SEC100, Annual Security Refresher Briefing

2016/2017

SAND Number: SAND2016-10913 TR
Introduction

Module 1 Protecting Critical Information
Module 2 Making Something Old New Again
Module 3 Escorting in Meetings
Module 4 Creating an Unclassified Presentation
Module 5 Reporting to Security Incident Management Program (SIMP)
Module 6 Using Social Media
Module 7 Suspect/Counterfeit parts

Conclusion

To get credit in TEDS, you must complete all the modules (1 through 7).
As we model our leadership brand and honor our calling to serve our nation and Sandia’s missions, we all must be guardians of our nation’s security. Every day because of the work we do our information is threatened by malicious attacks, espionage, inadvertent release, and human error.

We, together, are the first and most critical line of defense. All of us, every member of the Sandia workforce must do our part to protect the information entrusted to us.

This year’s Annual Security Refresher Briefing continues to address emerging threats and includes recent scenarios of security incidents at our sites and the lessons we have learned from them. You will also review scenarios from daily occurrences and receive some security tips to help you think, assess, and protect what is ours.

Together we will continue to provide exceptional service in the national interest.
<table>
<thead>
<tr>
<th>Incident</th>
<th>Lesson Learned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to seek classification review</td>
<td>Understand the information sensitivities for your program • Seek Derivative Classifier (DC) review and guidance • Unclassified information can become classified when new or additional unclassified facts, from open source, or other documents are combined • Use the Review and Approval process</td>
</tr>
<tr>
<td>Unauthorized disclosure</td>
<td>All information must go through Review and Approval (R&amp;A) before release • Understand the distribution requirements for classified information • Export Controlled Information (ECI) may be unclassified but requires need-to-know and US citizenship • Prior to meetings, verify proper clearance level of attendees</td>
</tr>
<tr>
<td>Misclassification of classified documents/matter</td>
<td>Classified matter must have appropriate markings • prior to using legacy data, get a DC review • Classified documents must have a cover and back sheet</td>
</tr>
<tr>
<td>Improper handling or storage of classified</td>
<td>Designate a work space for classified work • Do not comingle classified documents with unclassified matter • Prevent distractions while working with classified matter • Ensure repositories are secure • Seek guidance/assistance from Classified Matter Protection and Control (CMPC), DC, or your manager</td>
</tr>
<tr>
<td>Processing classified on an unauthorized system</td>
<td>Personal computers should not be used to create information for business purposes • Ensure you have the appropriate software/applications for email use and protection of Sandia information (Good) on your personal device</td>
</tr>
<tr>
<td>Improper storage on enterprise-wide systems (FileNet, SharePoint, Dropzone)</td>
<td>Ensure your information can be kept on the network you are adding it to • Ensure proper need-to-know controls are added • Keep metagroups up to date • Reassess if you are adding individuals based on convenience • Some metagroups can quickly grow to several hundred members • Use Protected Drop Zone for sensitive information</td>
</tr>
</tbody>
</table>
Module 1: Protecting Critical Information

Sam is a Q-cleared employee who has worked at Sandia for the past eight years. He has started a new job and is anxious to learn about what information he will be responsible for. Will it be Classified, Unclassified Controlled Information or OPSEC Critical Information? Sam meets with his manager to review the program’s Critical Information List.

THINK: What is the critical information that needs protection from adversaries (insiders, foreign spies, criminals, etc.)?

ASSESS: Identify the vulnerabilities and risk if the information is lost.

PROTECT: Implement countermeasures to effectively protect the information to an acceptable level of risk.

Your responsibilities

Recognize, understand, and protect critical information, as identified by the responsible program manager.

Protect critical information from inadvertent release (e.g., via the web, internet, social media, conferences/symposia, publications, Lab News or other means) to individuals who do not have a need to know (NTK) for that information.
Work with your Subject Matter Experts, OPSEC Professionals, Managers, and Project Leads to develop a Critical Information list for your programs and activities.

Critical Information: Specific facts about friendly (e.g., DOE, Sandia) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives. (Also known as: OPSEC Critical Information.)

For OPSEC questions, assistance or to schedule an OPSEC assessment, consultation, or presentation with your organization, contact Security Connection at 321 or 505-845-1321.

Resource: Corporate Policy ISS100.3.4, Conduct Operations Security
Module 2: Making something old new again

Sam has been asked by his manager to create a new document outlining a path forward after renewing a relationship with former customer. Sam extracts data from an unmarked document found on the customer’s open source website. Sam believes that combining portions of the open source document with Sandia’s information may be classified.

THINK: Could the information in the open source document become classified when combined with Sandia information?

ASSESS: Could classified information be inadvertently released if the new document is posted to the customer’s website?

PROTECT: A classification review is required when; finalizing a draft, and before releasing information.

Your responsibilities

Review program requirements to understand the sensitive aspects of your work.

Engage your Derivative Classifier (DC) for assistance with program sensitivities and classified related issues.

Use the classified network, if in doubt of the sensitivity of the information.

If asked about classified information in the public domain, state only “We do not comment on this type of information.” Do not comment on information in open literature.
Working with Classified

**Classified information** is information that is classified by a statute or executive order. **Classified matter** is any combination of documents and material containing classified information. Access is restricted to persons with appropriate access authorizations (security clearances) and “need to know.”

