Hi. I’m Kellie and with my extensive experience and passion for Safeguards and Security I’ll be your guide for the Annual Security Refresher Briefing. In this briefing, we will review some common incidents that have occurred this year.

We have provided resource documents that include information and guidance to ensure you meet the DOE and Sandia requirements for Safeguards and Security.
I’m Gabby Holcomb, a Quality Assurance Specialist with Sandia’s Suspect and Counterfeit Parts Program.

I am also a former Army civil affairs sergeant. I am a proud veteran and a proud Sandian and that’s why security is important to me.

The work I do and the work you do is crucial to mission success at this laboratory.

Military personnel use the technology developed here at Sandia to help ensure global peace, achieve their objectives, and get back home to their families.

Adversaries are looking to gain access to information that could compromise those efforts. At Sandia, information security is key to protecting our nation’s assets, the mission and our men and women in uniform.

This year, the Annual Security Refresher Briefing will focus on our responsibilities to protect information and ensure we all Protect What Is Ours. Thank you.
Course Objective:

Reinforce DOE and Sandia security duties and responsibilities related to physical and logical access to unclassified or classified information or matter through scenarios and resource documents to reduce the threat and address the biggest operational concerns associated with working at this laboratory.
INCIDENTS OF SECURITY CONCERN (IOSC) AT SANDIA

<table>
<thead>
<tr>
<th></th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>CATEGORY A</td>
<td>48.98</td>
<td>42.00</td>
</tr>
<tr>
<td>CATEGORY B</td>
<td>131.00</td>
<td>118.00</td>
</tr>
</tbody>
</table>

**Category A:** may involve the loss, theft, suspected compromise, or compromise of departmental assets.

**Category B:** may involve failure to adhere to security procedures where the likelihood of compromise is remote or not suspected.
COURSE MODULES

IMPROPER PROTECTION OF UNCLASSIFIED CONTROLLED INFORMATION (UCI)

IMPROPER STORE OF CLASSIFIED

UNAUTHORIZED DISCLOSURE OF CLASSIFIED

UNAUTHORIZED NETWORK-BASED TRANSMISSION

COUNTERINTELLIGENCE UPDATE

SAFEGUARDS AND SECURITY UPDATE
Approximately 4% of Incidents of Security Concern (IOSCs) are a result of sensitive UCI not being protected according to DOE storage and protection requirements.
THE BARBEQUE

Friday evening, Chris realizes he accidentally brought home some Official Use Only Ex. 3 (Export Controlled Information) documents. He puts them on his kitchen table to remind himself to take them back to work on Monday.

Chris had some friends over for a barbecue. Monday morning he sees the documents and realizes they were not properly stored.

What Must Chris Do?

- Chris trusts his friends. He should just bring the papers back to work.
- Chris must call the Security Incident Management Program (SIMP) to report that his friends might have seen the documents.
THE BARBEQUE

Friday evening, Chris realizes he accidentally brought home some Official Use Only Ex. 3 (Export Controlled Information) documents. He puts them on his kitchen table to remind himself to take them back to work on Monday.

Chris had some friends over for a barbecue. Monday morning he sees the documents and realizes they were not properly stored.

What Must Chris Do?

- Chris trusts his friends. He should just bring the papers back to work.
- Chris must call the Security Incident Management Program (SIMP) to report that his friends might have seen the documents.
THE BARBEQUE

A SIMP inquiry was conducted and determined that Chris did not store the document properly and it could have been accessed by individuals that did not meet access requirements for OUO Ex. 3 ECI.

Chris received an incident for improper protection of sensitive UCI. He returned the documents to Sandia and reviewed the laboratory policies for OUO and ECI to understand his security responsibilities for preventing unauthorized access.
Did You Know?

You are required to ensure UCI is protected from being accessed by individuals who do not meet all requirements for accessing that information (e.g., Need To Know [NTK]).
Think

What are the protection requirements when I take a document outside of Sandia?

Assess

- If I am working with UCI outside of Sandia, can anyone around me see or hear the information?
- While I am not working on it, is it stored in a way where no one can access it?

Protect

- Control access at all times.
- Lock it in a container, desk, or cabinet.
- Don’t leave it in a briefcase, bag, or a folder, etc.

- UCI Handout
- National Security and You Brochure
- IT017 Official Use Only Information Policy
- IT022 Export Controlled Information (ECI) Policy
Unclassified Controlled Information

Unclassified Controlled Information (UCI) - information which disclosure, loss, misuse, alteration, or destruction could adversely affect national security, Sandia National Laboratories, or our business partners. It is the policy of DOE and Sandia to conduct as much research and development on an unclassified basis as possible to promote the free exchange of ideas, which is essential to scientific and industrial progress. DOE and other federal agencies require controls on the availability of certain scientific and technical information, classified or unclassified.

First, determine if your information is:

- Sandia-owned = Sandia Propriety
- U.S. Government-owned

Then, based on content, what type of proprietary information it is:

- Employment Related Records
- Confidential Financial/ Honeywell International Correspondence
- Procurement Actions
- Legal Records
- Technology Transfer

Such as:
- IP license agreements
- Protected CRADA Information
- Certain Intellectual property

Then, based on content/sponsor, what type of information it is:

- OUO
- UCNI
- SGI
- U-NNPI
- Other U.S. Gov’t Agency

PIE exemptions must commonly used at Sandia are 3-7

Personally Identifiable Information (PII) can apply to both U.S. government-owned and Sandia-owned information

Unclassified Controlled Information (IT012 - Unclassified Controlled Information Policy)

OUO is U.S. Government-owned unclassified information that is exempt from public release under the FOIA (Freedom of Information Act) and has the potential to damage government, commercial or private interests if disseminated to persons without a NTK. Your Derivative Classifier should have guides that include OUO topics relevant to your organization’s work. Members of the workforce should identify which subjects, programs, processes, documents, emails, slideshow presentations, faxes, or any other forms within your organization or programs have the potential to include OUO information. Once a document is identified as OUO, a FOIA exemption must be selected and applied to your information.

<table>
<thead>
<tr>
<th>FOIA Exemption</th>
<th>Category Name</th>
<th>What it Protects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exemption 1</td>
<td>Classified</td>
<td>NEVER used for OUO. It is only used for classified information</td>
</tr>
<tr>
<td>Exemption 2</td>
<td>Circumvention of Statute</td>
<td>No Longer Applicable for DOE &amp; SNL</td>
</tr>
<tr>
<td>Exemption 3</td>
<td>Statutory Exemption</td>
<td>Information whose disclosure is specifically protected by law and not otherwise controlled</td>
</tr>
<tr>
<td>Exemption 4</td>
<td>Commercial/Proprietary</td>
<td>Trade secrets, commercial or financial information, if released could impair the government's ability to obtain information in the future.</td>
</tr>
<tr>
<td>Exemption 5</td>
<td>Privileged Information</td>
<td>Intergency or intra-agency memos or letters not available by law to a party unless the party is in litigation with the agency</td>
</tr>
<tr>
<td>Exemption 6</td>
<td>Personal Privacy</td>
<td>Information that could cause an individual personal distress or embarrassment, or expose them to identity theft</td>
</tr>
<tr>
<td>Exemption 7</td>
<td>Law Enforcement</td>
<td>Information that if released could endanger the life or physical safety or disclose techniques and procedures for law enforcement investigations or prosecutions</td>
</tr>
<tr>
<td>Exemption 8</td>
<td>Financial Institutions</td>
<td>Evaluation of a financial institution’s stability</td>
</tr>
<tr>
<td>Exemption 9</td>
<td>Wells</td>
<td>Geological and geophysical information and data, resource maps, and new drilling techniques</td>
</tr>
</tbody>
</table>

FOIA exemptions most commonly used at Sandia are 3 - 7

Email

Protect and properly mark email containing UCI by using an approved encryption method, such as Entrust or other FIPS 140-2 compliant methods found in Laboratory Policy IT012 to avoid security incidents for improper transmission of UCN1, U-NNPI, and OUO Exemption 3.

Sandia has an email marking assistant tool to properly mark emails before sending outside the sandia.gov domain. Contact Security Connection for assistance.

CALL SECURITY CONNECTION AT 505-845-1321
Security Violations We've Seen
(We Can't Make This Stuff Up, Folks!)

