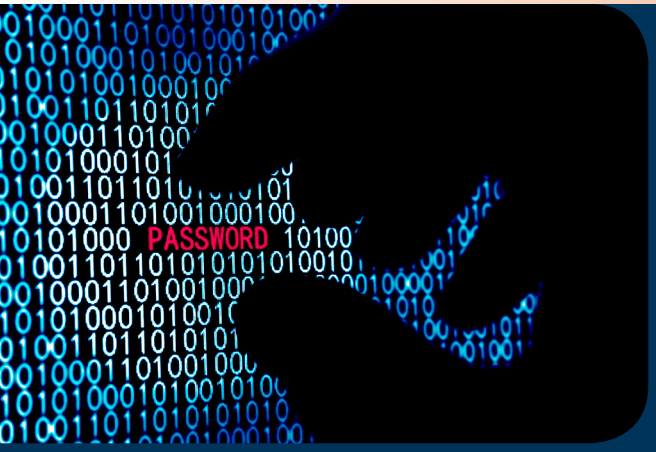
SEC150

Comprehensive Security Briefing



Exceptional service in the national interest

Sandia National Laboratories

>> security.sandia.gov

11/2011

Sandia National Laboratories

SEC150

Comprehensive Security Briefing

CONTENTS

CONTENTS (continued)

Overview & Background

SNL's resume highlights:

Radar
Super-computers
Clean rooms
Proximity fuses
Nuclear weapons

Federal Government

↓

Department of Energy (DOE)

↓

National Nuclear Security Administration (NNSA)

↓

Sandia National Laboratories (SNL)

↓

You

We Are a National Security Laboratory

Sandia is one of 21 DOE National Laboratories, part of the world's most advanced research network dedicated to weapons and energy work.

Our work has been crucial to America's success since 1949.

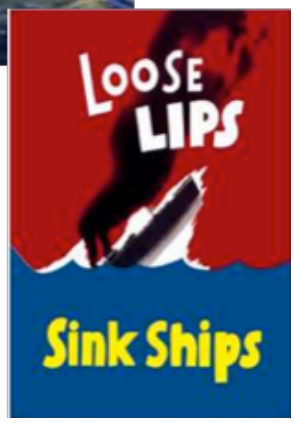
We are currently pioneering even more technological advances. The work we do here today will have an effect on our future; thus, other countries and companies are very interested in what we are doing.

Where Do You Fit In?

You are part of a large organization that has been entrusted to do very important work for the U.S. government. The American people have entrusted us to protect classified matter, including information about nuclear, chemical, and biological research, and other controlled information.

Security Threats Are REAL…

And so are the risks



Threats

- Adversaries
  People and governments want the information we have.
  - ◊ Insiders—Clandestine intelligence gathering is a reality. Also, some workers are willing to share information for various reasons (money, recognition, ideology, etc.).
  - ◊ External operatives—Espionage is an ever-present reality, whether conducted by foreign governments or industrial spies.
- Inadvertent disclosure
  Information can be compromised due to human error.
  - ◊ Carelessness is as big a threat as spies.
  - ◊ Changes in routine can lead to mistakes.
  - ◊ Failure to recognize vulnerabilities can result in lost information.
  - ◊ Ignoring established controls can create opportunities for adversaries.

Risks

- Harm to national security
- Loss of America's technological and military superiority
- Damage to Sandia's reputation
- Loss of Sandia's contracts
- Termination
- Fines and/or imprisonment

Some Sobering Facts

Did you know that New Mexico is a hot spot for spies? Counterintelligence expert Bruce Held says: "For many international intelligence operatives, the state's name is nearly synonymous with espionage."

Silicon Valley in California is also a hotbed for espionage. According to the FBI, Silicon Valley is home to many of the estimated 3,000 front companies nationwide that have been set up by foreign countries to steal secrets and acquire technology.