**Classification levels** and **categories** are based on the potential for damage to national security, also known as the “risk.” Levels, categories, and damage criteria define what protections are needed. As risk increases, so do protection measures, including the clearance level required for access to the information.

<table>
<thead>
<tr>
<th>Classification Level</th>
<th>Classification Categories and Clearance Levels</th>
<th>National Security Information (NSI)</th>
<th>Degree of Damage (if released)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Secret (TS)</td>
<td>Restricted Data (RD)</td>
<td>Q only</td>
<td>Exceptionally Grave</td>
</tr>
<tr>
<td></td>
<td>Formerly Restricted Data (FRD)</td>
<td>Q only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Formerly National Security Information (NSI)</td>
<td>Q only</td>
<td></td>
</tr>
<tr>
<td>Secret (S)</td>
<td>Restricted Data (RD)</td>
<td>Q and L</td>
<td>Serious</td>
</tr>
<tr>
<td>Confidential (C)</td>
<td>Restricted Data (RD)</td>
<td>Q and L</td>
<td>Undue</td>
</tr>
<tr>
<td></td>
<td>Formerly Restricted Data (FRD)</td>
<td>Q and L</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Formerly National Security Information (NSI)</td>
<td>Q and L</td>
<td></td>
</tr>
</tbody>
</table>

**Classification Office** - If you think a DC determination is incorrect, challenge the classification status of information by working with the Classification Office – SNL/NM (505) 844-5574 or SNL/CA (925) 294-2202.

**DOE Office of Classification** - If a classification challenge can’t be resolved locally, an SNL Classification Officer will submit a challenge in writing to the Director, DOE Office of Classification. You also have the right to submit a formal written challenge directly to the Director. Request information from outreach@hq.doe.gov. Under no circumstances will you be subject to retribution for making such a challenge.

**Security Tip**

**Derivative Declassifier (DD)** - an individual authorized to declassify or downgrade documents or material that an employee believes no longer requires protection, in specified areas, as allowed by his or her description of authority.

**Declassification review must occur when:**
- Prepared for declassification in full
- Prepared as redacted versions
- Requested under statute or E.O (i.e., declassification for public release)
- Referred to DOE by other Government agencies that are marked or identified as potentially containing RD/FRD/TFNI or DOE NSI equities

**Classified Administrative Specialist (CAS)** – an individual trained to mark, store, duplicate, destroy, and mail classified matter.

To find a DC or DD in your area (NM and CA sites), use the Jupiter application or contact Security Connection @ 505-845-1321.

**Resource:**
- Corporate policy ISS100.1.1, Identify Classified
- Classification Bulletin GEN-16, REVISION 2, "No Comment" Policy on Classified Information in the Open Literature
Module 3: Escorting in Meetings

Sam is escorting a new uncleared employee to a project design meeting with the customer. The meeting isn’t supposed to go into any classified area of discussion, but as the customer begins to discuss another upcoming project, Sam is sure the conversation is now classified.

THINK: Are all meeting attendees cleared?
ASSESS: What damage can be done if the information is classified?
PROTECT: Before beginning any meeting – identify the clearance levels of the attendees and the clearance level of the room to ensure information (classified or unclassified) is identified and protected.

Your responsibilities

Obtain, read, and possess a Security Notice card, and act accordingly. Cards are available from the Badge Office or Visitor Control Office.

Understand the area’s security requirements when escorting an uncleared individual.

Ensure measures are taken to prevent compromise of Safeguards & Security interests, especially classified matter.

Discuss the controlled and prohibited articles policies for the area being visited.
Areas at Sandia are designed with risk in mind: Public Areas allow open access, Property Protection Areas require swipe access, Limited Areas require two-factor authentication (badge and PIN) because of the potential for classified processing. As the desirability/sensitivity increases for information in the area, so do the security controls.

Request a Security Notice card through Security Connection 321 from a Sandia phone or 505-845-1321 from any phone.

Resource: Corporate policy ISS100.5.3, Control Site Access
Module 4: Creating a Presentation

Sam has been asked to create a specific program presentation and to keep it “unclassified” so it can be shared with uncleared individuals. Sam is a subject matter expert and much of the work is considered classified. Sam is not an authorized derivative classifier (DC) and is unsure of what computing system he should use to create the presentation.

**THINK:** Is there a risk of mistakenly creating classified on an unclassified system?

**ASSESS:** Could I compromise potentially classified information by creating the presentation on a system not approved for classified?

**PROTECT:** Create presentations on the appropriate computing system, mark it “system-high” as a classified draft until it is reviewed and given the level and category by an authorized DC.

**Your responsibilities**

Review program requirements to understand the sensitive aspects of your work.

Engage the appropriate DC to discuss the presentation, identify the potentially classified information and identify the appropriate classified system.

Mark, process, and protect as classified until reviewed by an authorized DC, if the potential for classified information exists.

Submit the presentation through the formal Review and Approval Process if it is going to be shared with an uncontrolled audience.
If you’re intending to release information to an uncontrolled, widespread, unknown, or public audience, you must obtain a formal review and approval (R&A). This includes information intended for release to Congress. You must also request a DC review (i.e., an informal or programmatic review) for:

- A newly generated document or material in a classified subject area that may potentially contain classified information.
- An existing, unmarked document or material that you believe may contain classified information.
- An existing, marked document or material that you believe may contain classified information.
- A document or material generated in a classified subject area and intended for public release (e.g., for a publicly available webpage, for news organizations), including documents provided to or testimony given to Congress.
- A newly generated document that consists of a complete section taken from another document (e.g., chapter, attachment, appendix)
- Printed output from a classified information system.

