SEC100, Annual Security Refresher Briefing

2017/2018

SAND Number: SAND2017-12533 TR
Introduction

Module 1 Unauthorized Network-Based Transmission
Module 2 Unauthorized Disclosure of Classified Information
Module 3 Improper Storage of Classified Information
Module 4 Improper Escorting
Module 5 Counterintelligence
Module 6 Operations Security (OPSEC)
Module 7 Security Awareness Updates

Conclusion

To get credit in TEDS, you must complete all the modules (1 through 7).
Introduction

In an effort to improve the mindset regarding, and personal ownership of, security across the nuclear security enterprise (NSE), DOE believes it is of paramount importance to emphasize Sandia’s commitment to establishing and maintaining high security values. Nuclear security is an evolving responsibility that requires ongoing vigilance and awareness to sustain and improve the level of knowledge among the entire workforce, so that you are empowered to do your part to ensure protection of NNSA’s sensitive and classified work.

This year’s security refresher are case files based on incidents of security concern from all sites. You will:
• see the human performance indicators that may have contributed to the incidents,
• review the lessons learned,
• see some best practices, and
• be able to download valuable resource information.

Sandia hopes that you can incorporate some of the information into your daily work to continue “protecting what is ours”.
MODULE 1

THE CASE OF THE CLASSIFIED EMAIL

A story of unauthorized network-based transmission.
Case File

A new Sandia employee reported sending an email with a classified attachment across the Sandia Restricted Network (SRN).

The attachment was a draft, 8 months old, and had been extracted from a classified document on the Sandia Classified Network (SCN).

After the incident was reported, a DC review determined that the email contained Secret Formerly Restricted Data (SFRD).

Fortunately, all of the recipients were within the Sandia firewall, appropriately cleared, and with a need to know (NTK).
What Went Wrong?

The individual failed to obtain a Derivative Classifier (DC) review before sending the email.

The individual was a recent new hire and did not know the information was classified.

- Unfamiliar with task/first time
- Lack of knowledge

How could this have been prevented?
**THINK:**
How do I prevent unauthorized disclosure of classified matter, especially when extracting information from a classified document?

**ASSESS:**
Should I be working on the SCN?

**PROTECT:**
Obtain a DC review when extracting information from a classified document.

---

All Members of the Workforce must know:

- Where to go for assistance with classification-related issues
  - Your assigned DC or the Classification Office

- When a document or material must be reviewed for classification:
  - Prior to finalizing a working paper or document in a potentially classified area (whether hard-copy or electronic)
  - Prior to releasing it outside of the activity (e.g., ad hoc working group or program)
  - Prior to filing it permanently
  - No later than 180 days after creation of the document or 180 days after last revision
If a Member of the Workforce needs to locate a DC, use Classification’s Jupiter online application. It has a search feature that allows anyone to locate a DC. Be sure to search for a DC knowledgeable and authorized for the classified subject matter.

Know:

- **Which official must conduct the review:**
  - Your assigned DC or the Classification Office

- **When a classified document or material must be reviewed for declassification, and which official must conduct the review:**
  - Prior to document declassification, a Derivative Classifier (DDs) must conduct the review. DDs are only in the Classification Office

- **Basic information on DOE’s “No Comment” policy (GEN-16)**

- Your responsibility to challenge classification decisions

- Where to find procedures for classification challenges

- Who to contact for help with challenging a classification decision
Lesson 1 - Regular Briefings

Managers should regularly brief all of their staff regarding the work they will be doing and whether the information they are working with is in a potentially classified subject matter area. Briefings should include a discussion of the levels and categories of classified matter, and the potential for damage to national security associated with each level and category.

This is important in the case of new hires, who may not be as confident of their knowledge and expertise as a long-term staff member. Managers should assign mentors to help new workers get familiar with project and classification information.
Lesson 2 - DC Review

The individual should have obtained a DC review of information that is potentially in a classified subject matter area prior to transmission, especially when extracting information from a classified document.

NOTE: Email-only DCs are strictly limited to derivatively classifying their own emails.
Corporate Policies:
ISS100.1.1, Identify Classified Information
ISS100.1.2, Control Classified Matter
ISS100.1.5, Use Classified Matter

Read or Print the following handouts (at the end of this briefing):
Everything You Need to Know About Classified Understanding Classification
GEN-16, DOE’s “No Comment” policy

For Help:
S&S-MAN-051, Classification Handbook for Derivative Classifiers

Security Connection: 505-845-1321 or 321 (from a Sandia phone)
Classification Office: NM and remote sites (505) 844-5574
CA (925) 294-2202

Helpful Links (with SRN access):
Jupiter online application
Security Speakers Bureau
MODULE 2

THE CASE OF THE CONFERENCE

A story of unauthorized disclosure of classified information.
Case File

A Sandia employee was invited to present to a large audience at an unclassified conference. The presentation had been submitted and approved through the formal Review and Approval (R&A) process and was provided to all conference attendees. Before going to the conference, the employee added one photo from a recent test.

During the presentation, another Sandia employee recognized that the photo and caption contained Secret National Security Information (SNSI).
What Went Wrong?

The information was added to the presentation after R&A. It did not receive a review of the new SNSI photo and caption.

The presenter did not believe the information was classified.

- Unsafe attitudes for critical tasks
- Complacency/over-confidence

How could this have been prevented?
THINK:
How do I prevent unauthorized disclosure of classified matter in technical publications, conference papers, and online publications?

ASSESS:
Has all of the content in my presentation been through the formal R&A process?

PROTECT:
Ensure the formal R&A process is the last step prior to public release of any information.

- All releases of information to a public, widespread, or unknown audience must be coordinated through the formal R&A process.
- R&A must be the last step before the public release.
- If a document is substantially modified after the review, it must be re-submitted.
- Read and be familiar with GEN-16, DOE's "No Comment" policy.
Lesson 1 - Review and Approval

All releases of information to an uncontrolled audience must be coordinated through the formal (R&A) process. Having information reviewed before it leaves SNL ensures that nothing classified is inadvertently released.

