Hello everyone.

I just want to talk to you about why I consider security to be so important. At this very moment, there are hundreds of people in Moscow, Beijing, and other places who spend all of their time trying to find out what happens at Sandia. Most likely there are foreign agents right here in Albuquerque. They want to know what we do, to gain a military advantage, to gain a commercial advantage. Why? Because Sandia’s the best science and engineering laboratory in the world, of course they'll come here. But also because of the type of work that we do here. The consequences of error are high. If a foreign power had access to our weapons designs, they could figure out ways to defeat them, or at least make them less reliable in battle. In a time of crisis, a foreign leader might call our President and say that he doesn't fear our nuclear deterrent because he knows how to take it out. The United States would be helpless. History would change in that moment. And it's not just nuclear. Sandia technology is everywhere that American soldiers, sailors, and Marines fight. If the adversaries knew the details of this technology they could find ways to neutralize it, and that could very well lead to the deaths of Americans. And it's not just military technology, the world is an intensely competitive place. Thousands -- millions of American jobs depend on us keeping a step ahead of the competition. Our competitors want to close that gap, so they come to where new technologies are invented, where new ideas are developed into practical applications. These are the reasons why security is so important to me. This is why we need to pay attention to security every hour of every day, with every conversation, every email, every document, every presentation. Along with safety, security is our top priority. It has to be.

Thank you.
Introduction

PROTECTING WHAT IS Ours!
Introduction
Unauthorized Network-Based Transmission
Salutations Sandia.

This is Sam Seriously, reporting today’s Top Story.

Cecilia, a Sandia employee, received an unclassified email on the SRN from an external contractor, for a newly funded project, requesting comments. Cecilia replied to all, which included an uncleared colleague, adding project information that made the email classified.

Here’s Lynn Laser-Lab with more on what happened.
Thanks Sam. Lynn Laser-Lab here with Cecilia. Cecilia, we understand you hit reply all. What went wrong?

I didn’t consider/review the entire content of the email prior to sending. I also didn’t consider that I was working in a potentially classified subject area.

As a result, I compiled unclassified information that revealed classified on an unauthorized network which also resulted in an unauthorized disclosure.

Thanks for walking us through it, Cecilia, now back to Sam in the studio for more details on Today’s Top Story.
Great reporting Lynn. Here’s what we learned:

A Derivative Classifier (DC) reviewed Cecilia’s response and determined the email was “Confidential Restricted Data” due to the additional information Cecilia added.

We now have classified information residing on a network not approved for classified.

After reviewing the individuals in the reply, a colleague was identified that did not have the proper clearance level or a Need to Know for the information.
Nick Nuclear will have more on unauthorized disclosure in a special update.
And here with me to provide some lessons learned, best practices, and helpful resources is Patty Protection, a top notch Derivative Classifier.
Thanks Sam. If you are working in a potentially classified subject area: Make sure you’re working on an approved classified network. If working on an approved classified network isn’t viable, work with the appropriate DC before generating information to understand its sensitivities. When working on a new project, it is the perfect time to engage a DC.

<table>
<thead>
<tr>
<th>Classification Level</th>
<th>DOE Classification</th>
<th>Categories and Clearance Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restricted Data</td>
<td>Formerly Restricted Data (FRD)</td>
</tr>
<tr>
<td>Top Secret (TS)</td>
<td>Q only</td>
<td>Q only</td>
</tr>
<tr>
<td>Secret (S)</td>
<td>Q only</td>
<td>Q and L</td>
</tr>
<tr>
<td>Confidential (C)</td>
<td>Q and L</td>
<td>Q and L</td>
</tr>
</tbody>
</table>

“Confidential” is one of the three classification levels, along with Secret and Top Secret and must be protected. For more information, view HELPFUL RESOURCES.
All Members of the Workforce must:

Get a review by an appropriate Derivative Classifier (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., adhoc 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).

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.
All Members of the Workforce must:

Get a review by an appropriate Derivative Declassifier (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.

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.

If a Member of the Workforce needs to locate a DC or DD, use the Jupiter application.

Be sure to search for the appropriate DC or DD (knowledgeable and authorized) for the classified subject area you’re working on.
Patty, what if the MOW believes the information, document or material is improperly classified?