Information processed on a classified computing system must be marked at the highest level and category you believe it may contain until it’s reviewed by an authorized DC. Such information should be marked and controlled appropriately until it has been reviewed for classification.

Do you have a classified computing account with the capability to send email? If yes, you are responsible for submitting a request through JUPITER system to become an email-only derivative classifier so you can appropriately classify and mark all email messages sent on approved classified systems.

### Security Tip

Ask your manager about attending classified training if your information is in a potentially classified subject area.

When exporting any data from a classified system to an unclassified one (whether electronically or by use of electronic media), an Authorized Transfer Point (ATP) must be used and approved processes must be followed.

When working with classified information, use only computers on the approved classified networks or an approved stand-alone system. Home computers are not considered approved systems, even for use with Sandia’s unclassified information.

If you see unattended classified matter, secure it and report it by calling 321 from a Sandia phone or 505-845-1321 from any phone.

### Resource:

- Corporate policy ISS100.1.4 [Create Classified Matter](#)
- Corporate policy ISS100.1.2 [Control Classified Matter](#)
Module 5: Reporting to Security Incident Management Program (SIMP)

Sam comes back from lunch and notices his manager trying to access the Limited Area. She realizes that she left her HSPD-12 credential in her smart card authentication badge reader in her office. Sam offers to assist her by going to her office and retrieving the credential and bringing it back out.

THINK: How do I know the individual has not lost his/her clearance?
ASSESS: What are the consequences for vouching someone without a badge into a Limited Area?
PROTECT: Prevent unauthorized access by offering to get their badge from the reader in their office.

Your responsibilities

Control site access by **not** vouching persons into non-public areas without a proper badge. **Report any violations to SIMP.**

Protect information from individuals that do not have the proper “Need to Know” by **not** escorting a person into an SNL access-controlled area (i.e., Non-Public General Access Area, Property Protection Area, or Limited Area) without a proper badge. **Report any violations to SIMP.**
The Security Incident Management Program (SIMP) offers the following guidance when users walk away from their computers and leave their badges inserted in the smart card readers:

If you are still in an SNL access-controlled area (i.e., Non-Public General Access Area, Property Protection Area, or Limited Area) when you realize that you left your badge behind, go back and retrieve it. **Do not call SIMP.**

If you have left an SNL access-controlled area (i.e., Non-Public General Access Area, Property Protection Area, or Limited Area) before realizing that you left your badge behind, contact someone to bring the badge to you. **Do not call SIMP.**

Before granting access to others, at a minimum, perform the following badge-validation measures:

**Ensure** the badge is a DOE security badge.
**Ensure** badge photo matches the wearer.
**Ensure** the date on the badge (if any) has not expired.
**Ensure** the badge has not been tampered with or altered.
**Ensure** badge holders have appropriate clearance levels for the area being accessed.
**Report** discrepancies to the Protective Force.
Module 6: Using Social Media

Sam has settled in for a new day in his new office. He opens his emails on his Sandia mobile device and finds a Facebook notification with a link. He notices that it is from Cathy, but no last name. He knows there’s a Cathy in his organization, but he isn’t sure.

Before clicking on social media links:

**THINK:** Do I know this person well enough to click on their information?

**ASSESS:** could clicking on a link on a Sandia owned device, download a virus or malware?

**PROTECT:** Learn and use all the security controls on each site and keep up with them as they change.

Your responsibilities

Verify that any requests are from personas you know and trust.

Beware of links, downloads, and attachments, just as you would in email.

Understand that even a small bit of information can be important to an adversary.
Use OPSEC Social Media Tips for protecting you, your family, friends, and coworkers from online threats.

Personal Information

• Keep sensitive, work-related information OFF your online profile.
• Keep your plans, schedules, and location data to yourself.

Settings and Privacy

• Review and set all your privacy, search visibility, and security options on a regular basis.
• Beware of “apps” or plugins (often written by unknown third parties) often used to access your data and friends.
• Look for HTTPS and the lock icon that indicate active transmission security before logging in or entering sensitive data (especially when using wi-fi hotspots).

Security

• Keep anti-virus, anti-malware, operating system, and other software updated.
• Verify that an individual is legitimate by contacting the individual's employer when evaluating employment offers originating from any social networking site.

Security Tip

If in doubt, don’t send it out.
Link responsibly.
Respect copyrights.
Remember your day job.
Be vigilant.

For more information see:

Interagency OPSEC Support Staff’s brochure, "OPSEC and Social Networking Sites"

DOE and Sandia Reporting Requirements

Resource:
Corporate policy ISS100.3.4, Conduct Operations Security,
Module 6: Suspect/Counterfeit Parts

Sam has purchased a Microsoft mouse from a multi-leveled e-commerce site where anyone is allowed to sell products (i.e., Amazon, E-Bay, Alibaba, Group-on, Newegg, etc.). When Sam receives the item, he notices the packaging was damaged and was lacking product information such as the manufacturer, part description, model/part number, and warranty information. Sam knows the item does not seem right but he uses it anyways. Not long after plugging the mouse in, Sam’s computer would not work properly. Upon further investigation of the mouse it was determined that it was counterfeit and contained malware which was loaded onto Sam’s computer upon use.