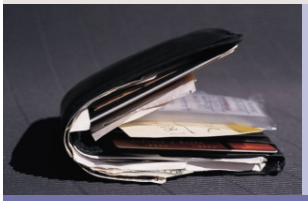
Did you know that New Mexico is a hot spot for spies?

You Already Understand and Practice Security

At home, you know the risks…and the consequences. We need you to be as diligent at work as you are at home.

You leave for work and can't recall if you closed the garage…so you go back and check.

Yet we have situations where people suspected they left a safe open, but went home anyway.



You lock the doors of your car…automatically.

But we have a high number of situations where people left a classified network open and unlocked.

You test the front door after you lock it to ensure that it is, indeed, locked.

Yet many safes that were thought to be closed are found open because people didn't test the lock.

You keep your wallet in a safe place.

But we've found passwords taped to the back of monitors and under keyboards.

You must need the information to do your work…a concept known as NTK.

Need to Know (NTK)

Your clearance is your access authorization, but it does not give you permission to access all information. You must need the information to do your work…a concept known as NTK.

> *You don't have the right to pick something up off of someone else's desk just because you have a clearance. You must have NTK to view any classified or unclassified controlled information (UCI).*
>
> *Likewise, the people with whom you share information must have NTK. Just because a coworker has a clearance doesn't mean we/she needs access to the information with which you have been entrusted.*

Seemingly insignificant bits of information can be combined to build a bigger picture.

Information Must Be Protected

This applies to both classified and unclassified. Seemingly insignificant bits of information can be combined to build a bigger picture.

Would you…

Share your address with a stranger?

Give a coworker your credit card number?

Reveal your Social Security Number?

None of this information is classified, but think of the damage that can be done when this information is combined.

Use Operations Security (OPSEC)

- **Think.** Recognize and acknowledge that you are at risk.
- **Assess.** Evaluate your routines and your environment. Where are you vulnerable?
- **Protect.** Adopt security measures and work controls, and make security a part of everything you do.

How it Works

This morning, I thought about the actions I took when leaving the house and wondered, "Did I close the garage door?" I assessed the risk: "Do I want my house vulnerable all day?" I decided that the risk was not acceptable, so I went back to make sure the garage was closed. That was my protective measure.

About That Badge

Think of your badge as your key. You use your key to get into your house or your car. At SNL, your badge is the key you use to get into work. You need to protect your badge like you protect your house or car keys.

Homeland Security Presidential Directive 12 (HSPD-12)

HSPD-12 established a federal credential, which is now the most common form of identification at SNL. However, unlike DOE-issued credentials, other federal agencies don't specify clearance levels on the credentials they issue. If you don't recognize the person or the badge, play it safe and don't let them in.

If you don't recognize the person or the badge, play it safe and don't let them in.

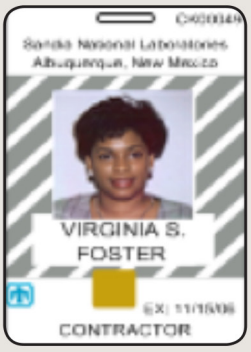
Local Site-specific Only (LSSO) Badges

As the name implies, LSSO badges are used only at specific sites. At SNL, they are required if you don't have an HSPD-12 credential.

Q-Cleared

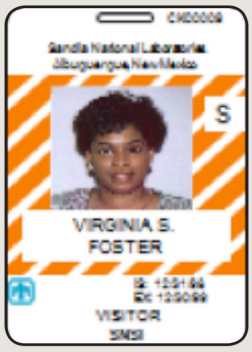
L-Cleared

Uncleared



Top Secret

Secret



Foreign National

With your badge comes certain responsibilities.

