sure you're knowledgeable enough to do so...or even if you just feel uncomfortable with the idea.

SEC100

Additional Things to Know

Working With a Foreign National

Special rules apply when escorting FNs, especially regarding areas they may visit. Some of these were addressed in the preceding scenario, but they bear repeating:

- FNs must have an approved FNR SP.
- All hosts and escorts must be listed on the FNR SP.
- FNs are allowed only in the areas listed on the FNR SP.

If you will be working directly with FNs, even cleared FNs, there are special rules for that type of interaction. Review the applicable corporate procedures (see sidebar) and consult your manager to ensure that you know all pertinent requirements.

Other Foreign Interactions

Among the other unique responsibilities you incur when interacting with FNs, the following reporting requirements apply (your complete responsibilities are addressed in the various corporate procedures and other resources cited in the sidebar).

Report any time you:

- Publish with an FN.
- Receive an unsolicited email or phone call from an FN.
- Suspect you are being assessed or targeted by an FN.
- Suspect unauthorized loss of information to which an FN may have access.
- Have substantive contact with **any** FN.

  Note: "Substantive contact" refers to a personal or professional relationship that is enduring and involves substantial sharing of personal information and/or the formation of emotional bonds (does not include family members).

- Are employed by, represent, or have other business-related associations with a foreign or foreign-owned interest or FN.
- Have an immediate family member who assumes residence in a sensitive country.

See the DOE and Sandia Reporting Requirements pamphlet for contact information.

You must also report certain foreign travel (per criteria specified in the DOE and Sandia Reporting Requirements pamphlet). And, if you will be taking Sandia cyber resources with you (effectively "handcarrying" them), you must comply with the requirements of the Laptops on Foreign Travel (LOFT) program.

And don't forget about exports, which may even be an issue with your foreign travel. Export Control involves foreign interactions, and carries with it a wholly unique set of requirements, including special training. Be sure to review ISS100.4.3, *Comply With Export/Import Controls*, and consult the Export/Import Control Office (EICO).

Note: For a thorough understanding of Export Control, see EC100, *Export Control Awareness Training*

Module 6: Personal Reporting Responsibilities

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 06: PERSONAL REPORTING RESPONSIBILITIES

Sam has had a challenging day. He is comforted that he did the right things necessary to ensure secure operations. Regardless, he's glad the day is done, and he's looking forward to seeing his girlfriend Ana at dinner.

As Sam walks into the restaurant, he spots Ana sitting with a man he doesn't recognize. She introduces him as "an old friend." As the evening goes on, Ana's *friend* becomes very interested in Sam's work, and starts asking Sam very detailed and pointed questions about the classified SSRG project. Sam gets a little nervous being around Ana's inquisitive friend, so he offers to take Ana home.

During the drive home, Sam is so distracted, he speeds right through a red light—and immediately is pulled over. The police officer checks his computer and discovers that there is a Samson Seriously who is wanted for several crimes. Sam assures the officer that the wanted criminal isn't him. Despite his pleas of innocence, the officer places him in the back of the cruiser while he investigates. Turns out, our Sam isn't the criminal they wanted. In the end, Sam is released with only a $360 traffic ticket.

DOES SAM HAVE ANYTHING TO REPORT?

Select the three that apply to Sam. Upon doing so, the "Next" button will allow you to proceed.

- ☐ Approached by an individual seeking access to classified
- ☐ Foreign travel
- ☐ Detained by law enforcement
- ☐ Traffic fine over $300
- ☐ Hospitalized for mental illness
- ☐ Family member living in a sensitive country

SEC100 ANNUAL SECURITY REFRESHER BRIEFING

MODULE 06: PERSONAL REPORTING RESPONSIBILITIES

Closing Summary

All of the things cited on the preceding list are reportable, and you have successfully identified those that apply to Sam's unfortunate circumstances. Of course there are many other types of reportable events, including "incidents of security concern" (aka: security incidents); waste, fraud, and abuse; theft of government property; drug use; etc. A complete set of reporting responsibilities is included in the DOE and Sandia Reporting Requirements pamphlet, along with details about when and to whom you must report.