THINK: Does the item appear to be genuine or does it have signs that it might be counterfeit? How was the item ordered?

ASSESS: Could the item being ordered pose a safety, security, and/or environmental risk?

PROTECT: Work with a Sandia Contracting Representative (SCR or “Buyer”) to aid in choosing the correct procurement method as well as to specify any quality assurance requirements for items where the risk of receiving a suspect or counterfeit item exists.

Your responsibilities

Items that pose a risk should be ordered using the appropriate and allowable methods per procurement policies. Items at risk of possible suspect or counterfeit should also be visually inspected prior to use.
Security Tip

Items ordered through JIT and Purchase Order have a lower likelihood of being counterfeit versus through online e-commerce sites.

To request training and information on Suspect or Counterfeit Items or to report an item:
email sqasci@sandia.gov

Also visit the Suspect/Counterfeit Items webpage by typing in:
counterfeit.sandia.gov

The webpage offers an easy way to report items, additional information about suspect/counterfeit items, newsletters, and detailed contact information.

Don’t toss it, report it!

Visit the Suspect/Counterfeit Items webpage!
Conclusion

See Something, Say Something!

When you "See Something" or make a mistake, “Say Something.” Mistakes never get better with time.

For details about your reporting responsibilities, see the DOE and Sandia Reporting Requirements.

What's the risk?
Reporting is about mitigating potential consequences, which include:

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

Every day, because of the work we do our information is threatened by malicious attacks, espionage, inadvertent release, and human error.

Every member of the Sandia workforce is the first and most critical line of defense and we must do our part to protect the information entrusted to us.

We accomplish this by:
Working with management and other security professionals to understand the information that is critical to Sandia.

Using the Review and Approval process to avoid inadvertent disclosure of classified or sensitive information.

Applying sensible caution when giving anyone access to Sandia's security areas.

Understanding corporate policy to prevent loss and protect what is ours.
Sam made it through another year.

He learned a lot about preparing presentations, identifying critical information, determining the recipients of Sandia’s information, both internally and externally and the steps he is required to take to protect that information.

Sam has a better understanding of his security responsibilities and will have an incident free year in his new job.

Think. Assess. Protect.

Keep Sandia Secure.

security.sandia.gov

Security Connection

505-845-1321
or 321 from a Sandia phone

Reminder: In addition to SEC100, Counterintelligence Training CI100 is required annually for all Sandia employees, all staff-augmentation contractors, and any other contractors or visitors who work on-site side-by-side with Sandians and who might therefore be targeted and approached by foreign entities, excluding contractors/visitors who receive their training through other government facilities.
After reading all the modules of SEC100, complete this form and send it via email to security@sandia.gov or via fax to 505-844-7802 to receive credit.

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

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

<table>
<thead>
<tr>
<th>Print Full Name (Last, First, Middle):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SNL Org # or Company Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>□ Employee</th>
<th>□ Contractor</th>
<th>□ Consultant</th>
<th>□ Student</th>
<th>□ KMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
<td></td>
<td></td>
<td></td>
<td>Date:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SEC100 Feedback Form

Your feedback is important to us. Please complete this evaluation and send it to us via email at security@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 tool?
SOCIAL NETWORKING SITES (SNS), like Facebook® and Twitter®, are software applications that connect people and information in spontaneous, interactive ways. While SNS can be useful and fun, they can provide adversaries, such as terrorists, spies and criminals, with critical information needed to harm you or disrupt your mission. Practicing Operations Security (OPSEC) will help you to recognize your critical information and protect it from an adversary. Here are a few safety tips to get you started.

THINK BEFORE YOU POST! Remember, your information could become public at any time due to hacking, configuration errors, social engineering or the business practice of selling or sharing user data. For more information, visit the Interagency OPSEC Support Staff’s website.

---

**Personal Information**

Do you:

- Keep sensitive, work-related information OFF your profile?
- Keep your plans, schedules and location data to yourself?
- Protect the names and information of coworkers, friends, and family members?
- Tell friends to be careful when posting photos and information about you and your family?

**Posted Data**

Before posting, did you:

- Check all photos for indicators in the background or reflective surfaces?
- Check filenames and file tags for sensitive data (your name, organization or other details)?

**Settings and Privacy**

Did you:

- Carefully look for and set all your privacy and security options?
- Determine both your profile and search visibility?
- Sort “friends” into groups and networks, and set access permissions accordingly?
- Verify through other channels that a “friend” request was actually from your friend?
- Add “untrusted” people to the group with the lowest permissions and accesses?

**Passwords**

Are they:

- Unique from your other online passwords?
- Sufficiently hard to guess?
- Adequately protected (not shared or given away)?

**Security**

Remember to:

- Keep your anti-virus software updated.
- Beware of links, downloads, and attachments just as you would in e-mails.
- Beware of “apps” or plugins, which are often written by unknown third parties who might use them to access your data and friends.
- Look for HTTPS and the lock icon that indicate active transmission security before logging in or entering sensitive data (especially when using wi-fi hotspots).