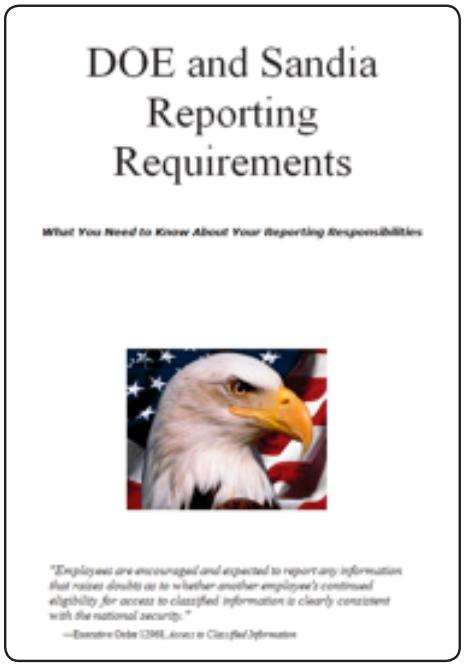
Badge Responsibilities

With your badge come certain responsibilities. It is important for you to know these responsibilities:

- **Don't:**
  - ◊ Wear your badge offsite
  - ◊ Use it for personal identification
  - ◊ Allow it to be photocopied
- **Wear it:**
  - ◊ Above your waist
  - ◊ Over any outerwear
- **Renew if:**
  - ◊ It becomes faded or damaged
  - ◊ Your physical appearance significantly changes
  - ◊ Your name changes
- **Report if:**
  - ◊ Lost
  - ◊ Stolen
- **Return if:**
  - ◊ You take an extended leave of absence (90 consecutive calendar days or longer)
  - ◊ Your clearance is no longer required
  - ◊ You separate from SNL
  - ◊ Your badge expires

Makes sense doesn't it? You'd want your house key back if your house sitter no longer needed access to your home.

Additional Security-related reporting requirements are addressed in the DOE and Sandia Reporting Requirements pamphlet, which is available online or by contacting Corporate Investigations.


DOE and Sandia Reporting Requirements

What You Need to Know About Your Reporting Responsibilities

"Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security."

Maintaining Your Clearance

As previously discussed, your badge provides evidence of your identity and can be thought of as your key to SNL. However, your clearance is actually your access authorization. With this in mind, it's important to know that:

- Being granted a clearance does not guarantee you will remain cleared or retain employment forever.
- You can lose your clearance and may be terminated for:
  - Theft of government property
  - Careless handling of, failure to protect, or disclosure of classified matter
  - Habitual use of alcohol without rehabilitation or reformation
  - Use of illegal drugs, or legal drugs without a prescription
  - Gross misconduct

Because of the significant trust bestowed upon you when you're granted a clearance, there are consequences associated with certain security violations, including:

- Civil penalties of $10,000 to $250,000
- Criminal penalties of 10 years to life in prison

Report anything the U.S. government believes could call into question your trustworthiness or integrity. (The reporting pamphlet cited above provides examples of such issues.)

Keep this in mind: Corporate Investigators know that mistakes happen, and bad things happen to good people.

- Don't give them a reason to question you.
- Don't try to hide anything—it will come out during an investigation.

You can't be coerced or blackmailed if you don't have anything to hide.

With regard to alcohol, a good rule of thumb is to determine if it is affecting your (or a coworker's) performance. If the answer is yes, seek help or report it.

Drinking a glass of wine every night with dinner is not an issue. Drinking shots of vodka before coming to work is—it shows poor judgment.

Report Waste, Fraud, and Abuse

You must report to Corporate Investigations if you suspect that someone is committing waste, fraud, or abuse.

Examples

Waste: Ordering 10 replacement parts for a piece of equipment that will never be used, just to spend year-end funds

Fraud: Submitting an expense report that contains false information

Abuse: Using a Sandia computer, printer, or telephone for outside employment

Fraud: Coming to work late, taking long lunches, and leaving early, but recording full shifts on your time sheet

Abuse: Using a government vehicle to deliver Avon products around the Labs

Each of the above examples is clearly just a wrong behavior; it's not important which type of wrong-doing it is. The important thing is to not engage in such activities and to report anyone who does.