R&A must be the last step before public release. If a document is substantially modified after the review, it must be re-submitted. Typographical and grammar/syntax corrections are administrative and do not need to be re-submitted.
DOE’s “No Comment” policy states: “Information in the public domain (e.g., technical industry publications, conference papers, online news stories), must not be commented on if there is classified present, even if merely confirming the technical accuracy of the information.”

**Information does not automatically become unclassified simply because it is published in the public domain.**

If contacted, state only, “We do not comment on items in the public domain.”

**GEN-16** contains further information. Members of the Workforce are highly encouraged to read and be familiar with the policy.
Corporate Policies:
ISS100.1.1, Identify Classified Information
ISS100.1.2, Control Classified Matter
ISS100.1.5, Use Classified Matter

Read or Print the following handouts (at the end of this briefing):
GEN-16, DOE’s “No Comment” policy

For Help:
S&S-MAN-051, Classification Handbook for Derivative Classifiers
Records Management Manual
R&A Homepage

Security Connection: 505-845-1321 or 321 (from a Sandia phone)
Classification Office: NM and remote sites (505) 844-5574
CA (925) 294-2202
MODULE 3

THE CASE OF
THE
INTERRUPTION

A story of improper storage of classified information.
Case File

A Q-cleared individual was working on a classified document in his office in a limited area.

His neighbor called to tell him that his garage door was open. He left the office in a panic, closing the office door, but leaving the classified document on his desk.
What Went Wrong?

The individual had his normal routine interrupted because of the concern regarding his garage door being left open.

- Distractions/interruptions
- Change in routine
- Stress

How could this have been prevented?
THINK:
How do I protect classified matter when it is removed from its storage location?

ASSESS:
What are the security risks and consequences associated with not properly storing classified information?

PROTECT:
Know and understand what you can and cannot do regarding the proper storage and protection of classified information.

- Always store classified matter in a GSA-approved repository (i.e., Vault/VTR, GSA-approved safe).
- Have departmental discussions about what to do if a personal emergency arises.
- Use visual reminders when classified matter is in use (signage, door barriers, etc.).
- Distractions and interruptions are Human Performance Indicators that can lead to an increase in incidents of security concern.
Corporate Policies:
ISS100.1.1, Identify Classified Information
ISS100.1.2, Control Classified Matter
ISS100.1.5, Use Classified Matter

Read or Print the following handouts (at the end of this briefing):
Everything You Need to Know About Classified Understanding Classification

For Help:
S&S-MAN-013, Classified Work Station Manual

Security Connection: 505-845-1321 or 321 (from a Sandia phone)
MODULE 4

THE CASE OF THE POOR INTRODUCTIONS

A story of improper escorting.
Case File

A new, uncleared employee was escorted to a project meeting in a limited area conference room. The escort did not introduce the new individual or remind the attendees of the individual’s uncleared status. The host of the meeting did not remind the attendees to keep conversations unclassified.

A classified statement was made at the meeting in front of the uncleared employee.
What Went Wrong?

The escort and host failed to remind attendees that an uncleared individual was present.

A meeting participant made a classified statement in an area where classified meetings were common, but did not verify the clearance levels of other attendees.

How could this have been prevented?

- Changes in routine
- Unexpected conditions
THINK:
What are the clearance levels of the attendees? Is the room approved for classified discussions?

ASSESS:
What are the security risks and consequences associated with divulging classified information without verifying need to know (NTK)?

PROTECT:
Escorts should ensure measures are taken to prevent unauthorized disclosure of classified information.
Corporate Policies:
ISS100.5.3, Control Site Access

Read or Print the following handouts (at the end of this briefing):
Who and What Can Go Where?

For Help:
Security Connection: 505-845-1321 or 321 (from a Sandia phone)
MODULE 5

THE CASE OF THE CURIOUS COLLEAGUE

A story of counterintelligence.
Case File

A nuclear-weapons scientist believed that she had developed a new method to use a laser to initiate nuclear fusion. The laser fusion research was not supported by the program or her supervisors.

She made numerous attempts to gain access to other research projects and records for which she did not have a need to know (NTK). She received multiple security infractions and was eventually fired.

After an investigation, it was determined that she tried to sell her knowledge of the new laser method to a foreign government.
What Went Wrong?

The individual had access to classified and was disgruntled by the fact no one would support her research.

Managers and coworkers need to be mindful of when an employee changes their behavior because it could indicate a problem.

How could this have been prevented?

- Complacency
- Mindset
- Inaccurate risk perceptions
THINK:
Is a coworker attempting to gain access to research projects without appropriate authorization and NTK?

ASSESS:
Could sharing this information result in harm to our national security or damage Sandia’s reputation?

PROTECT:
Don’t share classified or sensitive unclassified information with someone who does not have proper access authorization and NTK.

- Report any and all suspicious behavior or activity immediately.
- You don’t have the right to see someone else’s information just because you have a clearance.
Corporate Policies:
IM100.1, Use and Protect Information Technology Resources
IM100.2.5, Identify and Protect Unclassified Information
ISS100.1, Perform Classified Work
ISS100.3.1, Report Personnel Security Information; Security Incidents; and Waste, Fraud, and Abuse
Executive Order 12333
DOE O 475.1, Counterintelligence Program

Read or Print the following handouts (at the end of this briefing):
Insider Threat PowerPoint

For Help:
Security Connection: 505-845-1321 or 321 (from a Sandia phone)
MODULE 6

THE CASE OF THE CHATTY TEAM

Case File

A team of Sandia researchers was working on an unclassified project that could have a major impact on fuel efficiency. Before the team could have its work published, a competitor announced that it had patented the same type of product and was ready to produce it to the mass market.

The Sandia team frequently posted about its work on Facebook, spoke to vendors about the progress, and skipped the formal Review and Approval (R&A) process for its publication.
What Went Wrong?

The team initially developing the project became lax regarding security.

Critical information about the project was not protected, allowing a competitor to steal the information shared by team members in the public domain.

- Complacency
- Inaccurate risk perceptions

How could this have been prevented?
THINK:
What information do you have that might be useful to anyone trying to gain access to Sandia’s information?

ASSESS:
Consider NTK before sharing critical information in public venues.