---

**THink Before You Post!** Remember, your information could become public at any time due to hacking, configuration errors, social engineering or the business practice of selling or sharing user data. For more information, visit the Interagency OPSEC Support Staff’s website.
Inside This Issue:

Open House 1
Counterfeits-Organized Crime 2
Counterfeit Quiz 2

Upcoming Events:

Suspect/Counterfeit Items Quarterly Meeting
When: June 1st, 2016
Time: 2:00-3:00 p.m.
Where: Bldg. 823 Breezeway

If you are an assigned point of contact you are automatically enrolled to attend the quarterly meetings.

If you are not an assigned point of contact, email sqasci@sandia.gov if you would like to attend this meeting.

Counterfeit Quiz Answer:

Example 1 is counterfeit. Genuine cables have a grey/metallic faceplace insert not black or white.

Visit our webpage!

Suspect/Counterfeit Items Presentation & Open House

Come and join the Suspect/Counterfeit Items team from Sandia and Los Alamos National Laboratories for our annual presentation and open house on April 7th, 2016 in the Tech Area IV Building 962 Auditorium from 10 AM to 3 PM.

Learn to prevent and detect Suspect/Counterfeit Items (S/CI) by attending any of the presentations offered as well as hands on training sessions. No pre-registration required, just show up whenever you want to! Presentations will also be available via video stream if you are unable to attend.

Don’t miss out on this great opportunity to learn more about these items and have a lot of fun.
Buying counterfeit goods such as handbags, sunglasses, shoes, or movies may seem harmless compared to the dangers of purchasing other counterfeit items such as electrical products. The problem with counterfeit items is that they are not harmless no matter what type of item. In fact, most counterfeit goods are often produced by organized criminal groups and terrorist organizations. By buying these harmless items you may be funding the next big terrorist operation or even the criminal activity in our neighborhoods.

The sale of counterfeit goods has been recognized by organized criminal groups as a large source of untapped income. There has been defined movement in many of these organizations from selling illegal drugs to selling counterfeit products and medicines. There are many reasons for this such as the greater income provided from selling counterfeit products as well as the legal recourse they face if caught.

The sad truth is that most countries do not have any laws against counterfeiting and even if laws do exist they are often very lenient resulting in some fines and minimal jail time. In comparison to facing a lifetime in jail this option as well as making even more money than selling illegal drugs such as heroin seems like a win/win situation for the criminal.

It is also very easy for these criminal organizations to make the switch from drugs to counterfeits as they already have routes and processes set up for smuggling illegal drugs, firearms, or even people.

The important thing to remember is that there is no such thing as a harmless counterfeit. The cost of buying into organized crime hurts everyone!

If you have time check out the documentary “Counterfeit Culture” from the CBC News network at: [http://www.cbc.ca/player/play/2324389261/](http://www.cbc.ca/player/play/2324389261/) to learn more.

---

**Counterfeit Quiz**

These are both Apple Lightening to USB cables. One of them is counterfeit, can you figure out which one?

Answer is on page 1 left hand column

---

“Intellectual Property has the Shelf Life of a Banana.”

-Bill Gates

Request training for your group!

To request training with your group, ask questions, or report items contact sqasci@sandia.gov

---

COUNTERFEITS AND ORGANIZED CRIME

---

**Detect & Protect: March 2016**

S/CI Quarterly Quarterly Newsletter

SAND Number: SAND2016-1874 M

---

COUNTERFEIT Quiz

These are both Apple Lightening to USB cables. One of them is counterfeit, can you figure out which one?

Answer is on page 1 left hand column

---

**Example 1**

**Example 2**
### Other Reporting Requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
</table>
| **Incidents of Security Concern (aka Security Incidents)** | Report immediately, but **do not provide details over the phone.**  
NM: OOPS (311) and SIMP (505-283-7467)  
CA: Security Connection (321) or SIMP (925-294-2600);  
TTR: Central Alarm Station (702-295-8285)  
**Note:** Contractors have added responsibility of reporting incidents to their Facility Security Officer (FSO). |
| **Waste, Fraud, & Abuse**       | Incidents of waste, fraud, abuse and criminal matters must be reported to Ethics Advisory and Investigative Services (505-845-9900) and other appropriate authorities (e.g., manager, security officials). |
| **Theft of Property**           | Any theft of Sandia or U.S. Government property must be reported immediately to Property Management (505-284-3265).  
**Note:** All property that is considered stolen, lost, or missing must be reported regardless of value and regardless of whether it is considered controlled or uncontrolled property. |
| **Wrongdoing**                  | Report incidents of wrongdoing to Ethics Advisory and Investigative Services (505-845-9900).  
**Note:**  
- *Incidents of wrongdoing* are not limited to circumstances listed in the previous table.  
- You may also report directly to the Office of the Inspector General any information concerning wrongdoing by DOE employees, contractors, subcontractors, consultants, grantees, other recipients of DOE financial assistance, or their employees. |
| **Drug Use**                    | Report incidents of illegal drugs in the workplace to Ethics Advisory and Investigative Services (505-845-9900). This includes, but is not limited to, trafficking in, selling, transferring, possessing, or using illegal drugs.  
**Note:**  
- Illegal drugs are prohibited on both Sandia-controlled premises and Kirtland Air Force Base property.  
- The use of illegal drugs—or legal drugs in a manner that deviates from medical direction—is a serious offense and could result in termination of your clearance and your employment, as well as arrest. |

### Managers

Managers are responsible for immediately reporting to Personnel Security (NM: 505-844-4493, CA: 925-294-1358) when an employee’s clearance is no longer required, employment is terminated, individual is on extended leave of 90 calendar days or more, or access authorization is not required for 90 calendar days or more. Ensure completed DOE F 5631.29, Security Termination Statement, and badges are immediately delivered to the Clearance Office.