In addition to reporting personal issues, you are obligated to report anything you see that may be a violation of security requirements (not just incidents). Keep this particular point in mind: If you fail to report something you see, you aren't just ignoring a security violation, you yourself are violating a requirement. The ultimate goal is simple—we need to help each other maintain secure operations. This is a key aspect of Operations Security (OPSEC), often expressed as... ***See something? Say something!***

Answer: Approached by an individual seeking access to classified; Detained by law enforcement; Traffic fine over $300

SEC100

General Reporting Requirements

As a reminder, here is a complete list of "Concerns of Personnel Security Interest," all of which are reportable within specific time frames (see the DOE and Sandia Reporting Requirements pamphlet for details, and to learn which organizations you must report to).

Report immediately if you are:

- Approached or contacted by ANY individual seeking unauthorized access to classified matter or special nuclear material (SNM).
- Aware of information about other Members of the Workforce that raises concerns of personnel security interest.

Legal Issues

Report orally within 2 work days of occurrence and also in writing within the next 3 work days if you:

- Are arrested, subject to criminal charges (including charges that are dismissed), or are detained by federal, state, or other law-enforcement authorities for violations of the law within or outside of the U.S. Traffic fines of less than $300 do not have to be reported, unless the violation was drug or alcohol related.
- File for bankruptcy, regardless of whether it is for personal or business-related reasons.
- Have your wages garnisheed for ANY reason (e.g., divorce, debts, child support).

Citizenship

Report within 2 work days of occurrence and in writing within the next 3 work days if you:

- Are a current U.S. citizen who changes citizenship or are acquiring dual citizenship.
- Are a foreign citizen who changes citizenship.

Life Circumstances

Report if you:

- Have a name change (time frame: orally within 2 work days of occurrence, and in writing within the next 3 work days).
- Marry or cohabitate with a person in a spouse-like relationship (time frame: in writing within 45 days).
- Are hospitalized for mental illness, or are treated for drug or alcohol abuse (time frame: orally within 2 work days of occurrence, and in writing within the next 3 work days).
- No longer require your clearance, terminate your employment, are on extended leave of 90 calendar days or longer, or your access authorization is no longer required for 90 calendar days or longer (time frame: immediately).

Foreign Travel

Report prior to travel (except where otherwise stated) if you:

- Have business-related travel to a sensitive or non-sensitive country (time frame: 37 days prior to travel).
- Have personal foreign travel to sensitive country.
- Hold a Special Access Program (SAP) clearance and:
    - Travel for personal reasons to a sensitive foreign country, or
    - Travel for business to any foreign country, sensitive or non-sensitive.
- Hold a Sensitive Compartmented Information (SCI) clearance and travel to any foreign country (sensitive or non-sensitive) for personal or business reasons.

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

SEC100 Completion Record

After reading all the modules of SEC100, complete this form and send it via email to securityed@sandia.gov or via fax to 505-844-7802 to receive course credit.

I have read and understand all the modules in SEC100, *Annual Security Refresher Briefing*.

Print Full Name (Last, First, Middle):				
SNL Org # or Company Name:				
☐ Employee	☐ Contractor	☐ Consultant	☐ Student	☐ KMP
Signature:				Date:

If you would like confirmation of completion, provide your email or fax number (please write legibly).

_____

SEC100 Feedback Form

Your feedback is important to us. Please complete this evaluation and send it to us via email at securityed@sandia.gov or via fax at 505-844-7802.

Rate the following on a scale of 1 to 5, with 1 = poor and 5 – excellent.

The ease of use of this learning.	1	2	3	4	5
The organization of the 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.	1	2	3	4	5
Your level of knowledge related to this topic AFTER using this learning tool.	1	2	3	4	5

Fill in the blanks.

What was the most valuable about this learning tool?

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

What could be done to improve or enhance this learning too?