- An employee’s husband wanted to surprise her on her birthday by putting a new smart phone in her lunch bag. She was definitely surprised when she realized that she had brought a controlled article into an area where it wasn’t allowed.
- An employee’s wife got him a subscription to a beer-of-the-month club and used his office address for delivery to avoid having the beers sitting on his doorstep at home in all kinds of weather. (Alcohol is a prohibited article.)
- A contractor brought an electronic picture frame into a limited area, wrapped as a Secret Santa gift for a department gift exchange. (Electronic devices of any type that have internal memory are controlled articles.)
- A member of the workforce arranged for an FBI agent to enter a restricted area based on the agent’s contention that her FBI credentials were sufficient to access the lab. (All persons must have a DOE-approved badge to access security areas at SNL.)
- A worker with a concealed-carry permit (which allows him to carry a concealed firearm in Albuquerque) forgot that he was wearing his firearm when he stopped by his office on a Saturday afternoon. (Personal firearms are prohibited articles.)
- A new employee brought his family on site to see his office. (All persons in SNL’s security areas must be properly badged and have a business reason for accessing the site.)

OPSEC: A Tool You Already Use

Operations Security, or OPSEC, is a way of protecting information. By thinking about our information, assessing vulnerabilities, and implementing protections, we protect ourselves and our information.

At home, for example, you avoid putting too much information about yourself on Facebook—you wouldn’t post your Social Security number or the dates when you will be on vacation. That’s OPSEC. You also wouldn’t tell someone you just met all of your personal details. That, too, is OPSEC. Because there’s a risk, you’re careful about how much information you share with others.

In the same way, we ask that you not share details about your Sandia friends or family members. It’s okay to say they work at the Labs and what their job title is, but details about their projects or mentioning that their work is classified can make them a target for espionage.

Apply OPSEC, or as we say around here:

Think. Assess. Protect.

National Security & You

A Family Guide to Security at Sandia National Laboratories

12/2012

Helping Your Friend or Family Member

Information Protection

When people receive security clearances, they’re required to sign a non-disclosure agreement, essentially a promise to never reveal classified information. They also receive training on how to protect certain types of unclassified information.

You can help by understanding that clearance holders can’t talk about certain things:
- Information can only be shared with people who have a need-to-know.
- Even unclassified information may need to be protected—it may be sensitive or it could lead an adversary to classified data.

Reporting Requirements

People who have security clearances are required to report certain things, including personal information.

You can help by reminding your friends or family members when they become aware of a reportable circumstance. Some common things that need to be reported are:
- Traffic fines of $500 or more
- Detention by law enforcement
- Contact with foreign nationals
- Foreign travel
- Cohabitation
- Marriage
- Bankruptcy

A comprehensive list of things that must be reported is available at:

Prohibited and Controlled Articles

Some items, such as illegal drugs and dangerous weapons, are designated as prohibited articles and are not allowed at the Labs. Others, called controlled articles, aren’t allowed in certain areas or only with prior approval. Typically, these are electronic devices that can capture or transmit information, such as computers, cell phones, or cameras.

You can help by:
- Not putting prohibited/controlled items in briefcases, purses, etc.
- Reminding your family member to avoid common pitfalls like distractions (e.g., interruptions while preparing to leave for work), time pressures (e.g., running late), or altered routines (e.g., taking the bus instead of driving).

Doing Your Part

If you have questions about security at the Labs, we welcome your call. More importantly, if you see something that just doesn’t seem right, let us know. Contact the Security Connection hotline at (505) 845-1321.

National Security & You

Does someone you know work at Sandia National Laboratories? If so, you too have a role in security.

A Family Guide to Security at Sandia National Laboratories

12/2012

A comprehensive list of things that must be reported is available at:

Prohibited and Controlled Articles

Some items, such as illegal drugs and dangerous weapons, are designated as prohibited articles and are not allowed at the Labs. Others, called controlled articles, aren’t allowed in certain areas or only with prior approval. Typically, these are electronic devices that can capture or transmit information, such as computers, cell phones, or cameras.

You can help by:
- Not putting prohibited/controlled items in briefcases, purses, etc.
- Reminding your family member to avoid common pitfalls like distractions (e.g., interruptions while preparing to leave for work), time pressures (e.g., running late), or altered routines (e.g., taking the bus instead of driving).

Doing Your Part

If you have questions about security at the Labs, we welcome your call. More importantly, if you see something that just doesn’t seem right, let us know. Contact the Security Connection hotline at (505) 845-1321.
COURSE MODULES

- Improper Protection of Unclassified Controlled Information (UCI)
- Improper Storage of Classified
- Unauthorized Disclosure of Classified
- Unauthorized Network-Based Transmission
- Counterintelligence Update
- Safeguards & Security Update
Approximately 25% of IOSCs are a result of classified matter not being stored according to DOE storage and protection requirements.
OUT TO LUNCH

Pat gets an email from Password Administration to pick up a Sandia Classified Network password.

Pat picks up the SCN password and heads back to her office. Pat gets distracted by a coworker’s invitation to lunch, locks the password in a drawer and leaves the office for lunch.

What Must Pat Do?

- Pat is pretty sure that no one saw the password that she left unattended. She should just forget it and go to work.
- Pat must contact the Security Incident Management Program (SIMP) to report that she left the classified password unattended.
OUT TO LUNCH

Pat gets an email from Password Administration to pick up a Sandia Classified Network password.

Pat picks up the SCN password and heads back to her office. Pat gets distracted by a coworker’s invitation to lunch, locks the password in a drawer and leaves the office for lunch.

What Must Pat Do?

- Pat is pretty sure that no one saw the password that she left unattended. She should just forget it and go to work.
- Pat must contact the Security Incident Management Program (SIMP) to report that she left the classified password unattended.
A SIMP inquiry was conducted and determined that Pat’s SCN password could have been accessed by unauthorized individuals while she was at lunch.

Pat received an incident for the improper storage of classified. She immediately changed the potentially compromised SCN password and now works closely with a Classified Administrative Specialist to secure all classified.
Did You Know?

You can work with your Classified Administrative Specialist (CAS) to identify approved storage locations for classified.
Think

Do I understand proper storage requirements for classified?

Assess

Do I have access to an approved storage repository for classified (safe or vault type room)?

If not, have I coordinated proper storage with someone who does?

Protect

Protect and store classified passwords at the highest classification to which they grant access (e.g., Sandia Classified Network [SCN] passwords as Secret Restricted Data [SRD]).

- Reporting Requirements
- Getting Started With Classified
- SS003 Classified Matter Protection and Control (CMPC) Policy
- IT002 Use Sandia’s Information Technology Resources Policy
<table>
<thead>
<tr>
<th>Other Reporting Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incidents of Security</strong></td>
</tr>
<tr>
<td>Concern; i.e. Security</td>
</tr>
<tr>
<td>Incidents</td>
</tr>
<tr>
<td>Report immediately, but do not provide details over the phone.</td>
</tr>
<tr>
<td>NM: Security Connection (321)</td>
</tr>
<tr>
<td>CA: Security Connection (321) or SIMP (925-294-2600)</td>
</tr>
<tr>
<td>Note: Contractors must also report incidents to their Facility Security Officers.</td>
</tr>
<tr>
<td><strong>Waste, Fraud, &amp; Abuse</strong></td>
</tr>
<tr>
<td>(WFA)</td>
</tr>
<tr>
<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>
<tr>
<td><strong>Counterfeit/ Suspect Items</strong></td>
</tr>
<tr>
<td>Upon discovery of suspect or counterfeit items, report the circumstance or submit questions to <a href="mailto:sqasci@sandia.gov">sqasci@sandia.gov</a>, or via counterfeit.sandia.gov.</td>
</tr>
<tr>
<td><strong>Theft of Property</strong></td>
</tr>
<tr>
<td>Immediately report any theft of Sandie or U.S. Government property to Property Management (<a href="mailto:bostolen@sandia.gov">bostolen@sandia.gov</a>).</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>Wrongdoing</strong></td>
</tr>
<tr>
<td>Report incidents of wrongdoing to Ethics (505-845-9900).</td>
</tr>
<tr>
<td>Note:</td>
</tr>
<tr>
<td>* Incidents of wrongdoing are not limited to items listed elsewhere herein.</td>
</tr>
<tr>
<td>* You may also report directly to the Office of Inspector General.</td>
</tr>
<tr>
<td><strong>Drug Use</strong></td>
</tr>
<tr>
<td>Report the following to Ethics at 505-845-9900:</td>
</tr>
<tr>
<td>* Positive drug test results (regardless of source [e.g., court system and military testing])</td>
</tr>
<tr>
<td>* Incidents of illegal drugs in the workplace. This includes trafficking in, selling, transforming, possessing, or using illegal drugs.</td>
</tr>
<tr>
<td>Note:</td>
</tr>
<tr>
<td>* Illegal drugs are prohibited on Sandia-controlled premises and KAFB property.</td>
</tr>
<tr>
<td>* 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.</td>
</tr>
</tbody>
</table>

**Managers**

Managers are responsible for immediately reporting to Personnel Security (NM: 505-845-9355, CA: 925-294-1356) when an employee's clearance is no longer required. Employment is terminated, individual is on extended leave of 30 calendar days or more, or access authorization is not required for 30 calendar days or more. Ensure DOE F 5621.29, Security Termination Statement, and badges are immediately delivered to the Clearance Office.