### TTR & Remote Sites Personnel

Report to SNL/NM, unless otherwise indicated.

### SCI- and SAP-Briefed Personnel

Contact the appropriate Special Security Officer or Program Security Officer for guidance regarding program-specific reporting requirements.

---

"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."

—Executive Order 12968, Access to Classified Information
**Concerns of Personnel Security Interest**

<table>
<thead>
<tr>
<th>If you...</th>
<th>Report to...</th>
<th>By this date...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Rqmts</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are approached or contacted by ANY individual seeking unauthorized access to classified matter or special nuclear material (SNM).</td>
<td>NM—Counterintelligence (505-284-3878) or SIMP pager (505-283-7467)  CA—Counterintelligence (925-294-1362) or SIMP (321 or 925-294-2600)</td>
<td>Immediately.</td>
</tr>
<tr>
<td>Are aware of information about other Members of the Workforce that raises concerns of personnel security interest. <strong>Note:</strong> Such information must be reliable and relevant, and create a question as to the individual's access authorization eligibility.</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900)  CA—Clearance Processing (925-294-2061)</td>
<td>Immediately.</td>
</tr>
<tr>
<td><strong>Legal Issues</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Are arrested; subject to criminal charges (including charges that are dismissed); receive citations, tickets, or summonses; or are detained by federal, state, or other law-enforcement authorities for violations of the law within or outside of the U.S. <strong>Note:</strong> Traffic citations/tickets/fines are reportable only if they exceed $300 and only when the fine is assessed, unless drugs or alcohol were involved. To court and the court's ruling equals a fine above $300. Court fees or other administrative costs associated with the traffic citation/ticket/fine should not be added to the final assessed amount.</em></td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900)  CA—Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and In writing within the next 3 work days.</td>
</tr>
<tr>
<td>*File for bankruptcy, regardless of whether it is for personal or business-related reasons.</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900)  CA—Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and In writing within the next 3 work days.</td>
</tr>
<tr>
<td>*Have your wages garnished for ANY reason. <strong>Examples:</strong> divorce, debts, child support.</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900)  CA—Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and In writing within the next 3 work days.</td>
</tr>
<tr>
<td><strong>Citizenship</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Have legal action resulting in a name change.</td>
<td>Personnel Security Info Line (505-284-3103)</td>
<td>Orally within 2 work days of occurrence, and In writing within the next 3 work days (via SF 2730 NCB).</td>
</tr>
<tr>
<td>Marry or cohabitate with a person.</td>
<td>Personnel Security Info Line (505-284-3103)</td>
<td>In writing within 45 days of marriage or cohabitation (via DOE F 5631.34).</td>
</tr>
<tr>
<td><strong>Life Circumstances</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Are hospitalized for mental health reasons.</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900)  CA—Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and In writing within the next 3 work days.</td>
</tr>
<tr>
<td>*Are treated for drug or alcohol abuse.</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900)  CA—Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and In writing within the next 3 work days.</td>
</tr>
<tr>
<td><em>Use an illegal drug or a legal drug in a manner that deviates from approved medical direction.</em></td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900)  CA—Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and In writing within the next 3 work days.</td>
</tr>
<tr>
<td>No longer require your clearance, terminate employment, are on extended leave of 90 calendar days or more, or access authorization isn’t req’d for 90 calendar days or more.</td>
<td>NM—Personnel Security Info Line (505-284-3103)  CA—Clearance Processing (925-294-2061)</td>
<td>Immediately and follow up by providing completed DOE F 5631.29.</td>
</tr>
<tr>
<td><strong>Foreign Travel</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have personal foreign travel to a sensitive country. <strong>Note:</strong> Although you are not required to report travel to a non-sensitive country, you should keep a personal record of personal foreign travel for future clearance (re)investigations.</td>
<td>NM—Counterintelligence (505-284-3878)  CA—Counterintelligence (925-294-1362)</td>
<td>Prior to travel or as soon as practicable.</td>
</tr>
<tr>
<td>Have substantive contact with any foreign national. <strong>Note:</strong> “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). At SNL, substantive contact includes associations that involve meeting and the sharing of SNL business information.</td>
<td>NM—Counterintelligence (505-284-3878)  CA—Counterintelligence (925-294-1362)</td>
<td>Immediately through: Foreign National Interaction System website</td>
</tr>
<tr>
<td>*Are employed by, represent, or have other business-related associations with a foreign or foreign-owned interest, or with a non-U.S. citizen or other individual who is both a U.S. citizen and a citizen of a foreign country.</td>
<td>NM—Counterintelligence (505-284-3878)  CA—Counterintelligence (925-294-1362)</td>
<td>Immediately through: Foreign National Interaction System website</td>
</tr>
<tr>
<td>*Have an immediate family member who assumes residence in a sensitive country, and when that living situation changes; e.g., your family member returns to the U.S. or moves to another country, sensitive or non-sensitive. (See list of sensitive countries at the International Travel Office website.)</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900)  CA—Personnel Security (925-294-2061)</td>
<td>Immediately.</td>
</tr>
</tbody>
</table>

* You are required to report these items to the Sandia organizations listed, but you have the option of also reporting them directly to DOE Personnel Security.
Classification Bulletin GEN-16, Revision 1, ""NO COMMENT' POLICY ON CLASSIFIED INFORMATION IN THE PUBLIC DOMAIN," has been updated to address concerns regarding documents marked as classified in the open literature and to clarify the actions to be taken when encountering such documents. This revision also replaces the term "public domain" with "open literature." These instructions have been coordinated with the Department of Energy (DOE) Office of the Chief Information Officer.