Security Areas

Each security area has different requirements for what you can or cannot bring in.

SNL has many different types of security areas, as shown in the following chart. Each security area has different requirements for what you can or cannot bring in.

General Access Area		Property Protection Area (PPA)	Limited Area (LA)	Closed Area
Public	**Non-Public**			
Badges are **not** required.	Badges are required.	Badge swipe typically required, no PIN.	Badge swipe and PIN typically required.	Badge swipe and PIN required.
Clearance **not** required.	Clearance **not** required.	Clearance typically **not** required for access.	Clearance typically required, or must be under escort.	Clearance typically required.
No classified processing.	**No** classified processing.	Potential to encounter classified.	Classified processing/ handling.	Classified processing/ handling.

You may also hear the phrase "technical area" or "tech area." This describes certain geographic boundaries. Tech areas are not a type of security area.

Prohibited & Controlled Articles

Examples of ….	
Prohibited Items	**Controlled Items**
Explosives	Recording equipment
Dangerous weapons	Cell phones
Alcohol	iPods/iPads
Controlled Substances*	Cameras

*For prescription drugs, you must be able to produce a doctor's prescription under your name. Certain prescribed drugs, such as medicinal marijuana, are not allowed on federal property (DOE, SNL, etc.) even in states where they are otherwise legal.

- Prohibited articles are things that can harm you or are illegal. Although certain programs at SNL are approved to work with prohibited articles, personally owned examples are not allowed anywhere on Sandia-controlled premises.
- Controlled articles are typically "gadgets" that can record, store, or transmit data and, thus, are capable of compromising information. These items are not allowed at in limited or more restricted areas without prior approval. If you have questions about a certain item (e.g., a bicycle pedometer, medical device)…ask! You are responsible for knowing what your gadgets do.

You are responsible for knowing what your gadgets do.

Escorting

- To be an escort, you must:
  - ◊ Have appropriate access authorization (Q or L clearance).
  - ◊ Possess a DOE-approved badge.
  - ◊ Be a U.S. citizen.
- When escorting uncleared individuals, you must:
  - ◊ Take measures in advance to prevent compromise of sensitive information, especially classified.
  - ◊ Escort no more than eight uncleared individuals at a time.
  - ◊ Observe all requirements of spaces visited.
  - ◊ Explain safety and security requirements for the area being visited.

Upon transfer of escorting duty, ensure that the new escort accepts responsibility.

Note: *SNL/CA has additional, site-specific escorting requirements. Thus, Members of the Workforce at that site should contact Security Awareness or Visitor Control to ensure they are aware of their responsibilities.*

- When escorting Foreign Nationals, you must:
  - ◊ Follow special rules set up for Foreign Nationals, especially regarding areas they may visit.
  - ◊ See your manager for guidance.

Vouching

If you use your badge to allow another individual access to SNL, you accept responsibility for that individual. At a minimum, you are expected to perform a basic badge check and verify that no prohibited or unauthorized controlled articles are being brought in. Ultimately, however, you are responsible for any consequences associated with allowing access by other individuals.

YOU are responsible for any consequences associated with allowing access by other individuals.

Special Nuclear Material

Special Nuclear Material (SNM) is fissionable material that releases energy when its atoms split. SNL is authorized to have Category (CAT) III and CAT IV SNM. Safeguards required to protect SNM depend on its category (quantity of material) and its attractiveness (I, II, III, IV), both of which relate to the ease with which it can be turned into a weapon.

Because SNM requires additional protections, you'll receive specific training before working with it.

What is Classified Matter?

Matter is a general term used to describe documents, information, or material. Typically, classified matter is information on weapons or cutting-edge technology. It is ***compartmented*** to prevent damaging loss to national security, which ensures that no one has more information than he/she needs. This is why, if you work with classified, you will only see a limited amount of what is out there.