PROTECT:
Use the formal R&A process before sharing Sandia information in public venues, to external partners, or to large audiences.

- Whether your project is classified or not, always put in protections for your project’s critical information.
- Critical information is any information that may be useful to an adversary or competitor.
Corporate Policies:
IM100.3.4, Conduct Operations Security

Read or Print the following handouts (at the end of this briefing):
Critical Information List
Social Media Guidelines for Sandia National Labs

For Help:
Security Connection: 505-845-1321 or 321 (from a Sandia phone)
SECURITY AWARENESS UPDATES
UPDATE:

As allowed by DOE directive, SNL has begun to request Interim “Q” Security Clearances (ISCs) for individuals who occupy a position supporting a mission-essential program/critical position, as determined by executive leadership. NNSA may grant an ISC to an uncleared individual based on favorable completion of the required preliminary checks, pending completion of the full investigative requirements for the final clearance. A “Q” ISC allows a person to have access to collateral Secret Restricted Data (SRD) or lower (no caveats) while his/her final clearance is being processed.

Badges will not distinguish between those individuals with final clearances and those with an ISC.

Members of the Workforce (MOWs) with ISCs cannot have access to Top Secret matter and will not be considered for inclusion in the Human Reliability Program.

MOWs with ISCs may not have access to other programs or types of information (SIGMA, SCI, SAP, COMSEC, CRYPTO and NATO) unless authorized at the sole discretion of the office with authority for such access.

To learn more about Interim Clearances (ISCs) contact:

Security Connection: 505-845-1321 or 321.
UPDATE:
The “Classified Information Non-Disclosure Agreement, Standard Form 312” (SF-312) was revised in July 2013 by the Office of the Director of National Intelligence to conform with two new federal statutes: The Financial Services and General Government Appropriations Act (Public Law 112-74) and the Whistleblower Protection Enhancement Act (WPEA) (Public Law 112-199). The WPEA was enacted into law on November 27, 2012, and strengthens protections for federal employees who disclose evidence of waste, fraud or abuse. In addition, the WPEA modifies rules on the use of non-disclosures policies, forms, or agreements by government agencies.

If you have already signed an SF-312, you will not be required to sign another.

To learn more about SF-312 form updates contact: Security Connection 505-845-1321 or 321 (from a Sandia phone) or click here to view the form.
The data below summarize the most common incidents in the past four years. Most incidents involve the unauthorized disclosure, transmission, or improper storage of classified information.
Security Incident Data

**Requirement:** Ensure that work done in a Potentially Classified Subject Area (PCS) is reviewed by a Derivative Classifier (DC) prior to dissemination.

**Best Practices:** Before beginning a new project or creating a new document:

- Familiarize yourself with the sensitivities of the information.
- Engage a knowledgeable DC.
- Regularly review metagroups to limit access to individuals with a NTK.
- When in doubt, start the work on a classified network and use the Downshift Application.

**Corporate Procedure:** ISS100.1.1, *Identify Classified Information*
Security Incident Data

Requirements:
- **Mark** classified matter appropriately and use cover sheets to easily identify classified.
- **Store** classified matter in a GSA-approved safe or Vault-Type Room (VTR); ensure safes and VTRs are properly secured.
- **Store** documents only on electronic systems approved for the particular level and category of the information.
- **Understand** the protection requirements for sensitive information (e.g., Export Controlled Information).

Best Practices: Implement an end-of-day monitoring procedure to check for classified documents that may have been left out or classified computing systems that may be logged on.

Corporate Procedures:
- ISS100.1.1, Identify Classified Information
- ISS100.1.6, Store Classified Matter
- IM100.2.5, Identifying and Protecting OUO Information
Security Incident Data

Requirements:
- Know your audience.
- Verify that individuals have the appropriate clearance and NTK before sharing classified information.
- Verify that you are in the appropriate environment for classified discussions (e.g., the room is set up correctly and no electronic devices are present).

Best Practices:
- Verify the sensitivity of information you are sharing; if unsure, check with a knowledgeable DC.
- Uncleared individuals self-identify.
- Escorts announce un cleared individuals.
- Announce the classification level of a meeting prior to getting started.

Corporate Procedure: ISS100.1.1 - Identify Classified Information
**Common Causes of Incidents**

Task demands, individual capabilities, work environment, and human nature are just some of the Human Performance Indicators that can lead to an increase in Incidents of Security concern.

<table>
<thead>
<tr>
<th>Human Performance Indicators</th>
<th>Task Demands</th>
<th>Individual Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time pressure</td>
<td>Unfamiliarity w/ task / First time evolution</td>
<td>Lack of knowledge</td>
</tr>
<tr>
<td>High Workload</td>
<td>New technique not used before</td>
<td></td>
</tr>
<tr>
<td>Simultaneous, multiple tasks</td>
<td>Imprecise communication habits</td>
<td></td>
</tr>
<tr>
<td>Repetitive actions/ Monotony</td>
<td>Lack of proficiency / inexperience</td>
<td></td>
</tr>
<tr>
<td>Irrecoverable acts</td>
<td>Indistinct problem-solving skills</td>
<td></td>
</tr>
<tr>
<td>Interpretation of requirements</td>
<td>“Unsafe” attitude for critical tasks</td>
<td></td>
</tr>
<tr>
<td>Unclear goals, roles, and responsibilities</td>
<td>Illness / fatigue</td>
<td></td>
</tr>
<tr>
<td>Lack of or unclear standards</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Environment</th>
<th>Human Nature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distractions/Interruptions</td>
<td>Stress</td>
</tr>
<tr>
<td>Changes/Departures from routine</td>
<td>Habit patterns</td>
</tr>
<tr>
<td>Confusing displays or controls</td>
<td>Assumptions</td>
</tr>
<tr>
<td>Workarounds/OOS instruments</td>
<td>Complacency / Overconfidence</td>
</tr>
<tr>
<td>Hidden system response</td>
<td>Mind-set</td>
</tr>
<tr>
<td>Unexpected conditions</td>
<td>Inaccurate risk perception</td>
</tr>
<tr>
<td>Lack of alternative indication</td>
<td>Mental shortcuts (biases)</td>
</tr>
<tr>
<td>Personality conflicts</td>
<td>Limited short-term memory</td>
</tr>
</tbody>
</table>