**Remote Sites Personnel**

Report to SNL/MM, 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.

---

**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
## Concerns of Personnel Security Interest

<table>
<thead>
<tr>
<th>If you...</th>
<th>Report to...</th>
<th>By this date...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Concerns</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are approached or contacted by ANY individual seeking unauthorized access to classified material or special nuclear material (SNM).</td>
<td>Counterintelligence (505-284-3878)</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, relevant, and create a question as to the individual’s access authorization eligibility.</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Clearance Processing (925-294-2061)</td>
<td>Immediately.</td>
</tr>
<tr>
<td><em>Are arrested; subject to criminal charges (including charges that are dismissed), receive citations, tickets, or summons; 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>Orally within 2 work days of occurrence, and in writing within the next 3 work days. <strong>See exception noted below.</strong></td>
</tr>
<tr>
<td><strong>Legal Issues</strong></td>
<td><strong>Exception:</strong> Traffic citations/tickets/lines are reportable only if they exceed $300 and only when the fine is assessed, unless drugs or alcohol were involved (Assessed means you agree to pay or go to court and the court’s ruling equals a fine above $300. Court fees or other administrative costs associated with the traffic citation/ticket/line should not be added to the final assessed amount.)</td>
<td></td>
</tr>
<tr>
<td><em>File for bankruptcy, regardless of whether it is for personal or business-related reasons.</em></td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and in writing within the next 3 work days.</td>
</tr>
<tr>
<td><em>Have your wages garnished for ANY reason. Examples: divorce, debts, child support.</em></td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and in writing within the next 3 work days.</td>
</tr>
<tr>
<td><em>Change citizenship or acquire dual citizenship.</em></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>Are a foreign citizen who changes citizenship.</em></td>
<td>NM—Foreign Interactions (505-844-6263) 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><strong>Citizenship</strong></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>Orally within 2 work days of occurrence, and in writing within the next 3 work days (via SF 2730-NCR).</td>
</tr>
<tr>
<td>Marry or cohabitate with a person.</td>
<td>Personnel Security Info Line (505-284-3103)</td>
<td>In writing within 45 days of marriage or cohabitation (via DOE F 5631.34).</td>
</tr>
<tr>
<td><strong>Note:</strong> A cohabitant is a person who lives with the individual in a spouse-like relationship or with a similar bond of affection or obligation, but is not the individual’s legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.).</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>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>Orally within 2 work days of occurrence, and in writing within the next 3 work days.</td>
</tr>
<tr>
<td><em>Use an illegal drug or a legal drug in a manner that deviates from approved medical direction.</em></td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and in writing within the next 3 work days.</td>
</tr>
<tr>
<td>No longer require your clearance, terminate employment; are on extended leave of 50 calendar days or more; or access authorization isn’t re-credited for 90 calendar days or more.</td>
<td>NM—Personnel Security Info Line (505-284-3103) CA—Clearance Processing (925-294-2061)</td>
<td>Immediately and follow up by providing completed DOE F 5631.29.</td>
</tr>
<tr>
<td><strong>Foreign Travel</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have personal foreign travel to a sensitive country. <strong>Note:</strong> Although you are not required to report travel to a non-sensitive country, you should keep a personal record of personal foreign travel for future clearance (re)investigations.</td>
<td>Counterintelligence (505-284-3878)</td>
<td>Prior to travel or as soon as practicable.</td>
</tr>
<tr>
<td>Have substantive contact with any foreign national.</td>
<td>Foreign National Contacts Reports (online application)</td>
<td>Immediately.</td>
</tr>
<tr>
<td><strong>Note:</strong> &quot;Substantive contact&quot; refers to a personal or professional relationship that is enduring and involves substantial sharing of personal information and/or the formation of emotional bonds (does not include family members). As SNL, substantive contact includes associations that involve meeting and the sharing of SNL business information.</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>Foreign National Contacts Reports (online application)</td>
<td>Immediately.</td>
</tr>
<tr>
<td>*Have an immediate family member who assumes residence in a sensitive country, and when that living situation changes; e.g., your family member returns to the U.S. or moves to another country, sensitive or non-sensitive. (See list of sensitive countries at the International Travel Office website.)</td>
<td>NM—Ethics Advisory and Investigative Services (505-845-9900) CA—Personnel Security (925-294-2061)</td>
<td>Immediately.</td>
</tr>
</tbody>
</table>

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

The purpose of the Classification Program is to identify information classified under the Atomic Energy Act or Executive Order (EO) 13526, so that it can be protected against unauthorized dissemination. Identifying Classified Information Policy (SSI02) 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 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.”

Department of Energy (DOE) 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>Category</th>
<th>Top Secret (TS)</th>
<th>Secret (S)</th>
<th>Confidential (C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted Data (RD)</td>
<td>Q only</td>
<td>Q only</td>
<td>Q and L</td>
</tr>
<tr>
<td>Formerly Restricted Data (FRD)</td>
<td>Q only</td>
<td>Q and L</td>
<td>Q and L</td>
</tr>
<tr>
<td>Transclassified Foreign Nuclear Information (TFNI)</td>
<td>Q only</td>
<td>Q and L</td>
<td>Q and L</td>
</tr>
<tr>
<td>National Security Information (NSI)</td>
<td>Q only</td>
<td>Q and L</td>
<td>Q and L</td>
</tr>
</tbody>
</table>

Degree of Damage: Exceptionally Grave, Serious, Damage

Restricted Data (RD), all data concerning the design, manufacture, or use of nuclear weapons; production of special nuclear material; or use of special nuclear 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), all information concerning scientific, technological or economic matters relating to 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 (SSI03, Classified Matter Protection and Control (CMPC) Policy)

When working with classified information on a computer, use only computers connected to an approved classified network (e.g., Sandia Classified Network [SCN]) or an approved classified stand-alone system.

Information processed on a classified computing system must be marked and protected at the highest potential level and category for that information you believe it contains. If unsure, consult your DC or mark as “system high” until it is reviewed by an authorized Derivative Classifier, then the markings must be updated as necessary.

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.
Getting Started with Classified

Derivative Classifier (DC) – An individual authorized to confirm that an unclassified 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 or 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.

Derivative Declassifier (DD) – 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.

You must request a DC review (either a formal, or a programmatic review) for:
- A newly generated document or material in a classified subject area that may potentially contain classified information.
- An existing, unmarked document or material that you believe may contain classified information.
- An existing, marked document or material that you believe may contain information classified at a higher level or more restrictive category.
- A newly generated document that consists of a complete section (e.g., chapter, attachment, appendix) taken from another classified document.

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

You can find a DC or DD at the Jupiter website or call Security Connection

Classified Administrative Specialist (CAS) – An individual trained to mark, store, duplicate, destroy, and mail classified matter. Work with your manager to identify your CAS.

Classified Matter Protection and Control (CMPC) – assists staff and CASs with questions regarding marking, protection, storage, and transmission of classified information. Work with your CAS or manager to address CMPC issues.

Classification Office – assists DCs and staff with classification decisions. 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 the Classification Office. NM (505) 844-5574 | CA (925) 294-2202

DOE Office of Classification – If a classification challenge can’t be resolved locally, Sandia’s Classification Office 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. Request information from outreach@hq.doe.gov.

You must use the formal Review and Approval (R&A) process if you intend to release information to an uncontrolled, widespread, unknown, or public audience. This includes information intended for release to Congress.

Work with your Cyber Security Representative to identify secure forms of communication (e.g., for classified computing).

If you see unattended classified matter, secure it and report it to Security Connection.
<table>
<thead>
<tr>
<th>COURSE MODULES</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMPROPER PROTECTION OF UNCLASSIFIED CONTROLLED INFORMATION (UCI)</td>
</tr>
<tr>
<td>IMPROPER STORAGE OF CLASSIFIED</td>
</tr>
<tr>
<td>UNAUTHORIZED DISCLOSURE OF CLASSIFIED</td>
</tr>
<tr>
<td>UNAUTHORIZED NETWORK-BASED TRANSMISSION</td>
</tr>
<tr>
<td>COUNTERINTELLIGENCE UPDATE</td>
</tr>
<tr>
<td>SAFEGUARDS &amp; SECURITY UPDATE</td>
</tr>
</tbody>
</table>
Approximately 2% of IOSCs are due to classified information being disclosed to unauthorized individuals.
THE CLASSIFIED MEETING

Sally and Joe are having a classified discussion in the Limited Area, but have to go to a meeting in the next building.