It is compartmented to prevent damaging loss to national security, which ensures that no one has more information than he/she needs.

Classification Levels & Categories

Levels indicate the sensitivity of classified matter.

Damage is based on the level of sensitivity and indicates possible consequences to national security.

Categories specify the type of classified matter.

Level	Damage to U.S.
Top Secret (TS)	Exceptionally Grave
Secret (S)	Serious Damage
Confidential (C)	Undue Risk

When in doubt, consult your manager!

Criteria for Access to Classified

- You must have the appropriate clearance.
- You must have signed DOE Standard Form (SF) 312, *Non-disclosure Agreement*.
- You must have NTK.

Level	Category		
	Restricted Data (RD)	Formerly Restricted Data (FRD)	National Security Information (NSI)
Top Secret (TS)	Q Only	Q Only	Q Only
Secret (S)	Q Only	Q or L	Q or L
Confidential (C)	Q or L	Q or L	Q or L

Classification Help

A Derivative Classifier (DC) determines whether documents and material are classified, and at what level and category.

Classified Administrative Specialists (CASs) are trained to mark, store, duplicate, destroy, and mail classified matter.

Derivative Declassifiers (members of the Classification Office staff) are the only individuals authorized to declassify classified matter.

Identifying Classified Matter

Classified is not just documents. That's why we refer to it as "matter." You are obligated to protect it in all its forms.

Classified comes in many forms: it could be a paper document, a computer disk, or a piece of hardware. It could also be a thumb drive that contains classified information, an e-mail, or a laboratory notebook. You could even have a classified conversation.

Classified matter must be protected. The higher the risk, the higher the classification. Therefore, all classified matter must be protected to the highest level and category.

It must be processed:

- In Limited Areas or more restricted areas
- Using computers on the Sandia Classified Network (SCN) or on an approved stand-alone system
- Using secure forms of telecommunication and other electronic transmissions

Minimum marking requirements include one level and one category per item, and any caveats that may be applicable. Documents should be marked on the top, bottom, front, and back, and must have cover and backing sheets. Material may be tagged, labeled, or stored in a marked container.

Compilation

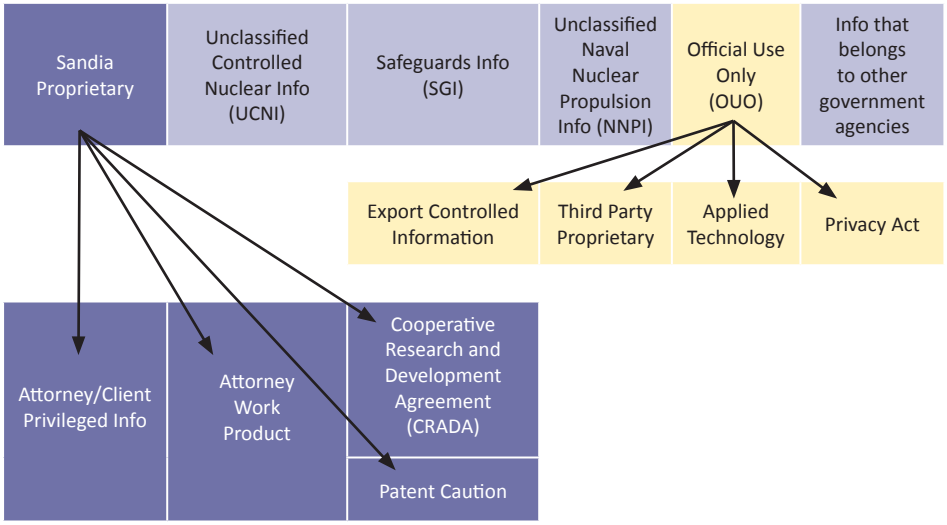
Combining unclassified information can create classified matter. E-mail can be particularly problematic. As replies are forwarded, in which new information is added, a seemingly unclassified e-mail can suddenly become classified. Be aware of all information in e-mail strings.