In many cases, the classification markings for documents in the open literature do not accurately convey the current classification status of the document (e.g., historical documents released by the National Archives and Records Administration with classification markings without any apparent indication of declassification). In cases where the current classification status of marked documents in the open literature is unknown, only an appropriate authority from the originating agency may determine the current classification status of the document.

GEN-16, Revision 2, recognizes that it is possible to have incidental contact online with a document that is marked as classified but its actual classification status is unknown. Such a document must be treated as classified to the extent that cleared employees must not save the document on their computer system or forward the document via e-mail though it may be printed only to a printer with volatile memory. The document must be reported through secure means following DOE policies and local instructions.
In those cases where the document is ultimately determined to contain classified information, merely reading the document online does not constitute a comment and there are no classification issues. As long as the document has not been saved, forwarded, or printed to a printer with non-volatile memory, sanitization of the computer is not necessary. Sanitization may be counterproductive by drawing attention to the document.

If you have any questions regarding the classification of a document or whether GEN-16 applies, contact your local Classification Officer (CO) for a determination. Also contact your local CO if you encounter situations not addressed in this bulletin where you think GEN-16 might apply or if you need additional guidance. If you have any questions concerning sanitization, contact your local security office.

This revision replaces the term “public domain” with “open literature.” This is done to be consistent with classification guidance and for the meaning to be more accurate. Public domain documents are limited to documents that are not copyrighted, whereas open literature is a broader term that includes documents that may be copyrighted but are still available to the public. For the purposes of this bulletin, “open literature” refers to resources (e.g., publications, presentations) in the public domain, as well as copyrighted resources that are publicly available.

If you have any questions concerning this bulletin, please contact Nick Prospero at 301-903-9967 or nick.prospero@hq.doe.gov.

Attachment
I. PURPOSE. To provide guidance to DOE Federal and contractor employees authorized access to classified information (e.g., authorized person) on appropriate actions when unmarked documents, publications, or verbal comments containing classified information (i.e., Restricted Data (RD), Formerly Restricted Data (FRD), Transclassified Foreign Nuclear Information (TFNI), National Security Information (NSI)) or documents that are marked as containing classified information appear in the open literature and to clarify the circumstances that constitute comment.

II. CANCELLATION. This bulletin supersedes GEN-16, Rev "NO COMMENT" POLICY ON CLASSIFIED INFORMATION IN THE PUBLIC DOMAIN," dated August 31, 2011.

III. RATIONALE. In today's information environment, it is likely that persons who are authorized access to classified information will encounter such information especially online in the open literature. DOE's goal is to avoid comment in order to minimize the damage to national security. Commenting on classified information in the open literature can cause risk of greater damage to the national security by confirming its location, classified nature, or technical accuracy. This bulletin establishes DOE standards for what constitutes a comment in regard to classified information.

Classified information can appear in the open literature in documents marked as classified that are generated by the Government. Classified information can also appear in the open literature in documents that are not generated by the Government and do not have any indication of the classification status of the information. Classification markings or the lack of classification markings do not always accurately reflect the classification status of information in the document. In order to maintain effective policies in an increasingly challenging information technology environment and for consistency with cybersecurity practice, this bulletin addresses classified information in the open literature contained in unmarked documents, as well as documents with classification markings.
IV. NATIONAL POLICY.

a. "No Comment” Policy. 10 CFR § 1045.22

(1) Authorized holders of RD and FRD shall not confirm or expand upon the classification status or technical accuracy of classified information in the public domain.

(2) Unauthorized disclosure of classified information does not automatically result in the declassification of that information.

(3) If the disclosure of classified information is sufficiently authoritative or credible, the DOE Associate Under Secretary for Environment, Health, Safety and Security shall examine the possibility of declassification.

b. Executive Order 13526, Classified National Security Information, Part I, Section 1.1(c). “Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.”

V. PRINCIPLES.

a. Comment. A comment is any activity that would allow a person who is not authorized access to classified information to locate the information or confirm the classified nature or technical accuracy of the information.

b. Classification Status. An authorized person must not comment, either verbally or in writing, to a person who is not authorized access to classified information on the classification status of any classified information in the open literature (including the fact that a document is being reviewed for classification or the results of such a review, which may be disclosed only to the person who submitted the document for review).

c. Technical Accuracy. An authorized person must not comment, either verbally or in writing, to a person who is not authorized access to classified information about the technical accuracy of classified information in the open literature.