Recognize when you’re at risk, step back, and regroup.
Your reporting responsibilities are outlined in the Corporate Policy below

**Corporate Procedure: ISS100.3.1 Report Personnel Security Information; Security Incidents; and Waste, Fraud, and Abuse**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Responsible Individual</th>
<th>Required Action</th>
</tr>
</thead>
</table>
| Report Security Related Concerns | Members of the Workforce         | **NOTE:** Do not discuss details of an incident via telephone, alphanumeric pager, email or voicemail. An IO or other Security professional will contact you. Immediately report the following:  
  - Security incidents (see: [DOE and Sandia Reporting Requirements](#)) to one of the following:  
    - Security Incident Reporting Pager at 505-283-SIMP (7467) (SN/NM) or the CA IO at 925-294-2600 (SNL/CA).  
    - Security Connection at 321 from an SNL phone or 505-845-1311 from non SNL phones. |
Your Responsibility

If you suspect you have caused an incident or witnessed one, report immediately.

If you can’t call, have someone report on your behalf.

Don’t discuss details on the phone.

Quick reporting can prevent a bigger incident.

SIMP is on-call 24 hours a day, 365 days a year.
Corporate Policies:
IM100.1.1, Identify Classified Information
ISS100.3.1, Report Personnel Security Information; Security Incidents; and Waste, Fraud, and Abuse

Read or Print Handouts (at the end of this briefing):
DOE and Sandia Reporting Requirements
Suspect/Counterfeit Items

For Help:
Security Connection: 505-845-1321 or 321 (from a Sandia phone)
Conclusion

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

Each 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 (R&A) process to avoid inadvertent disclosure of classified or sensitive information.
Understanding the security requirements of the area in which you are escorting.
Understanding how Human Performance Indicators can lead to an increase in incidents of security concern.

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

Our mission success depends on each and every one of us “protecting what is ours”.

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></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<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?
The purpose of the **Classification Program** is to identify information classified under the Atomic Energy Act or Executive Order (E.O.) 13526, so that it can be protected against unauthorized dissemination.

Corporate procedure ISS100.1.1, *Identify Classified Information*, contains much of what you’ll need to know when working with classified information at SNL. Below are some of the terms you’ll hear regarding classified information.

**Classified information** – Information that is classified by a statute or executive order.

**Classified matter** – 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>Restricted Data (RD)</th>
<th>Formerly Restricted Data (FRD)</th>
<th>Trans-classified Foreign Nuclear Information (TFNI)</th>
<th>National Security Information (NSI)</th>
<th>Degree of Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Secret (TS)</td>
<td>Q only</td>
<td>Q only</td>
<td>Q only</td>
<td>Q only</td>
<td>Exceptionally Grave</td>
</tr>
<tr>
<td>Secret (S)</td>
<td>Q only</td>
<td>Q and L</td>
<td>Q and L</td>
<td>Q and L</td>
<td>Serious</td>
</tr>
<tr>
<td>Confidential (C)</td>
<td>Q and L</td>
<td>Q and L</td>
<td>Q and L</td>
<td>Q and L</td>
<td>Undue</td>
</tr>
</tbody>
</table>

**Restricted Data (RD)**, all data concerning the design, manufacture, or use of nuclear weapons; production of special nuclear material; or use of special material in the production of energy.

**Formerly Restricted Data (FRD)**, classified information that relates primarily to the military utilization of atomic weapons. Examples of FRD include nuclear weapon stockpile issues, nuclear weapon yields and past and present weapon storage locations.

**Transclassified Foreign Nuclear Information (TFNI)**, deals with specific intelligence information concerning certain foreign nuclear programs removed from the RD designation by agreement between DOE and the Director of National Intelligence.

**National Security Information (NSI)**, information concerning all information concerning scientific, technological or economic matters relating to the national security; programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities of systems/installations; nonproliferation studies; foreign government information; and intelligence/counterintelligence information.

**Protecting and Controlling Classified Information and Matter**

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

**Information processed on a classified computing system** is considered classified at the system level and category (also known as “system high”) until it’s reviewed by an authorized DC. Such information should be marked and controlled appropriately until it has been reviewed for classification.

**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.
**EVERYTHING YOU NEED TO KNOW ABOUT CLASSIFIED**

<table>
<thead>
<tr>
<th><strong>Derivative Classifier (DC)</strong> – An individual authorized to confirm that an unmarked document or material is unclassified or determine that it is classified as allowed by his or her description of authority. Only trained DCs determine whether documents and material are classified, and to what level and category. DCs are trained on specific technologies/programs—what is not classified on one technology may be classified in other circumstances. Be sure to choose the right DC. You must request a DC review (i.e., an informal or programmatic review) for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A newly generated document or material in a classified subject area that may potentially contain classified information.</td>
</tr>
<tr>
<td>• An existing, unmarked document or material that you believe may contain classified information.</td>
</tr>
<tr>
<td>• An existing, marked document or material that you believe may contain information classified at a higher level or more restrictive category.</td>
</tr>
<tr>
<td>• A newly generated document that consists of a complete section (e.g., chapter, attachment, appendix) taken from another classified document.</td>
</tr>
<tr>
<td>• Printed output from a classified information system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Derivative Declassifier (DD)</strong> – An individual authorized to declassify or downgrade documents or material in specified areas, as allowed by his or her description of authority. DDs are located in the Classification Office. Declassification review must occur when:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prepared for declassification in full.</td>
</tr>
<tr>
<td>• Prepared as redacted versions.</td>
</tr>
<tr>
<td>• Requested under statute or Executive Order (i.e., declassification for public release).</td>
</tr>
<tr>
<td>• Referred to DOE by other government agencies that are marked or identified as potentially containing RD/FRD/TFNI or DOE NSI equities.</td>
</tr>
</tbody>
</table>

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

| **Classified Matter Protection and Control (CMPC)** – assists staff with questions regarding marking, protection, storage, and transmission of classified information, and serves as a resource for SNL’s CAS community. |

<table>
<thead>
<tr>
<th><strong>Classification Office</strong> – assists DCs and staff with classification decisions, and reviews information for public release. If you think a DC determination is incorrect, you have the right and are encouraged to challenge the classification status of information by contacting your site’s Classification Office.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNL/NM (505) 844-5574</td>
</tr>
<tr>
<td>SNL/CA (925) 294-2202</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>DOE Office of Classification</strong> - 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. Under no circumstances will you be subject to retribution for making such a challenge.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request information from <a href="mailto:outreach@hq.doe.gov">outreach@hq.doe.gov</a>.</td>
</tr>
</tbody>
</table>

**Get a formal review** if you intend to release information to an uncontrolled, widespread, unknown, or public audience. This includes information intended for release to Congress. You must obtain a formal Review and Approval (R&A).