Always protect information at the highest level and category until you get a DC review. Find a DC in your subject area at the Sandia Security website. You can always challenge a DC determination if you think the determination is incorrect. Contact the ***Classification Office*** for more information.

Always protect information at the highest level and catagory until you get a DC review.

Unclassified Controlled Information

There are several different types of UCI, as illustrated below. For each type of UCI, there are different marking and handling requirements. More information can be found at the ***Sandia Security*** website.



Official Use Only

Information is considered OUO if it could damage government, commercial, or private interests if released into the wrong hands. More to the point, if the information has the potential to cause damage, or it falls under one of the OUO exemptions, then it's OUO. Always evaluate information:

- At the original draft stage
- After each revision
- Before distributing
- Before disposing

If the information has the potential to cause damage, or it falls under one of the OUO exemptions, then it's OUO.

Review and Approval (R&A) Process

Any information that will be released to the public must go through formal review and approval R&A. See the online R&A website for more information or to initiate the process.

DOE's No Comment Policy

If asked about classified or sensitive-unclassified information:

- State only, "No comment."
- Do not confirm or deny anything.
- Refer all inquiries to Media Relations.

Accidental or unauthorized release of classified information does not eliminate the need to continue protecting it as classified.

When an incident occurs

- *Report immediately or have someone report on your behalf.*
- *Don't discuss details over the phone.*

Security Incidents

What Is The Security Incident Management Program (SIMP)?

SIMP conducts inquiries into potential security incidents. Their role is to collect facts; their goal is to mitigate the incident and prevent recurrence, not to punish.

If you suspect you have caused an incident or witnessed one, you must report to SIMP. An inquiry will determine whether an incident has actually occurred.

What Is a Security Incident?

Releasing classified matter is a violation of law, whether it was intentional or not. Examples include:

- Potential release of classified information
- Classified e-mail sent unencrypted outside the firewall, even if the recipient has the appropriate clearance and NTK
- Cell phone brought into a classified meeting
- Classified matter that is taken home

What Is an Infraction?

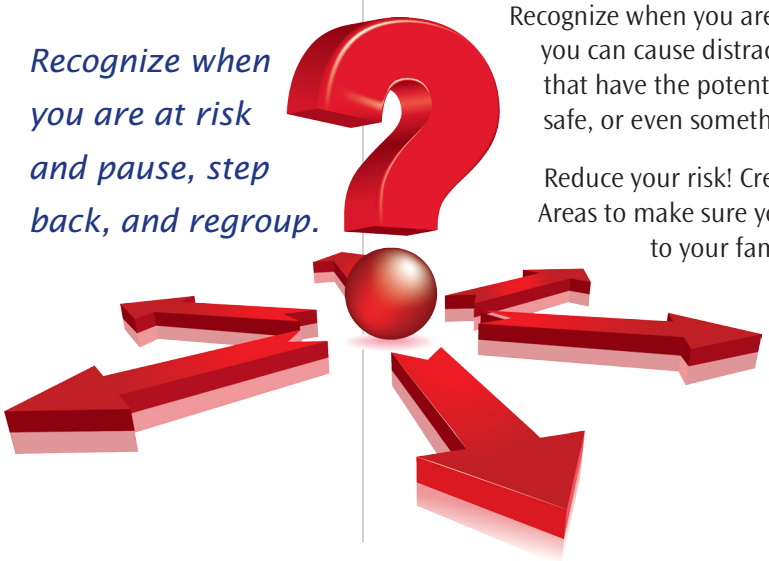
"Incidents" don't always result in "infractions."

An infraction merely assigns responsibility for an incident. Basically, an infraction means that the responsible party failed to follow a security requirement, and corrective actions may be needed.