Joe continues the conversation while they are waiting outside the conference room.

Andrew (an uncleared staff member) and his escort wait with Sally and Joe to enter the conference room. Sally discretely changes the conversation.

What Must They Do?

- Sally is pretty sure that Andrew didn’t overhear. How would he know he was listening to classified anyway?
- Sally must call SIMP to report the potential disclosure of classified.
Sally and Joe are having a classified discussion in the Limited Area, but have to go to a meeting in the next building.

Joe continues the conversation while they are waiting outside the conference room.

Andrew (an uncleared staff member) and his escort wait with Sally and Joe to enter the conference room. Sally discreetly changes the conversation.

**What Must They Do?**

- Sally is pretty sure that Andrew didn’t overhear. How would he know he was listening to classified anyway?
- **Sally must call SIMP to report the potential disclosure of classified.**
THE CLASSIFIED MEETING

A SIMP inquiry was conducted and determined that Joe’s conversation in the presence of an uncleared Member of the Workforce resulted in the disclosure of classified information.

Joe received an incident for the unauthorized disclosure of classified. His manager directed him to retake SEC301 Classified Matter Training to review requirements associated with classified.
Did You Know?

Prior to a classified discussion, you must identify the highest potential classification. Ensure participants have the appropriate authorization and comply with the controlled and prohibited articles policy.
Think

Am I controlling and protecting classified from unauthorized access (physical, visual, aural, cyber, or other)?

Assess

Am I in an area where only those who meet all the requirements, including NTK, can see or hear the information?

Protect

Classified discussions should occur only within a structure in the Limited Area, with individuals who have the appropriate clearance and NTK.

- Who & What Can Go Where
- SEC301 Classified Matter Training
- SS003 Classified Matter Protection and Control (CMPC) Policy
## Who and What Can Go Where?

**SS008 - Control Access to Information and Facilities Policy**

At Sandia, Tech Area or Technical Area is used to designate certain geographical areas at our sites. Security Area refers to a physically defined space (identified by posted signs and some form of access control). Controlled Articles are devices that have the potential to record and/or transmit information with or without authorization. The Controlled Article Registration Process (CARP) application is used for registering controlled articles that will enter a Limited Area (or higher). Prohibited Articles are items that are not allowed anywhere on Sandia controlled premises that are likely to produce injury or damage to persons or property. Report unauthorized articles on Sandia controlled premises to Security Connection.

### WHO

<table>
<thead>
<tr>
<th>General Access Area</th>
<th>Security Area</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### General Access Area

- Public (Badge is not required)
- Non-Public (Badge is required)

#### Security Area

- Property Protection Area (PPA) (Badge is required)
- Limited Area (LA) (Badge & PIN is required)
- Vault Type Room (VTR) (Badge & PIN is required)

| Q-cleared individual (SNL ISSO badge or DOE HSPD-12 credential) | ✓ | ✓ | ✓ | ✓ |
| L-cleared individual (SNL ISSO badge or DOE HSPD-12 credential) | ✓ | ✓ | ✓ | ✓ |
| Uncleared individual (SNL ISSO badge) | ✓ | ✓ | ✓ | ✓ |
| Children/Friends | ✓ | ✓ | ✓ | ✓ |
| Uncleared foreign national | ✓ | ✓ | ✓ | ✓ |

*A Foreign National Request Security Plan (FNR SP) may be required before working with an unclesred foreign national. FNR SPs list areas they may access. For additional guidance contact the Foreign Interactions Office (505-844-8263).*

### WHAT

| AM/FM radio | ✓ | ✓ | ✓ | ✓ | ✓ |
| Electronic medical device capable of recording or transmitting data | ✓ | ✓ | ✓ | ✓ | ✓ |
| Sandia-owned PEDs (includes blackberries, iPods, and iPhones) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Sandia-owned camera | ✓ | ✓ | ✓ | ✓ | ✓ |
| Non-Sandia-owned Portable Electronic Devices (PEDs) (includes personal, business, & other government agency) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Personal weapons/Alcohol | ✓ | ✓ | ✓ | ✓ | ✓ |
| Marijuana (medical, extracts such as CBD, etc.) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Someone else’s prescription medication | ✓ | ✓ | ✓ | ✓ | ✓ |

*Reporting required*  
*Prohibited Article*  
*Prohibited Article*  
*Prohibited Article*

*Sensitive Compartmented Information (SCI) and Special Access Program (SAP) facilities have their own rules and restrictions. Contact the POC of that facility for more information. Comply with all posted local (such as facility-specific) restrictions and control measures for controlled devices and media.*

*Some areas of a GAA or PPA may not be approved for PEDs. Always be aware of local signage before leaving your device anywhere.*

*Sensitive Compartmented Information (SCI) and Special Access Program (SAP) facilities have their own rules and restrictions. Contact the POC of that facility for more information. Comply with all posted local (such as facility-specific) restrictions and control measures for controlled devices and media.*
SEC301
Classified Matter Training

This training can be found on the FSO Contractor Toolcart at the website below.


SAND 2015-7085 TR
ANNUAL SECURITY REFRESHER BRIEFING

COURSE MODULES

1. Improper Protection of Unclassified Controlled Information (UCI)
2. Improper Storage of Classified
3. Unauthorized Disclosure of Classified
4. Unauthorized Network-Based Transmission
5. Counterintelligence Update
6. Safeguards & Security Update
Approximately 35% of Sandia’s IOSCs are a result of classified information on networks not authorized for classified information.
THE TRANSMISSION

Alex received an email on the Sandia Restricted Network (SRN) from her Sandia team lead that contained project information in a potentially classified subject area.

Alex replies to rest of the project team with her input from her Sandia Restricted Network (SRN) computer.

A team member recognized the information Alex provided created a classified association.

What Must the Team Member Do?

- It’s only to the team members, they have a NTK, right?
- The team member must call SIMP to report the incident.
THE TRANSMISSION

Alex received an email on the Sandia Restricted Network (SRN) from her Sandia team lead that contained project information in a potentially classified subject area.

Alex replies to rest of the project team with her input from her Sandia Restricted Network (SRN) computer.

A team member recognized the information Alex provided created a classified association.

What Must the Team Member Do?

- ✗ It's only to the team members, they have a NTK, right?
- ✔ The team member must call SIMP to report the incident.
A SIMP inquiry was conducted and determined that Alex did not get a Derivative Classifier (DC)* review of the information in the email before forwarding it to the team.

Alex received an incident for the unauthorized network-based transmission. The manager scheduled a project meeting to introduce their DC, discuss project sensitivities, and assign classified subject matter briefings, to prevent reoccurrence.

*A Derivative Classifier (DC) is a person authorized to determine that a document or material is either unclassified or classified as allowed by his or her description of authority.
Did You Know?

The OPSEC Critical Information List identifies Sandia programs and activities that are of interest to the adversary.
Think

Is the information I’m working with potentially classified?

Assess

Does adding information change the classification level of the email?

Protect

Work with your DC to determine the sensitivity of your information before transmitting information on the SRN.

- OPSEC Critical Information List
- Classification Brochure
- SS002 Identifying Classified Information Policy
- SS003 Classified Matter Protection and Control (CMPC) Policy
Sandia National Laboratories Critical Information List (CIL)

Sandia National Laboratories critical information applies to all sites.

The site (or organizational) OPSEC Coordinators can disseminate site-specific critical information. If the release of critical information can cause harm to Sandia National Laboratories' programs, activities, personnel, customers, or assets, then it must be protected from inadvertent and unauthorized disclosure, even if it is not on this or any other CIL. Sites and organizations (divisions, centers, departments, sub-contractors, and/or programs) should use this list as a baseline for developing and maintaining their own CIL.

Critical Information: 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.

PROGRAMS AND ACTIVITIES:
New or established programs that present a target to adversaries, including but not limited to classified, sensitive, and unclassified programs, and those programs that fall into applicable governmental sensitive technology lists.

The table below is the CIL and used for SNL programs and activities.