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

Use **secure forms of telecommunication** (classified fax machine, copier and other electronic transmissions).

**If you see unattended classified matter**, secure it and report it to 321 from a Sandia phone or 505-845-1321 from any phone.
WHEN SHOULD YOU HAVE A DOCUMENT REVIEWED?
Documents must be reviewed before they are (1) finalized, (2) sent outside of the organization or working group on which you are serving, or (3) filed permanently. Prior to getting a review, you should protect and mark the document at the highest potential classification level, category, and caveat (Sigmas 14, 15, 18 and 20) of information that you believe is in the document.

Working papers and/or living documents are documents or drafts that are being revised frequently. These documents must have “Draft” or “Working Papers” on the front cover until final. They must also include classification markings for the highest potential classification level, category and caveat of the information you believe is in the document.

Regardless of type, a document must be reviewed and finalized no later than 180 days after creation, or in the case of working papers, 180 days after the last revision.

WHO IS AUTHORIZED TO CONDUCT CLASSIFICATION REVIEWS?
As required by DOE Order 475.2B, Identifying Classified Information, only Derivative Classifiers (DCs) may conduct a review of information for classification.

DCs must:
- Be trained in derivative classification.
- Be authorized in specific subject areas.
- Have access to current classification guidance for subject areas of authority.
- Be appointed by the local Classification Officer.

This brochure highlights your responsibilities for identifying classified information as per Department of Energy (DOE) Order 475.2B, Identifying Classified Information.

Classification is the process of identifying information that needs to be protected in the interest of national security. DOE has a formal process for classifying and declassifying information, documents, and materials.

As Members of the Workforce handling classified information, your primary responsibilities are to ensure that documents or materials you originate, modify, or possess in a classified subject area are reviewed by a Derivative Classifier.
WHAT INFORMATION IS CLASSIFIED?

DOE's classified information is primarily identified in the Atomic Energy Act (AEA), and in Executive Order (E.O.) 13526. In both law and E.O., the process of classification uses three levels (Top Secret, Secret, and Confidential) to define the severity of damage to national security. The information is further subdivided into different categories depending on the authority and rules used to handle the specific information.

The four categories are:

- **Restricted Data (RD)**, controlled by the AEA regarding information concerning design and manufacture of nuclear weapons, fissile materials, naval nuclear propulsion, and space power systems.

- **Formerly Restricted Data (FRD)**, also controlled by the AEA, relates primarily to the military utilization of nuclear weapons. Examples of FRD include nuclear weapon stockpile quantities, nuclear weapon delivery, nuclear weapon yields, and past and present weapon storage locations.

- **Transclassified Foreign Nuclear Information (TFNI)**, controlled by both the AEA and E.O. 13526, regarding specific intelligence information concerning certain foreign nuclear programs that is comparable to US RD or design-related CRD information.

- **National Security Information (NSI)**, controlled by E.O. 13526, is information concerning all other kinds of classified information. Examples of NSI include safeguarding of nuclear materials or facilities, vulnerabilities or capabilities of systems/installations, nonproliferation studies, foreign government information, and intelligence and counterintelligence information.

WHAT IS A CLASSIFIED SUBJECT AREA?

A classified subject area is a subject area for which a classification guide has been issued (e.g., nuclear assembly systems, safeguards and security, Strategic Petroleum Reserve). A classification guide indicates what specific information in a given subject area is classified.

At Sandia, common classified subject areas include:

**Areas Related to Weapons**
- Nuclear Weapon (NW) Production and Military Use
- NW Use Control
- NW Safing, Arming, Fuzing, and Firing
- NW Design of Nuclear Components
- NW Materials
- NW Vulnerability and Hardening
- NW Boosting and Transfer Systems
- NW Detonation Systems
- NW Initiators (Neutron Generators)
- NW Weapon Outputs
- NW Weapon Science
- Inertial Confinement Fusion
- Nuclear Explosion Monitoring
- Improvised Nuclear Devices
- Subcritical Experiments
- Fissile Material Disposition
- Chemical/Biological Defense Information
- Radiological Emergency Response
- Non-Nuclear Testing
- Nonproliferation of Weapon Information

**Areas Related to Security**
- Intelligence/Counterintelligence
- Transportation Safeguards System
- Safeguards and Security

**Weapon Programs**
- W76-0-1
- W80-1
- W84
- W88
- B61-7
- B61-12
- W78
- W80-4
- W87
- B61-3/4/10
- B61-11
- B83-1

WHAT ARE SOME “RED-FLAG” INDICATORS?

“Red-Flag” indicators can be used to take a proactive stance in preventing the release of classified information. You are encouraged to take an active role in helping to reduce occurrences by using the information topics on the checklist below as a reference to become aware of possible areas of security concern:

- Neutron generator (NG) design and performance details (NG timing, etc.)
- Timer/driver design and performance details
- Firing set design and performance details
- Gas transfer system design and performance details
- Fuzing/Height of Burst (HOB) design and performance details
- Weapon use control features
- Data and photos from lab or flight tests
- Critical weapon association concerns (including part and MC numbers)
- Unique materials used in weapon application
- Unfavorable statement about a component or a weapon
- Weapon performance or quality details
- Production issues or concerns
- Shipments schedules (dates or times)
- Weapon quantities
- Production quantities
- Weapon locations
- Weapon or component cutaways
- Component models or drawings
- Assembly models or drawings
- Radiation hardness levels
- Flight trajectories and profiles
- Weapon retirement dates
- Nicknames and code words
- Weapon outputs and testing
- Configuration of components within the weapon

If you are creating information in areas mentioned above (documents, emails, etc.), be sure to have a DC review prior to release!
GEN-16 Revision 2: "NO COMMENT" POLICY ON CLASSIFIED INFORMATION IN THE OPEN LITERATURE

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, 1(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.