Security incidents are mostly caused by:

- Being careless, making assumptions, or becoming over-confident
- Distractions and interruptions
- Changes in routine
- Time pressures
- Misperception of risk

Recognize when you are at risk and pause, step back, and regroup.



Recognize when you are at risk and pause, step back, and regroup. And be aware that you can cause distractions. Don't interrupt others while they're performing tasks that have the potential for a high rate of error, such as securing a closed area or safe, or even something as simple as entering a Limited Area.

Reduce your risk! Create a routine. Perform a self-check prior to entering Limited Areas to make sure you don't have unauthorized controlled articles with you. Talk to your family about Sandia's security rules so they don't inadvertently cause you to have an incident. An example of how this can happen: Your spouse tries to surprise you with a new electronic gadget as a birthday present, putting it into your briefcase so that you'll find it when you get to work.

Espionage & Indicators

Did You Know

- One third of people passing information have no clearance. This means that people who didn't have access to classified still found valuable information to share, such as travel itineraries, fields of research, etc.
- More than twice as many people volunteer to be a spy than are recruited. People want money, recognition, and fame. There are all kinds of reasons they might volunteer to pass information.
- Today's agents are professors, engineers, and businessmen. They're criminal capitalists who see only dollar signs.
- Spies don't just work for governments; some work for private enterprise. Basically, it's not spies like you see in the movies. These are regular folks, average Joes. You cannot determine who's a threat based on nationality, appearance, etc.
- Two-thirds of adversaries used social media to establish contact with an insider. Be careful of what you put out there, and be careful talking to strangers. Be aware that other people may be posting information about YOU! Cancelling your accounts doesn't make the information go away.

This Is Espionage Today

Potential targets of foreign intelligence services are:

- People with a clearance
- People who have access to someone with a clearance
- Any type of media that might contain useful information

Foreign Intelligence Service Tactics to Target YOU

- Targeting electronic media (e.g., computers, social networks)
- Eliciting during conferences/trade fairs
- Intellectual property theft through research sponsorship in the U.S.
- Targeting ethnic communities for recruitment
- Routine debriefing of foreign visitors to the U.S.
- Tasking employees of U.S. firms
- Tasking foreign students at U.S. universities
- Sexpionage
- Requiring violence as a religious duty
- Blackmail

Over 80% of information collected about SNL is from open sources. You can learn a lot from information that has been posted on the web.

You may not realize you've been targeted—this is why there are special reporting requirements associated with foreign interactions.

Be careful: *the internet provides a sense of anonymity and a false sense of security.*

Be Vigilant

- Increased use of computers makes us vulnerable. Hackers and cyber criminals target our electronic media for information or other actions, such as a denial of service attack. Be careful: the internet provides a sense of anonymity and a false sense of security.

Protect Yourself

- Don't place sensitive information on social networks.
- Don't provide unnecessary details about you or your work in social interactions; adversaries can compile information about you from different sources, which puts you at risk.
- Maintain a skeptical attitude; be aware when things don't seem right.
- Plan ahead—know what you're going to say if someone asks you about your work.

If you suspect you've been targeted or see suspicious activity, contact the Counterintelligence Office.

Security Briefing Quiz

You must correctly answer the following questions:

1. "Access authorization" is another term for _____.

2. Your clearance alone does not permit you to access classified matter; you must also have which of the following:

    a. Derivative classifier's permission
    b. Need to Know
    c. *a* and *b*
    d. All of these

3. **True** or **False**: Classified Matter must be marked with a level or a category, but not both.

4. Which of the following are possible consequences (aka: risks) of poor security (check all that apply)?

    ☐ Harm to national security
    ☐ Loss of America's technological and military superiority
    ☐ Damage to Sandia's reputation
    ☐ Loss of Sandia's contracts
    ☐ Termination (of responsible individuals)
    ☐ Fines and/or imprisonment

5. The concept of OPSEC can be effectively summarized in these three words: _____, _____, _____.

    Hint: These terms can be defined as follows:
    - Recognize and acknowledge that you are at risk.
    - Evaluate your routines and your environment.
    - Adopt security measures and work controls.