<table>
<thead>
<tr>
<th>CRITICAL INFORMATION LIST (CIL)</th>
<th>Program/project and personnel relationships</th>
<th>Purchasing/procurement, vendors, shipping, and receiving requests</th>
<th>Scope and type of work conducted</th>
<th>Shipment details for sensitive materials</th>
<th>Travel and conference details, travel requests and reports</th>
<th>Work schedules and staffing changes/reports, milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications of new technology</td>
<td>Diagrams, blueprints, and schematics</td>
<td>Facilities and infrastructure</td>
<td>Critical job details, roles, and responsibilities</td>
<td>Financial, budget, accounting, and contract information</td>
<td>Network information</td>
<td>Plans, publications, and procedures</td>
</tr>
<tr>
<td>Capabilities and limitations</td>
<td>Emergency response and procedures</td>
<td>Facilities and infrastructure</td>
<td>Critical job details, roles, and responsibilities</td>
<td>Financial, budget, accounting, and contract information</td>
<td>Network information</td>
<td>Plans, publications, and procedures</td>
</tr>
<tr>
<td>Communication methods, user name/passwords</td>
<td>Facilities and infrastructure</td>
<td>Facilities and infrastructure</td>
<td>Critical job details, roles, and responsibilities</td>
<td>Financial, budget, accounting, and contract information</td>
<td>Network information</td>
<td>Plans, publications, and procedures</td>
</tr>
<tr>
<td>Current and future operations</td>
<td>Network information</td>
<td>Facilities and infrastructure</td>
<td>Critical job details, roles, and responsibilities</td>
<td>Financial, budget, accounting, and contract information</td>
<td>Network information</td>
<td>Plans, publications, and procedures</td>
</tr>
<tr>
<td>Dates, times, locations, and events (tests, exercises, etc.)</td>
<td>Network information</td>
<td>Facilities and infrastructure</td>
<td>Critical job details, roles, and responsibilities</td>
<td>Financial, budget, accounting, and contract information</td>
<td>Network information</td>
<td>Plans, publications, and procedures</td>
</tr>
</tbody>
</table>

Disclaimer: Critical Information listed here may not be all inclusive. Programs and activities should review their CIL on a recurring basis. For assistance contact the OPSEC Program Office.

IMPORTANT NOTICE: A printed copy of this document may not be the document currently in effect. Contact the OPSEC Program Office at OPSEC@sandia.gov or 505.844.OPSEC (6773).

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. AC04-94

10/2018 | SAND2018-11284M

CALL SECURITY CONNECTION AT 505-844-1321
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 (Sigmats 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/living documents, 180 days after the last revision; additionally, the originator of the document must be listed.

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.

Sandia National Laboratories
Classification Department
NM Location
P. O. Box 5800, MS 0175
Albuquerque, NM 87185-0175

CA Location
PO Box 569, Mail Stop 9021
Livermore, CA 94551-0066

E-mail classificationdept@sandia.gov

Understanding Classification

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. Four different categories further describe the information depending on the authority and rules used to handle it. 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 present 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 utilization 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 Safeguarding, 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
- BB9-1

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.)
- Time/trigger 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
- Date and photos from lab or flight tests
- Critical weapon association concerns (including part and NIC numbers)
- Unique materials used in weapon application
- Unfavorable statement about a component or a weapon
- Weapon performance or quality details
- Production issues or concerns
- Shipment 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
You can locate a DC or DD through the Jupiter application (Jupiter.sandia.gov).

A MESSAGE FROM THE CLASSIFICATION OFFICE

A Derivative Classifier (DC) is 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. Get a review by an appropriate DC 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 the last revision (if a living document).
You can locate a DC or DD through the Jupiter application (Jupiter.sandia.gov).

A MESSAGE FROM THE CLASSIFICATION OFFICE

A Derivative Declassifier (DD) is an individual authorized to declassify or downgrade documents or material in specified areas, as allowed by his or her description of authority. Get a review by an appropriate DD for declassification when documents or material is:

- Prepared for declassification in full.
- Prepared as redacted versions.
- Requested under statute or Executive Order (i.e., declassification for public release).
- Referred to DOE by other government agencies that are marked or identified as potentially containing RD/FRD/TFNI or DOE NSI equities.
If a MOW believes the information, document, or material is improperly classified, they are encouraged and expected to challenge it, and resolve the challenge with their local Classification Office.

If it cannot be resolved locally, the MOW has the right to submit a written challenge directly to the Director, Office of Classification (outreach@hq.doe.gov). Under no circumstances will you be subject to retribution for making such a challenge.
COURSE MODULES

- IMPROPER PROTECTION OF UNCLASSIFIED CONTROLLED INFORMATION (UCI)
- IMPROPER STORAGE OF CLASSIFIED
- UNAUTHORIZED DISCLOSURE OF CLASSIFIED
- UNAUTHORIZED NETWORK-BASED TRANSMISSION
- COUNTERINTELLIGENCE UPDATE
- SAFEGUARDS & SECURITY UPDATE
In one year, 35 Sandia employees reported they were contacted (through email or by personal contact) for controlled information.

Many of the contacts go unreported.

Counterintelligence is here to protect the Department of Energy and Sandia National Laboratories interest from foreign and domestic intelligence and terrorist threats.

- CI Newsletter
- Insider Threat Newsletter
- CI-Help@sandia.gov
- CA & NM: 505-284-3878
Unusual Solicitation

Any attempt by any unauthorized persons to gain access to classified is a matter of significant Counterintelligence concern and, per formal DOE/NNSA reporting requirements, should be reported immediately to Counterintelligence.

This applies equally to sensitive foreign nationals, non-sensitive foreign nationals, as well as unauthorized U.S. citizens. Such attempts can be in the form of pointed questions or more subtle elicitation.

This reporting requirement also applies to unusual situations that make you feel that you or a colleague is being targeted by a foreign intelligence service or international terrorist group.
Foreign Travel

Travel to sensitive countries must be reported (regardless of clearance level and/or citizenship). Foreign intelligence services perceive your DOE clearance as actual and/or potential access to information of value to foreign governments. You are vulnerable to the tactics of a foreign intelligence service while in their country.

Intelligence Services may:
- Surveil your movements (audio and video coverage of your hotel room, conference room, and dining facilities)
- Enter your hotel room or other quarters at will
- Compromise your electronic devices (tap your telephone, fax machine, or laptop computer)
- Use interpreters to monitor your conversations and behaviors
Insider Threat

Report to Counterintelligence, any individual who:

- Seeks unauthorized access to classified information, matter or special nuclear material without a Need To Know
- Appears to be living well beyond their means
- Has unusual foreign contacts or travel

We handle sensitive information with discretion to protect the good name and reputation of the person who is the object of your concern and balance our responsibility to protect Sandia and national security.

Foreign intelligence services seek the cooperation of an authorized insider to betray the trust of his or her colleagues. This is also the case for international terrorist groups who would target well defended, sensitive facilities like Sandia.
Substantive Contact/Relationship

All Sandia MOWs, regardless of clearance and/or citizenship status, are required to report substantive contacts with foreign nationals. Substantive contact is a personal or professional relationship that is enduring and involves substantial sharing of personal information and/or the formation of emotional bonds (does not include family members).

Substantive contact can be professional, personal, or financial in nature and includes, associations that involve meeting and sharing Sandia information or ongoing contact that is solely through electronic communication (e.g., email, telephone, or social media networking sites).

Non-U.S. citizens are considered “Foreign Nationals” if they are citizens of, were born in, or are employed in a foreign country. Natural Born U.S. citizens are always U.S. citizens.
CI TOPICS
Sponsored by The SNL Office of Counterintelligence Newsletter #62 July 19, 2018

Special counsel Mueller charges 12 Russian intelligence officers with hacking election

Special counsel Robert Mueller has obtained a new indictment charging 12 Russian intelligence officers with hacking Democrats to interfere in the 2016 presidential election, and with stealing information of about 500,000 American voters, the Justice Department announced Friday.

The indictment lodged by a federal grand jury in Washington, D.C., accuses the Russian spies of hacking into the Democratic National Committee and the presidential campaign of former Secretary of State Hillary Clinton, and of releasing emails obtained from that cybersecurity with a goal of influencing the election. More than 300 people associated with the DNC and the Clinton campaign were targeted, the indictment charges.

For the full story, click the link:
Special counsel Mueller charges 12 Russian intelligence officers with hacking Democrats during 2016 election

The Not-So-Secret Tech the CIA Wants

Back in the day the CIA’s Cold War foes would do anything — including kill — to learn what high-tech gadgets the spy agency was trying to get into the field.

Nowadays, anyone interested can look up at least a chunk of that kind of information on the public website of a curious organization called In-Q-Tel, the CIA’s very public investment firm.

The nonprofit company, which began as In-Q-IT, was first revealed publicly in 1999. It was the result of a then-revolutionary idea: If the private sector can make a lot of the high-tech things the CIA wants, why not publicly put some skin in the game to help ensure the company’s success?

According to its website, In-Q-Tel “identifies startups with the potential for high impact on national security and works closely with them to deliver new capabilities that our customers need to boost their technological edge.”

For the full story, click the link:
The not-so-secret tech the CIA wants

CI Topics is a monthly publication that seeks to raise CI awareness with intelligence related topics that are relevant to Sandia or DOE.