[Signature]
Andrew P. Weston-Dawkes
Director
Office of Classification
Office of Environment, Health, Safety and Security
At Sandia and throughout the DOE complex, Tech Area or Technical Area is used to designate certain geographical areas, typically (but not always) enclosed by a fence. A Security Area refers to a physically defined space (identified by posted signs and some form of access control) containing special nuclear material, classified matter or property.

<table>
<thead>
<tr>
<th>WHO</th>
<th>General Access Area</th>
<th>Property Protection Area (PPA)</th>
<th>Limited Area (LA)</th>
<th>Vault Type Room (VTR)/SCIF/SAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q-cleared individual</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>L-cleared individual</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Uncleared individual w/SNL LSSO badge</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Children</td>
<td>✓</td>
<td>Only during certain special events with prior permission</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Friend (uncleared)</td>
<td>✓</td>
<td>Only during certain special events with prior permission</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Uncleared foreign national</td>
<td></td>
<td>Only in areas listed on their Foreign National Request Security Plan (FNR SP) for additional guidance contact your Center Security Coordinator or the Foreign Interaction Office (FIO).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WHAT</th>
<th>General Access Area</th>
<th>Property Protection Area (PPA)</th>
<th>Limited Area (LA)</th>
<th>Vault Type Room (VTR)/SCIF/SAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non Gov’t-owned Portable Electronic Devices (PEDs) (includes laptops)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>local restrictions may apply</td>
</tr>
<tr>
<td>Sandia-owned PEDs (blackberry w/credential, IPad, and IPhone)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AM/FM radio</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Electronic medical device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sandia-owned camera</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Personal weapons/fireworks</td>
<td>Prohibited Article</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alcohol</td>
<td>Prohibited Article</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medicinal marijuana</td>
<td>Prohibited Article</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Someone else’s prescription medication</td>
<td>Prohibited Article – if your drug test indicates the presence of a prescription medication, and you cannot produce a prescription in your name, you will be subject to disciplinary action which may include termination of employment.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See SNL Corporate policies or contact Security Connection @ 505-845-1321 for information regarding other electronic devices.

Posted local restrictions that are more limiting may apply. It is your responsibility to understand and follow those restrictions.
What is insider threat?

**INSIDER THREAT**

**Insider**: Any person with authorized access to Department of Energy (DOE) resources by virtue of employment, volunteer activities, or contractual relationship with DOE.

**Insider Threat**: The threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.
What does an insider threat look like?

2010 WikiLeaks. Private Chelsea (formerly Bradley) Manning leaked classified or unclassified but sensitive military and diplomatic documents to WikiLeaks. Manning was arrested in May 2010 and convicted in July 2013 of violations of the Espionage Act and sentenced to 35 years imprisonment.

2013 DOE. Pedro Leonardo Mascheroni, a former Los Alamos National Laboratory scientist in the nuclear weapons division, was convicted and sentenced to five years in prison for offering to help develop nuclear weapons for Venezuela. Mascheroni and his wife pled guilty in 2013 to offering to help develop a nuclear weapon for Venezuela through dealings with an undercover FBI agent posing as a representative of the socialist South American country.

2013 Washington Navy Yard Shooting. A Navy contractor with access, opened fire and killed 13 people and wounded three others. The gunman was killed by responding police officers. It was the second-deadliest mass murder on a U.S. military base, behind only the Fort Hood shooting.
It’s not just a **Security** issue.
It’s not just a **Cyber** issue.
It’s not just a **Counterintelligence** issue.
It’s not just a **Human Capital** issue.
It’s not just a **General Counsel** issue.
It’s not just an **Inspector General** issue.

And....

It’s not just something that happens somewhere else.

**It requires all offices and all employees working together.**

The complexity, time-sensitive, context-sensitive and time-dependent nature of determining if particular actions are indicators of potential or even actual insider threat activity demand a team effort.

An effective approach to detecting, deterring and mitigating insider threats will require a change in certain mindsets, cultures and values. **That change begins with you.**
Behavioral Concerns: A single indicator may say little; however, if taken together with other indicators, a pattern of behavior may be established.

- **Individual vulnerabilities** – i.e. repeated irresponsibility, violating rules, extreme immaturity, etc.
- **Extreme, persistent interpersonal difficulties** – i.e. being argumentative, rejection of social interaction, disruptive workplace behavior, etc.
- **Hostile or vindictive behavior** – i.e. verbal or physical threats, stalking type behavior, recurrent statements demonstrating bitterness or resentment, etc.
- **Unreported or concealed contacts** with foreign nationals, failure to report overseas travel, and/or repeated short leaves.
- **Exploitable conduct or behavior traits** – i.e. Financial trouble, alcohol or other substance abuse or dependence
- **Attempts to access information** not needed for a job or attempting to enter restricted areas
Not all of our surveillance equipment is electronic. You are the first line of defense against insider threats. Be aware of the actions of those around you. Report indicators of insider threat to:

Your Local Insider Threat Working Group (LITWG) representative at:
**Phone**: CI Hotline 505-284-3878  
**Email**: CI-Help@ Sandia.gov

Or the IG Hotline at:
**Phone**: 1-800-541-1625  
**Email**: IGHotline@hq.doe.gov

If you have any questions please contact the DOE Insider Threat Program Management Office (ITPMO) at ITPMO@hq.doe.gov.
Resource Links

- DOE Insider Threat Program
  https://itp.energy.gov/

- DOE Intelligence and Counterintelligence Forrestal Field Office
  https://in.doe.gov/

- National Counterintelligence and Security Center
  https://www.ncsc.gov/nittf/

- CERT Software Engineering Institute
  http://www.cert.org/insider-threat/

- National Insider Threat Special Interest Group
  http://www.nationalinsiderthreatsig.org/index.html

- Center for Development of Security Excellence
  http://www.cdse.edu/toolkits/insider/awareness.html
This document establishes guidelines for using external social media for personal use and work-related purposes at Sandia National Laboratories. These guidelines apply to all web postings and online activities that disclose information about Sandia National Laboratories business, employees, contractors, partners, or customers, whether on Sandia-controlled social media sites, personal sites, or others’ social media sites. The guidelines apply to all Sandia members of the workforce and other third parties who have been provided a Sandia email address.