6. Uncleared foreign national visitor badges are this color: _____.

7. Which of the following are you **not** allowed to do with your badge (check all that apply)?

    ☐ Use it for personal identification
    ☐ Use it to vouch others into Limited Areas
    ☐ Wear it offsite
    ☐ Allow it to be photocopied
    ☐ Wear it in General Access Areas

8. If your badge is lost or stolen, what immediate action must you take? _____

9. **True** or **False**: Medicinal marijuana is allowed on Sandia-controlled premises in states where possession has been legalized.

    Hint: Your clearance is granted by the federal government and SNL is considered DOE property.

10. Classified processing is allowed in which of the following areas (check all that apply)?

    ☐ General Access Area (GAA)
    ☐ Property Protection Area (PPA)
    ☐ Limited Area (LA)
    ☐ Closed Area

11. Escorts must (check all that apply):

    - ☐ Be a Sandia employee
    - ☐ Have appropriate clearance
    - ☐ Possess a DOE-approved badge
    - ☐ Be a U.S. citizen

12. If you choose to vouch another cleared individual into a Limited Area, you must do which of the following at a minimum?

    a. Escort the person to their actual destination
    b. Perform a badge check
    c. Verify that the person has no prohibited or controlled articles
    d. Instruct the individual to notify the Facility Manager of his/her presence in the area
    e. *a* and *c*
    f. *b* and *c*
    g. Only *d*
    h. All of these

13. **True** or **False**: All information at SNL must be protected, even unclassified information.

14. Which of the following individuals determines whether documents or material are classified, and to what level and category?

    - ☐ Classified Administrative Specialist (CAS)
    - ☐ Safeguards and Security (S&S) Coordinator
    - ☐ Security Awareness Coordinator
    - ☐ Derivative Classifier (DC)

15. When marking classified documents, you should include all but which of the following (check the one that doesn't apply)?

    - ☐ One level and one category
    - ☐ Name of DC who determine it to be classified
    - ☐ Originating organization's name and number
    - ☐ Markings on top and bottom of each page
    - ☐ Anticipated expiration date
    - ☐ Markings on front and back
    - ☐ Cover and backing sheets

16. Classified information may be processed only on which type(s) of computer?

    a. Internal Restricted Network (IRN)
    b. Sandia Classified Network (SCN)
    c. Approved stand-alone systems
    d. *a* and *b*
    e. *b* and *c*
    f. Any of these

17. You should evaluate unclassified information at which of the following times to determine whether it is Official Use Only (OUO)? (Check all that apply)

    - ☐ At original draft stage
    - ☐ After each revision
    - ☐ Before distributing
    - ☐ Before disposing

18. If asked about classified or sensitive information by anyone outside SNL, you should state: _____.

19. Potential targets of foreign intelligence services include:

    a. People with a clearance
    b. People who have access to someone with a clearance
    c. Any type of media that might contain useful information
    d. *a* and *b*
    e. *a* and *c*
    f. All of these

20. **True** or **False**: You are a target of espionage.

    Hint: The answer is "True." If you need more convincing, please contact your S&S Coordinator or the Security Awareness Program.

SEC150 COMPLETION RECORD

After reading all the modules of SEC150:

1) Complete the SEC150 quiz.

2) Send the completed quiz via e-mail to securityed@sandia.gov or via fax to 505-844-7802 to receive course credit. You must score an 85 percent or higher to receive credit for this briefing.

I have read and understand all the modules in SEC150, *Comprehensive Security 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 e-mail or fax number (please write legibly).

_____

Sandia National Laboratories

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.
SAND2012-9394P dp

Approved for public release; further dissemination unlimited.

SEC150

Comprehensive Security Briefing

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories

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. SAND 2012-9394P. dp.