VI. GUIDANCE.

a. Guidance for Documents in the Open Literature that are Marked as Classified. Marked documents may appear in the open literature for several reasons. For example, they may have been leaked or they may have been appropriately declassified and released. In many cases, classification markings do not accurately convey the classification status of the document.
The markings may not be current and, unless the document is marked to indicate the document has been declassified, only an appropriate authority from the originating agency may determine the current classification status of the document. In cases where the classification status of marked documents in the open literature is ambiguous or unknown (e.g., declassification markings are not evident), the source must be treated as classified and the following guidance must be adhered to:

(1) **Viewing.** Inadvertent viewing of such documents is not a comment unless instructions to the contrary are issued by the U.S. Government regarding a specific compromise.

(2) **Links.** Links to such documents must not be forwarded via e-mail to any other person.

(3) **Printing.** Such documents may only be printed on a printer that has volatile memory. When printed, the documents must be protected, as required.

(4) **Saving or Sending.** The source itself must not be saved on an unclassified system or sent via e-mail to another person.

b. **Guidance for Documents Containing Classified Information in the Open Literature that are Not Marked.** The following guidance provides clarification as to the activities that are or are not considered comment:

(1) **Viewing.** Merely reading unmarked and unannotated documents or publications available in the open literature that contain classified information is not a comment unless instructions to the contrary are issued by the U.S. Government regarding a specific compromise.

(2) **Collecting Publications or Internet Web Pages in a General Subject Area of Interest.** Collecting unmarked and unannotated open literature publications or web pages in a given subject area or lists of open literature publications, assuming the title of that publication is not classified, is not a comment. Collections of topical news stories, favorite or bookmarked web sites, or listing of references do not by themselves constitute a comment. Basic summaries of collections of news articles may or may not constitute a comment depending on the content of the summary. Authorized persons must ensure that DOE classified information is not included within any summary of an open literature document. Authorized persons may collect open literature documents on such subjects as nuclear weapons, uranium centrifuges, etc., given that a variety of sources are widely available to the general public or to any informed researcher not authorized access to classified information, but they must not limit such
collections only to open literature publications that contain classified information.

(3) **Possessing, Printing, Saving, or Sending.** The mere possession, printing, storage, or distribution of material from the open literature (e.g., books, news articles, links to Internet sites) that may contain classified information and are not marked as classified does not by itself add credibility to such material or constitute comment.

(4) **Citing.** Authorized persons may cite (e.g., in footnotes and bibliographies) well-known, unmarked open literature sources that contain classified information if the vast majority of the open literature document or publication does not contain classified information and the specific reference does not point to the classified information in the document. Authors must consult with their local Classification Officer for guidance on acceptable citations.

(5) **Annotating.** Authorized persons must not annotate unmarked open literature material (including email containing such material or links to such material) to indicate in any way that the source contains classified information or that the section containing classified information is technically accurate. If authorized persons annotate an open literature source in a manner that does so, the annotated document must be reviewed by a Derivative Classifier and marked and protected at the level and category of the information as indicated in classification guidance.

c. **Unclassified Presentations and Discussions of a Classified Subject Area.** When an authorized person is required as part of his or her official capacity to give presentations or hold discussions (e.g., press conference, town hall meeting, unclassified presentation, dialog with a technical expert who is not authorized access to classified information, etc.) in a classified subject area, the employee may comment if the employee knows that the specific information is unclassified.

**WARNING:** Selective use of "No Comment" may result in confirming classified information. Therefore, an authorized person should avoid commenting in such a manner that the use of "No Comment" would implicitly reveal that the information is classified. Employees should consider responding with a statement similar to "We do not comment on this type of information." for any questions concerning classified subject areas (e.g., yields, stockpile locations, etc.).

d. **Reporting.** An employee encountering DOE classified information in the open literature must report the information following DOE policies and local instructions.
e. Review of Documents that Potentially Contain Classified Information. Per DOE Order 475.2A, Identifying Classified Information, Attachment 4, I(a)(1), “Newly generated documents or material in a classified subject area that potentially contain classified information must receive a classification review by a Derivative Classifier.” This requirement applies even if information contained in the document is taken from the Internet or another open literature source.

VII. ADVISORIES. Advisories may be issued when an incident is particularly noteworthy or significant concerns regarding release of the classified information arise. It is not possible or advisable to distribute an advisory in all instances when classified information appears in the open literature. Whether or not an advisory is released, the “No Comment” policy should be followed whenever classified information appears in the open literature.

VIII. EXCEPTIONS. Due to safety, environmental, public health, or other concerns, it may be necessary for the DOE to discuss documents in the open literature that contain classified information. Any official confirmation on the classification status or technical accuracy of information in the open literature is handled in accordance with DOE Order 471.6, Admin Chg. 1, Information Security, DOE Order 470.4B, Admin Chg. 1, Safeguards and Security Program, and any other applicable law, regulation, or policy.

IX. VIOLATIONS. Any authorized person who intentionally verifies the classification status of any information or the technical accuracy of classified information in the open literature to a person not authorized access to classified information is subject to appropriate sanctions. Sanctions may range from administrative, civil, or criminal penalties, depending on the nature and severity of the action as determined by appropriate authority in accordance with applicable laws.

X. CONTACT. Contact the Director, Office of Classification, (301) 903-3526, with any questions or comments concerning this bulletin.

Andrew P. Weston-Dawkes
Director
Office of Classification
Office of Environment, Health, Safety and Security