Social media offer alternative channels for enhancing communication, increasing Sandia’s visibility, and reaching and engaging with targeted audiences, such as the news media, policy makers, potential employees, partners and collaborators, other stakeholders, and the general public.

However, those who use social media must understand that their online activities can have immediate, far-reaching, and lasting consequences. Because of its immediacy and broad reach, social media heighten the need to communicate responsibly and represent the Labs appropriately. All of Sandia’s established policies that govern how sensitive information is managed apply to social media. Activities or behaviors by Sandia personnel, whether on Sandia-controlled social networking sites or on the sites of others, are likely to be attributed not only to the individual but also to Sandia. Information posted on these sites, and on the Internet in general, can remain discoverable indefinitely.

Participation in social media is an individual choice. If you decide to participate, you are making a commitment to follow these guidelines and use good judgment in your online communications and behavior, even in situations not specifically addressed here.

PERSONAL USE OF ANY SOCIAL MEDIA

1. You are responsible for your postings. Your behavior on publicly accessible websites is a reflection on your character. If you identify yourself as a Sandian, it reflects on the Labs as well. If you wouldn’t want your manager or colleagues at Sandia to see your comments, it’s unwise to post them to the Internet. Be careful of any personal or government information you include in online profiles and use the strongest cautions in deciding what information to post unprotected. If you are identifying yourself as a Sandian on social networks, be aware of your obligations to information security and Sandia's reputation.

2. Your use of social media and publication of content on social media sites must comply with Sandia policies, Sandia/NTESS Code of Ethics and Standards of Conduct, and management direction. Corporate Policy Statements that are especially relevant to this policy include, but are not limited to:
   • Ethics & Business Conduct (CG100.4.1)
   • Intellectual Property (ME100.6.9)
   • Personal Use of Sandia Assets (IM100.1.1)
   • Communicate Outside the Laboratory (CG100.3.2)
   • Comply with Export/Import Control (CG100.10.6)
   • Information Management (IM100)
   • Manage and Protection Information (IM100.2)
   • Harassment-Free Workplace (HR100.5.5)
   • Protection of Sensitive Information (IM100.2.5)

3. Remember that you are not an official spokesperson for Sandia. If you discuss Sandia-related matters on a publicly accessible website, make it clear that your
opinions are your own and do not reflect the views of Sandia. The same holds true of conversations at a social gathering.

4. While you are not an official spokesperson, your status as a Sandia employee may become relevant to subject matter discussed in certain social forums. You should identify yourself as a member of the workforce if failing to do so could be misleading to readers or viewers. Members of the workforce should not engage in covert advocacy for Sandia.

5. If you are contacted by the media as a result of a Sandia-related online posting, refer the person to Media Relations (see CG100.3.2, Communicate Outside the Laboratory)

6. If in doubt, don’t send it out. If you’re about to publish something that makes you even the least bit uncomfortable, take a moment to review it and try to figure out what’s bothering you. Alternately, ask a colleague or manager to review it. Remember, what you publish is your responsibility and will be discoverable for a long time. Make sure you’re comfortable with it.

7. Respect copyrights. Recognize and respect others' intellectual property rights, including copyrights. While certain limited use of third-party materials may be OK, it is still advisable to get the owner's permission. This includes songs and film clips that might be included in a video.

8. Remember that linking to content, such as video, from a blog or posting may be perceived as endorsing that content. Link responsibly.

9. Remember your day job. Make sure that your online activities do not interfere with your job or work commitments. Proper time charging practices must be followed when using social media during work hours.

10. An increased online presence means a potentially increased exposure to hackers and foreign agents. Be vigilant of potential attempts to improperly solicit information and refer any suspicious activities to Counterintelligence (http://info.sandia.gov/ci/)

Sandia maintains an official corporate presence, owned by Media Relations and Communications, on several social networking sites such as Twitter, YouTube, Flickr, Facebook, and LinkedIn. Authorized Sandia employees in Media Relations and Communications maintain these sites on behalf of Sandia. These sites offer alternative channels for increasing Sandia’s visibility and reaching and engaging with targeted audiences, such as the news media, potential new hires, and the general public.

Granting or permitting exceptions or violations of policy, process, or procedure without authority, regardless of position or title, may be cause for disciplinary action up to and including termination of employment. Violating a policy, process, or procedure may be cause for disciplinary action up to and including termination of employment.
OPSEC Critical Information applies to SNL/NM, SNL/CA, and SNL/TTR as indicated by their respective OPSEC Coordinators. Sites and organizations (divisions, centers, departments, and/or programs) should use this list as a baseline for creating their own CIL.

**OPSEC Critical Information** is: Specific facts about friendly (e.g., U.S., SNL) 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.

- Essential to the success of an operation, mission, or project.
- What the adversary vitally needs to defeat us or damage our interests.

Think about what is critical to the adversary, as well as your organization. Adversaries are defined in the **OPSEC Threat Analysis Document**. For more information, refer to the document.

The table below is the General CIL and applies to SNL programs and activities.

