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-18)**

- **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.
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
INTERUPTION

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.

- Obtain, read, and possess a yellow “Security Notice” card, and act accordingly.
- Understand and follow any local/site-specific requirements.
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.

- Complacency
- Mindset
- Inaccurate risk perceptions

How could this have been prevented?
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.

How could this have been prevented?

- Complacency
- Inaccurate risk perceptions
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.

Total Recordable Incidents of Security Concern FY14-FY17

FY14: 174
FY15: 171
FY16: 190
FY17: 149

ECI - Export Controlled Information
NNPI - Naval Nuclear Propulsion Information
UCNI - Unclassified Controlled Nuclear Information
Security Incident Data

**Requirement:** Ensure that work done in a Potentially Classified Subject Area (PCSA) 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 unclesed 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.

| Human Performance Indicators          |  |
|---------------------------------------|  |
| Task Demands                          | Individual Capabilities              |
| ◢ Time pressure                        | ◢ Unfamiliarity w/ task / First time evolution |
| ◢ High Workload                        | ◢ Lack of knowledge                   |
| ◢ Simultaneous, multiple tasks         | ◢ New technique not used before       |
| ◢ Repetitive actions/ Monotony         | ◢ Imprecise communication habits      |
| ◢ Irrecoverable acts                  | ◢ Lack of proficiency / inexperience |
| ◢ Interpretation of requirements       | ◢ Indistinct problem-solving skills   |
| ◢ Unclear goals, roles, and responsibilities | ◢ “Unsafe” attitude for critical tasks |
| ◢ Lack of or unclear standards         | ◢ Illness / fatigue                   |
| Work Environment                      | Human Nature                          |
| ◢ Distractions/interruptions           | ◢ Stress                              |
| ◢ Changes/Departures from routine      | ◢ Habit patterns                       |
| ◢ Confusing displays or controls       | ◢ Assumptions                          |
| ◢ Workarounds/OOS instruments          | ◢ Complacency / Overconfidence        |
| ◢ Hidden system response               | ◢ Mind-set                             |
| ◢ Unexpected conditions                | ◢ Inaccurate risk perception           |
| ◢ Lack of alternative indication       | ◢ Mental shortcuts (biases)            |
| ◢ Personality conflicts                | ◢ Limited short-term memory            |

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

Click [here](#) to link to the policy.

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 505-845-1321 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:**
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>
<tr>
<td>SNL Org # or Company Name:</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

- ☐ Employee  ☐ Contractor  ☐ Consultant  ☐ Student  ☐ KMP

<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.
The organization of the information presented.
The usefulness of the information presented.
Your level of knowledge related to this topic BEFORE using this learning tool.
Your level of knowledge related to this topic AFTER using this learning tool.

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?