This publication incorporates open source news articles from various sources. Viewpoints contained in this document are not necessarily shared by the Office of Counterintelligence.

Our goal is to provide timely, useful and relevant information on intelligence related topics and events happening in the world.

Inside this issue:

| Suspect in Cleveland July 4 terror plot | 2 |
| China wants to track every driver by putting RFID chips on car windshields | 2 |
| Awareness Corner | 2 |
| Interesting Reads | 3 |
| Movies to Watch | 3 |
Suspect in Cleveland July 4 terror plot allegedly scouted Rock & Roll Hall of Fame

The FBI says it has broken up a plot by a homegrown terrorist. The suspect, Demetrius Pitts, is accused of planning an attack in Cleveland for the Fourth of July.

Pitts appeared in court on Monday. He was allegedly inspired by al Qaeda, but was not trained by the terror group. According to court papers, the plan included driving a remote controlled car packed with explosives into a Fourth of July parade.

Pitts asked an undercover FBI agent, "What would hit them in the core?"

The 48-year-old American citizen, who expressed a hatred for the U.S. military, allegedly scouted several locations in downtown Cleveland, including a United States Coast Guard station and the Rock & Roll Hall of Fame.

"His extensive criminal history including felonious assault, domestic violence, aggravated robbery, and carrying a concealed weapon furthered our reason for concern," said FBI Special Agent in Charge Stephen Anthony.

For the full story, click the link:

Suspect in Cleveland July 4 terror plot allegedly scouted Rock & Roll Hall of Fame

China wants to track every driver by putting RFID chips on car windshields

China will soon begin tracking the movements of all new cars.

Beginning next year, China will require all new registered cars to have an RFID chip installed on windshields which will help study and manage traffic, pollution, and public security, according to a report from The Wall Street Journal.

Under the program, both a car's license plate and its paint color will be recorded. Card readers placed along roads will detect the RFID chips and pass information back to the Ministry of Public Security.

China's congestion is almost incomparable, with 5 million cars on the road in Beijing. China is also one of the most dangerous countries in the world for drivers, with the World Health Organization putting traffic deaths at more than 260,000 in 2013.

For the full story, click the link:

China wants to track every driver by putting RFID chips on cars

CI Awareness Corner: Academic Solicitation

Academic solicitation is the fastest growing method of operation and according to the Defense Security Service (DSS) it took over as the primary collection method reported in FY13.

DSS defines academic solicitation as the use of students, professors, scientists or researchers as collector improperly attempting to obtain sensitive or classified information. These attempts can include request for, or arrangement of, peer or scientific board reviews of academic papers or presentations; request to study or consult with faculty members; or request for and access to software and dual-use technology.

Most of these contacts are likely legitimate. However, some foreign academics may ultimately take advantage of their placement and access to further national research and development goals.

What to report? 1) unsolicited applications, 2) unsolicited request for assistance with or review of thesis papers, 3) unsolicited invitations to attend and/or present at international conferences.

Click here for more on Academic Solicitation from DSS.

If you have any questions, please do not hesitate to contact CI at 505-284-3878 or cihelp@sandia.gov.
Interesting Reads

Hersh, Seymour M. Reporter: A Memoir. 2018.

Seymour Hersh’s fearless reporting has earned him fame, front-page bylines in virtually every major newspaper in the free world, honors galore, and no small amount of controversy. Now in this memoir he describes what drove him and how he worked as an independent outsider, even at the nation’s most prestigious publications. He tells the stories behind the stories—riveting in their own right—as he chases leads, cultivates sources, and grapples with the weight of what he uncovers, daring to challenge official narratives handed down from the powers that be. In telling these stories, Hersh divulges previously unreported information about some of his biggest scoops, including the My Lai massacre and the horrors at Abu Ghraib. There are also illuminating recollections of some of the giants of American politics and journalism: Ben Bradlee, A. M. Rosenthal, David Remnick, and Henry Kissinger among them. This is essential reading on the power of the printed word at a time when good journalism is under fire as never before. (amazon.com)


In March 2012, at a meeting convened by the recently reelected Russian president Vladimir Putin, Minister of Defense Serdyukov informed Mr. Putin that a plan was being prepared for “the development of weapons based on new physical principles: radiation, geophysical wave, genetic, psychophysical, etc.” Subsequently, in response to concerns expressed both in Russia and abroad, the Russian government deleted the statement from the public transcript of the meeting. But the question remains: Is Russia developing an offensive biological warfare program? Raymond Zilinskas and Philippe Mauger investigate the multiple dimensions of this crucial security issue in their comprehensive, authoritative survey. Ranging from the Soviet legacy to current doctrine, from advanced weapons-development networks to civilian biotechnology research, from diplomatic initiatives to disinformation campaigns, they document and analyze the build-up and modernization of Russia’s bio-defense establishment under the Putin administration. (amazon.com)

Movies to Watch

Madras Cafe. 2013.

An Indian intelligence agent journeys to a war-torn coastal island to break a resolute rebel group and meets a passionate journalist. (tmdb.com)
The Army Ignored Her Warnings About a Dangerous Colleague. Then He Set Her on Fire

According to an article appearing in Task and Purpose on June 5, 2019, Katie Blanchard, a first lieutenant at Munson Army Health Center, suffered a brutal attack from a belligerent subordinate employee that left her with third degree burns all across her body and a case of Post-Traumatic Stress Disorder (PTSD).

As reported, Blanchard’s attacker, Clifford Currie, displayed many clear signs of being an insider threat. Blanchard repeatedly reported Currie’s open aggression towards her to superiors to no avail.

Workplace violence is yet another continuously growing insider threat, along with espionage and unintentional wrongdoing. It is best for everyone to work together to recognize the signs of insider threat and take immediate action. Every employee can essentially be a part of the Insider Threat Program if everyone works together to ensure the safety and security of their work environment.

“There were all these red flags, but nobody acted,” Blanchard told Task and Purpose. “I followed their process, I followed the procedure to a T and nobody did the hard, right thing.”

We all have to work together to ensure the safety of our Department. Help protect the Department of Energy by being aware of suspicious insider threat behaviors or activities that you may observe.

If you see something unusual, contact a LITWG representative, local security contact or the IG Hotline at 1-800-541-1825; or via email: (IG) IGHotline@hq.doe.gov or at the Insider Threat Hotline at 1-202-586-3335.

If you have a sensitive matter to report, please contact your local Counterintelligence Office to report the matter in person. Extremely Sensitive or potentially classified concerns should not be reported via unclassified email or unsecure telephone calls.

If you have any questions about (or recommendations for) the PMO, you may contact the Office of Insider Threat Program at 1-202-586-8426 or via email: ITPMO@hq.doe.gov

Please visit the Insider Threat Program website at https://itp.energy.gov.
Unusual Solicitation
Foreign Travel

58

COUNTERINTELLIGENCE UPDATE

InPSYder
By Nicole M. Alford, Ph.D.
The 'Human Side' of the Insider

Summer is typically thought of as a time of getting away from it all; of lazy days and mindless nights. Time away from the grind of work, school and home that serves to recharge and restore us. But in addition to kicking off the summer season, June also doubles as both Post-Traumatic Stress Disorder (PTSD) Awareness Month and Men’s Health Month, while July serves as Minority Mental Health Awareness Month. This is the time that clinicians and mental health advocacy groups dedicate to raising awareness, educating, and informing the public about mental health symptoms, issues, and resources. So what does any of this have to do with insider threats? Daily, people walk around struggling with moderate to severe depression, anxiety, addictions or other compulsive behaviors, or other emotional issues. And some have become so used to their conditions that they accept them as their normal level of functioning. They become so used to the doldrums that they don’t believe that things will improve. Others realize that they are not okay, but are afraid to reach out for assistance. They let these issues fester and worsen. When this occurs in our work, relationships, attitudes, and decision-making can all be negatively impacted.

There is a shift in the insider threat field to one that is increasingly focusing on the ‘human side’ of the insider. That is, more than ever, our concern is for those preventable behaviors that are linked to, or borne out of, burnout, overwhelming emotional strain, or mental illness. Not every insider threat is intentional. Some harm caused by insider threats are the result of impaired judgment and functioning that was likely preventable.

With this shift, and the aim to be preventive, I offer some tips that I believe will truly help you to wind down, calm your mind, and recharge.

1. Take your vacation. You’ve earned it! Literally. There’s always work, and lots of it. But try to plan your mission critical assignments and pace yourself so that you can take much needed time off periodically.

2. Unplug: The constant barrage of negativity in the news cycle can become too much at times. Consider unplugging from both news and social media platforms periodically.