<table>
<thead>
<tr>
<th>General Critical Information</th>
<th>Purchasing/procurement, vendors, shipping, and receiving requests</th>
<th>Scope and type of work conducted</th>
<th>Financial, budget, accounting, and contract information</th>
<th>Shipment details for sensitive materials</th>
<th>Network information</th>
<th>User name and passwords</th>
<th>Program/project and personnel relationships</th>
<th>Work schedules and staffing changes/reports, milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application of new technology, new uses of older technology</td>
<td>Diagrams, blueprints, and schematics</td>
<td>Emergency response, tactics, techniques, and procedures</td>
<td>Facilities, buildings, and construction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capabilities and limitations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical infrastructure and key resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current and future operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication methods</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical job details, roles, and responsibilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dates, times, locations, and events (tests, exercises, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Disclaimer**: OPSEC Critical Information listed here may not be all inclusive. Sensitive programs and activities must be review their CIL on a recurring basis. Recommendations/changes for newly identified or deleting old critical information made to managers (and the OPSEC Program Office). If the release of critical information can cause harm to Sandia National Laboratories’ programs, activities, customers, or resources, then it must be protected from inadvertent release, even if it is not on this or any other CIL.

**IMPORTANT NOTICE**: A printed copy of this document may not be the document currently in effect. The official version is located on the OPSEC Program website.
# 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."

—Executive Order 12968, Access to Classified Information

---

### Other Reporting Requirements

| 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). |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Waste, Fraud, &amp; Abuse (WFA)</td>
<td>Report incidents of WFA and criminal matters to Ethics Advisory &amp; Investigative Services (505-845-9900) and other appropriate authorities (e.g., manager, security officials). Alternatively, for WFA incidents, you may email the Office of Inspector General directly, or call 800-541-1625.</td>
</tr>
</tbody>
</table>
| Theft of Property | Immediately report any theft of Sandia or U.S. Government property to Property Management (loststolen@sandia.gov).  
**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.
<table>
<thead>
<tr>
<th>Concerns of Personnel Security Interest</th>
<th>If you...</th>
<th>Report to...</th>
<th>By this date...</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Rqmts</td>
<td></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>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>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Clearance Processing (925-294-2061)</td>
<td>Immediately.</td>
</tr>
<tr>
<td>Legal Issues</td>
<td></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.</em>*</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Clearance Processing (925-294-2061)</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. **See exception noted below.</td>
</tr>
<tr>
<td><em>Have your wages garnished for ANY reason. Examples: divorce, debts, child support.</em>*</td>
<td>NM—Personnel Security Info Line (505-284-3103) CA—Clearance Processing (925-294-2061)</td>
<td>NM—Personnel Security Info Line (505-284-3103) 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>Have a foreign citizen who changes citizenship.</em>*</td>
<td>NM—Foreign Interactions (505-844-8263) CA—Foreign Interactions (925-294-2061)</td>
<td>NM—Foreign Interactions (505-844-8263) CA—Foreign Interactions (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>Change citizenship or acquire dual citizenship.</em>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citizenship</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Have legal action resulting in a name change.</em>*</td>
<td>Personnel Security Info Line (505-284-3103)</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><em>Marry or cohabitate with a person.</em>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Life Circumstances</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Are hospitalized for mental health reasons.</em>*</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Clearance Processing (925-294-2061)</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>Are treated for drug or alcohol abuse.</em>*</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Clearance Processing (925-294-2061)</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>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>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>Foreign Travel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have personal foreign travel to a <strong>sensitive</strong> country. <strong>Note:</strong> Although you are not required to report travel to a <strong>non-sensitive</strong> 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>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 <strong>any</strong> foreign national.</td>
<td>NM—Counterintelligence (505-284-3878) CA—Counterintelligence (925-294-1362)</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>Foreign Interaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>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.</em>*</td>
<td>NM—Counterintelligence (505-284-3878) CA—Counterintelligence (925-294-1362)</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><em>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.)</em>*</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Personnel Security (925-294-2061)</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Personnel Security (925-294-2061)</td>
<td>Immediately.</td>
</tr>
</tbody>
</table>

* Although every circumstance cited above must be reported, asterisked items may be reported directly to DOE Personnel Security rather than the listed SNL organization.
Case Description

An employee ordered replacement USB chargers from an online source. Upon receipt of the replacement chargers the employee did not perform any inspection activities and immediately provided the chargers to multiple co-workers within the department.

One of the individuals who received a charger had completed suspect/counterfeit items training and noticed right away that the item had some strange markings. The individual knew to review critical markings such as Nationally Recognized Testing Laboratory (NRTL) markings and noticed right away that the item stated “USTED” where it would typically state “LISTED”. The individual reported the device to the Suspect/Counterfeit Items Program Coordinator at sqasci@sandia.gov. Upon further investigation by the Coordinator, the item was determined to be counterfeit. Communications directing all recipients of the counterfeit charger to discontinue use were immediately issued.

At the same time, on the other side of the laboratory, another individual who received the counterfeit charger decided to use the item and plugged the provided USB cable into a Sandia Owned Computer. The individual did not have Suspect/Counterfeit Items training and did not perform inspection of the item. It wasn’t long until they began to have computer issues. Soon after, the individual received the call to immediately discontinue use of the item but not before it was too late. The damage had been done!

What could have been done differently?

- **Source of Supply:** The chargers could have been ordered directly from a manufacturer or an authorized distributor instead of from the online source (this aids in reducing the likelihood of receiving a counterfeit product)
- **Inspection or Validation:** The employee who ordered and distributed the items could have performed a quick visual inspection and may have noticed some of the odd markings before distributing them to their department
- **Awareness and Training:** The employee who used the charger and cable did not have basic suspect/counterfeit awareness training and did not know what indications might suggest that the item may be counterfeit

Resources:

- **Corporate Policy:** [SCM100.3.13](#), Manage Suspect or Counterfeit Items
- **Suspect/Counterfeit Items Coordinator Email:** sqasci@sandia.gov (use to report items or ask questions)
- **Suspect/Counterfeit Items Webpage:** counterfeit.sandia.gov (information and ability to report items)
- **SCA050**, Suspect/Counterfeit Awareness (Online in TEDS-15 minutes) recommended for all employees and contractors.
- **SCA0100**, Introduction to Suspect/Counterfeit Items (In Class- 4 hours) recommended for Procurement, Requesters, Sandia Delegated Representatives, Electrical workers, Pressure workers, Installers, Maintenance/ Facilities, Craft, Fleet, Inspection, and Managers
- **SCA0200**, Suspect/Counterfeit Item in Electronics and Microelectronics (In Class- 3 hours) recommended for all employees who work with electronics in product or research and development projects.