3. Use your resources: DOE Cares has a number of resources to assist you in those ‘life happens’ moments, or if you’re just not feeling okay. The Employee Assistance Program is one that offers free, confidential mental health counseling for all DOE employees.

4. Engage: The busy-ness of life sometimes takes a toll on our social relationships. Our usual meet-ups with friends, date nights with partners, and outings with our children sometimes takes a back seat to everything else going on. Summer is the perfect time to re-engage with our social relationships and loved ones.

Oregon Department of Human Services
Data Breached; Clients at Risk of Identity Theft

As reported in The Statesman Journal on June 11, 2019, in January 2019 the Oregon Department of Human Services suffered a phishing attack that exposed the personal information of over 300,000 clients.

As reported by the article, DHS and its cybersecurity team confirmed a breach happened on Jan. 28. Nine employees opened a phishing email and clicked on a link that made their inboxes susceptible. Those inboxes had nearly 2 million emails in them, including personal client information, state officials said.²

As reported by the article, the hacker(s) used malicious code in order to further exploit the system’s weaknesses and steal sensitive information. More interestingly, the hacker(s) turned the employees themselves into unwitting insider threats.

As reported by the article, many insiders would like to believe that human error is only a minor issue; that their favorite co-workers are not insider threats. Many insiders would like to believe that they themselves cannot unintentionally become the insider threat. Despite what we like to believe, these situations must be taken into consideration, especially with the ever-growing threat of cyber-attacks.


² Ibid.
COURSE MODULES

IMPROPER PROTECTION OF UNCLASSIFIED CONTROLLED INFORMATION (UCI)

IMPROPER STORAGE OF CLASSIFIED

UNAUTHORIZED DISCLOSURE OF CLASSIFIED

UNAUTHORIZED NETWORK-BASED TRANSMISSION

COUNTERINTELLIGENCE UPDATE

SAFEGUARDS & SECURITY UPDATE
The Safeguards and Security programs continue to seek ways to assist everyone at Sandia with their security responsibilities through policy updates, best practices and information that can be used to protect yourself at work and at home.

Here is information about some of the security updates in 2019.

- U & E Responsibilities Card
- Supply Chain and Risk Management Newsletter
- GEN-16 Rev2: No Comment Policy
- Lock Before You Walk
The ‘U’ and ‘E’ cards:

- Provide highly visible cues to identify uncleared individuals and their escorts,
- Represent a physical confirmation when escorting responsibility is being transferred,
- Increase security awareness,
- Deliver expected results, and
- Enhance security culture.
### “E” Card Responsibilities

**AT ALL TIMES** while in a limited or more restricted area:

- Display both the “E” card and your LSSO badge or HSPD-12 credential (visibly, above the waist and over any outerwear).

**When escorting multiple individuals, it is advisable to possess additional “E” cards to ensure proper transfer of escort responsibilities, when necessary.**

- Maintain positive control of escorted individuals.

- Comply with requirements associated with controlled and prohibited articles.

- Comply with applicable security requirements, including any that may be unique to the spaces being accessed or the activities being performed.

- If you become separated from uncleared persons being escorted, report immediately to **Security Connection**.

### “U” Card Responsibilities

- Display both the “U” card and your uncleared LSSO badge (visibly, above the waist and over any outerwear).

- **Your escort must display the corresponding “E” card while escorting.**

- Remain within positive control of your escort.

- Comply with requirements associated with controlled and prohibited articles.

- Comply with applicable security requirements, including any that may be unique to the spaces being accessed or the activities being performed.

- If you become separated from your escort, report immediately to any cleared Member of the Workforce and contact **Security Connection**.

---

**To obtain “U” and “E” cards**

Contact **Security Connection** at 505-845-1321 or security@sandia.gov.

**To report improper escorting**

Call 321.
The ‘U’ and ‘E’ cards:
Provide highly visible cues to identify uncleared individuals and their escorts,
Represent a physical confirmation when escorting responsibility is being transferred,
Increase security awareness,
Deliver expected results, and
Enhance security culture.

**SUSPECT/COUNTERFEIT ITEMS**
Amazon’s annual report includes a new “Risk” section that indicates Amazon “could be liable for fraudulent or unlawful activities of sellers”.

Amazon filed legal actions against prolific counterfeit sellers, and insists Amazon will always refund the purchasers of counterfeits when the buyer returns the item (this is against DOE guidance and Sandia policy). Some critics argue that even after being notified by the brand owner, Amazon does not always notify purchasers that a fake product was supplied. There are also reports that products directly supplied by Amazon have been counterfeit. Apple recently reported that 90% of Apple products purchased directly from Amazon were fake.

The Supply Chain Risk Management recommends reviewing our newsletters for more information on items purchased everyday by you personally or by Sandia.

email sqasci@sandia.gov.
Top stories in this newsletter

COUNTERFEIT LITHIUM ION BATTERIES
A Lithium Ion ("Li-Ion") 18650 cell ("battery") purchase may be more than you bargained for. Counterfeit and recycled 18650 Lithium Ion batteries have been identified in one death, and a number of injuries and fires.

According to the U.S. Consumer Product Safety Commission, as of July 2016 there have been over 60 incidents in the United States where Lithium ion batteries in hoverboards reportedly caught fire, destroying bedrooms and even entire homes, totaling over $2 million in property damage.

170 air/airport incidents involving lithium battery fires and smoke, carried as cargo or baggage, have been recorded. Three major aircraft accidents were reported where lithium battery cargo shipments were implicated. Link to full report


SUPPLY CHAIN HACKING
A software supply chain attack represents one of the most insidious forms of hacking. By breaking into a developer's network and hiding malicious code within apps and software updates that users trust, supply chain hijackers can smuggle their malware onto hundreds of thousands—or millions—of computers in a single operation, without the slightest sign of foul play. Over the past three years, supply chain attacks that exploited the software distribution channels of at least six different companies have now all been tied to a single group of likely Chinese-speaking hackers. Link to full article:

https://www.wired.com/story/barium-supply-chain-hackers/

FROM THE PRESIDENT: MEMORANDUM ON COMBATING TRAFFICKING IN COUNTERFEIT AND PIRATED GOODS
On April 3rd, 2010, President Trump released a Memorandum on Combating Trafficking in Counterfeit and Pirated Goods. The memorandum addresses the concerns of the online and globalized marketplaces that e-commerce has to offer. He addressed the Government Accounting Office report which looked at various online markets and identified that more than 40% of the goods sold were in fact counterfeit. This news should be starting to consumers who often feel safe buying the goods online.

The President has called for a better understanding of this whole issue as the GAO report offered only limited insight to the issue. He has called upon various sectors within the government to analyze available data and other information to develop a deeper understanding of the extent to which online third-party marketplaces and other third-party intermediaries are used to facilitate the importation and sale of counterfeit and pirated goods; identify the factors that contribute to trafficking in counterfeit and pirated goods; and describe any market incentives and distortions that may contribute to third-party intermediaries facilitating trafficking in counterfeit and pirated goods.

Link to Memorandum: https://www.whitehouse.gov/presidential-actions/memorandum-combating-trafficking-counterfeit-pirated-goods/
GEN 16 NO COMMENT POLICY

The Gen-16 policy applies to classified information in the open literature. You can’t prevent classified information that is outside of your control from appearing in the public, but cleared individuals must not comment on them.

A comment is any activity (not just verbal) 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.

Even if you didn’t know the information is classified, you are responsible for not drawing attention to it. Never assume that information in classified subject areas found in public venue is unclassified.
IV. NATIONAL POLICY.
   a. "No Comment" Policy. 10 CFR § 1045.22
      (1) Authorized holders of RD and FRD shall not confirm or expand upon
          the classification status or technical accuracy of classified information
          in the public domain.
      (2) Unauthorized disclosure of classified information does not
          automatically result in the declassification of that information.
      (3) If the disclosure of classified information is sufficiently authoritative
          or credible, the DOE Associate Under Secretary for Environment,
          Health, Safety and Security shall examine the possibility of
          declassification.
   b. Executive Order 13526, Classified National Security Information, Part I,
      Section 1.1(c). "Classified information shall not be declassified
      automatically as a result of any unauthorized disclosure of identical or
      similar information."

V. PRINCIPLES.
   a. Comment. A comment is any activity that would allow a person who is not
      authorized access to classified information to locate the information or
      confirm the classified nature or technical accuracy of the information.
   b. Classification Status. An authorized person must not comment, either
      verbally or in writing, to a person who is not authorized access to classified
      information on the classification status of any classified information in the
      open literature (including the fact that a document is being reviewed for
      classification or the results of such a review, which may be disclosed only to
      the person who submitted the document for review).
   c. Technical Accuracy. An authorized person must not comment, either
      verbally or in writing, to a person who is not authorized access to classified
      information about the technical accuracy of classified information in the
      open literature.

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

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

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

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

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

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

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

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

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

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

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

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

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

d. Reporting. An employee encountering DOE classified information in the open literature must report the information following DOE policies and local instructions.
e. Review of Documents that Potentially Contain Classified Information. Per DOE Order 475.2A, Identifying Classified Information, Attachment 4, I(a)(11), "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 where classified information appears in the open literature. Whether or not an advisory is released, the "No Comment" policy should be followed whenever classified information appears in the open literature.

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

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

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

Andrew P. Weston-Dawkes
Director
Office of Classification
Office of Environment, Health, Safety and Security
Understanding the Department of Energy (DOE) GEN-16: NO COMMENT POLICY

In incidental exposure to classified information in a public venue can hardly be avoided these days. To address this, DOE in 2014 revised its No Comment Policy (Gen-16, Rev 2). The revision allows cleared individuals who view, access, or possess publicly available information that contains classified - to do so without incurring a security incident/infracton merely for having or accessing such material in unprotected venues, provided they do not comment on it.

All Sandia members of the workforce should read the Gen-16 Policy. Gen-16 does not authorize cleared individuals to seek out classified information in public venues with the intent of bringing it into use in unclassified venues. However, if a document, book, article, publication, etc., is necessary to support business or operational needs, the policy does allow individuals to access and even download such documents provided they do not comment or bring it into use on Sandia’s computing system.

To summarize, you cannot prevent classified from showing up in public places but as a cleared individual, you are obligated to avoid commenting on it.

What Constitutes a Comment?

Comments are made when you take any action that:

Reveals or suggests that the information is classified. It likely constitutes a comment by saying things like, “Hey, you might want to have a DC look at page 7 of this article, as it probably shouldn’t be public”, or “I think we should send this letter to the classification office for review, especially the second paragraph.”

Validates or confirms the technical accuracy of the information. It likely constitutes a comment to say things like, “I hope they don’t try to use that, because it will work”, or “Wow, that looks just like one of ours.”

Uses the information in a Sandia generated report, presentation, email, or other work product. By using the document in a Sandia work product, you are validating its merits, even if you are not discussing the classified portion of the document specifically.

Isolates the classified segment which may be a part of a larger document. A cleared individual who isolates it (i.e., pulls it out, highlights it, annotates it, or otherwise points to it), is making a comment. It is does not matter whether you are aware that what you pulled out is classified, nor does it matter whether you are commenting about the specific classified information, you will be held accountable for making a comment.

Your clearance implies to onlookers, that you have access to classified, and isolating the information implies that it has value.

Safeguards & Security Update

Understanding the Department of Energy (DOE) GEN-16: NO COMMENT POLICY

If you want to avoid the potential hazards that can arise when you acquire information from public venues, apply the principles of laboratory policy. Avoid acquiring, commenting on (written/oral), disseminating, or bringing into use, any information in a classified subject area, unless you get a DC review OR you are certain that a DC has deemed it unclassified.

Never assume that information in classified subject areas found in public venue is unclassified.

Cleared Individuals must treat information found in public venues that is marked as classified as if it is classified.

- You should not print it (although printing is allowed under certain circumstances, it should be avoided).
- You must not download it on unclassified media or computing systems.
- You must not comment.

Cleared individuals should not seek out classified information in public venues with the intent of bringing it into use at Sandia.

Incidental access to websites, social media platforms or other information venues that contain classified is not a violation if you do not comment on it.

Downloading or referencing a webpage or website that contains classified is not a violation if you do not limit the download to only the classified portion or otherwise comment on it.

Indicating that large venues (e.g., internet or books) contain classified information is not a violation if the venue is large enough that it would be impossible or unlikely that a person could take your statement and identify the classified piece. See Example below.

Forwarding an article, that is known to contain classified information is not a violation if it is sent without commenting. Note: It is discouraged, the recipient could be put at risk and inadvertently comment on the classified part of the article because a trusted person sent it to them.

Example:

Saying there is classified on the Internet is not a comment.

Saying there is classified in the 5-page article on Mary Poppins is likely a comment because few classified subject areas would be discussed in that article. So, the classified information would be readily identifiable.

Your clearance implies to onlookers, that you have access to classified, and isolating the information implies that it has value.

Safeguards & Security Update

Understanding the Department of Energy (DOE) GEN-16: NO COMMENT POLICY

If you want to avoid the potential hazards that can arise when you acquire information from public venues, apply the principles of laboratory policy. Avoid acquiring, commenting on (written/oral), disseminating, or bringing into use, any information in a classified subject area, unless you get a DC review OR you are certain that a DC has deemed it unclassified.

Never assume that information in classified subject areas found in public venue is unclassified.

Cleared Individuals must treat information found in public venues that is marked as classified as if it is classified.

- You should not print it (although printing is allowed under certain circumstances, it should be avoided).
- You must not download it on unclassified media or computing systems.
- You must not comment.

Cleared individuals should not seek out classified information in public venues with the intent of bringing it into use at Sandia.

Incidental access to websites, social media platforms or other information venues that contain classified is not a violation if you do not comment on it.

Downloading or referencing a webpage or website that contains classified is not a violation if you do not limit the download to only the classified portion or otherwise comment on it.

Indicating that large venues (e.g., internet or books) contain classified information is not a violation if the venue is large enough that it would be impossible or unlikely that a person could take your statement and identify the classified piece. See Example below.

Forwarding an article, that is known to contain classified information is not a violation if it is sent without commenting. Note: It is discouraged, the recipient could be put at risk and inadvertently comment on the classified part of the article because a trusted person sent it to them.

Example:

Saying there is classified on the Internet is not a comment.

Saying there is classified in the 5-page article on Mary Poppins is likely a comment because few classified subject areas would be discussed in that article. So, the classified information would be readily identifiable.

Your clearance implies to onlookers, that you have access to classified, and isolating the information implies that it has value.
LOCK BEFORE YOU WALK

Protect sensitive information and prevent security incidents—always secure your computer before walking away.

Report:
- any unsecured classified computing system
- if you suspect unauthorized access to sensitive, unclassified information in an unclassified environment
Lock before you Walk
Protect sensitive information and prevent security incidents—always secure your computer before walking away.

Shortcuts to secure your Windows computer
- Press Windows key + L on your keyboard
- Press “ctrl+alt+del” and select the “lock” option (Windows 10), or “lock this computer” (Windows 7)
- Windows 10: From Windows icon in lower left corner, choose your User icon, and then select “Lock”
- Windows 7: Windows “Start” option in lower left corner, expand the choices on “logoff” and select “lock”

(On a Zero Client – just “tap” the power button. This immediately disconnects your session. The power button will be "blue" to show it has remained ON, but disconnected.)

For questions or to report
321 from a Sandia landline  |  505-845-1321 from any phone
security@sandia.gov

Reporting
- In a classified environment, report any unsecured workstation.
- In an unclassified environment, report if you suspect unauthorized access to sensitive, unclassified information.

Resources
- Classified Computing Continual Service Improvement (3CSI)
- SS003 Classified Matter Protection and Control (CMPC) Policy
- IT002 Use Sandia’s Information Technology Resources Policy
- Article 191 Unattended Classified Desktops - Screen Locking and End-Of-Day Process
That wraps up the Annual Security Refresher briefing.

You can help prevent incidents by taking an active role in understanding what is sensitive or potentially classified in your program to ensure security is a top priority with every conversation, email, document and presentation.

On behalf of Safeguards and Security, keep up the good work, PROTECTING WHAT IS OURS.

Thank you.
SEC100 Completion Record: 2019/2020

By completing this form, you acknowledge that you have read the 2019/2020 Annual Security Refresher briefing and understand your security responsibilities.

Complete the information below and email to securityed@sandia.gov or fax to 505-844-7802 to receive credit in TEDS.

If you would like confirmation of completion, provide your email address below:

I have read and understand the content provided in the SEC100, Annual Security Refresher Briefing.

Print full name:

SNL Org # or Company Name:

Signature:  Date:

Email address:
SEC100 Feedback form

Your feedback is important to us.

Please complete this evaluation form and email to securityed@sandia.gov or fax to 505-844-7802 to receive credit in TEDS.

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

<table>
<thead>
<tr>
<th>Area</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ease of use for this learning.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The organization of the information presented.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The usefulness of the information presented.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Your level of knowledge related to this topic BEFORE using this tool.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Your level of knowledge related to this topic AFTER using this tool.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enter feedback below.

What was most valuable about this briefing?

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

What could be done to improve or enhance this briefing?