Sam, the MOW is encouraged and expected to challenge anything they believe is improperly classified.

They should try to resolve the challenge with their local Classification Office and 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.
Managers should regularly schedule a work planning meeting to brief staff and working group members to review:

- If the information they are working with is in a potentially classified subject area.
- Levels and categories of the classified information.
- The potential damage if not protected.

This is important for newly funded projects where MOWs may not have the same knowledge and familiarity with project and classification information.

Patty, great information. Will you please provide some HELPFUL RESOURCES for PROTECTING WHAT IS OURS!
Laboratory Policy (available on Sandia Restricted Network)
SS001 - Derivative Classifier
SS002 - Identifying Classified Information

Helpful link (available on Sandia Restricted Network)
Jupiter tool

Read the following handouts (provided at the end of all modules):
Everything You Need to Know About Classified
Understanding Classification

Helpful numbers
NM Classification Office: 505-844-5574
CA Classification Office: 925-294-2202
Security Connection: 321 from a Sandia phone or
505-845-1321 from a non-Sandia phone
Unauthorized Disclosure of Classified Information
Unauthorized Disclosure of Classified Information

Now for a Special Report on unauthorized disclosure of classified information, Nick Nuclear.
Thanks Sam. Because Cecilia did not work with a DC or manager to understand the sensitivities of the project, she sent the email to project members that didn’t have the appropriate clearance level for the information.

And that’s what caused the unauthorized disclosure?

Yes.

I understand you have some best practices to help the MOW.

I sure do Sam.
To prevent unauthorized disclosure, the MOW should:

**THINK:** Am I operating in a potentially classified subject area?

**ASSESS:** Do I need to work with a DC to understand the project sensitivities?

**PROTECT:** Know your audience. Work with your manager/project members to provide information on the appropriate network.

Thanks Nick, Think.Assess.Protect will certainly help.
But wait, there’s more. Not knowing the project information was classified, the external contractor highlighted some classified details of the new project on their company website. And if you comment that there is classified on the website, that is likely to be a violation of DOE Gen-16 policy and needs to be reported to SIMP.

Nick, can you help the MOW understand the DOE Gen-16 policy to know what is considered a comment?
Sure Sam. 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. The MOW must not comment on:

- Potentially Classified information found in open literature or forum (e.g., websites, blogs, wikis, news articles, videos) or
- Classification status or technical accuracy on information in the open literature.

And if we see it Nick, what should we do?
What else can we do to prevent unauthorized disclosure of classified, and avoid violating the DOE Gen-16 Policy?

Don’t comment!

Call the Security Incident Management Program (SIMP) and an Inquiry Official (IO) will provide guidance.
You must have documents or material reviewed by a DC before you present information in a potentially classified subject area in an unclassified setting.

Who can help the MOW understand the type of information they’re working with?

The MOW can ask their manager or security professional if their program has a Critical Information List (CIL) to identify and protect information from being released.

And I understand you also have some helpful resources for the MOW.
Laboratory Policy (available on Sandia Restricted Network)
SS002 - Controlling Classified Information
SS013 - Operations Security (OPSEC)

Helpful link (available on Sandia Restricted Network)
Review and Approval online tool

Read the following handouts (available at the end of all modules):
DOE Gen-16 policy
Critical Information List

Helpful numbers
Security Connection: 321 from a Sandia phone
505-845-1321 from a non-Sandia phone
Improper Storage of Classified
Our next story involves a security professional’s journey to train the MOW on proper storage of classified information.

Here to share that triumphant story of courage is Terry Techarea.
Sam, we attend meetings every day, all day and sharing information is how we accomplish work here at Sandia. We met with Andy Atom to discuss how he Saw Something and Said Something! and saved the day at Sandia.
It was a classified meeting in the limited area just like any other classified meeting and we were all there. David, a newly Q-cleared SNL employee was provided a Confidential National Security Information document.

And I said to myself, “Self, does David, being so new, understand that within DOE, Confidential is a level of classified information that requires specific protection and control?”

Then the meeting ran long and we were all left in a rush to get back to our offices and go home for the day.
On my way out, I passed David’s limited area office and noticed the same Confidential document on his desk.

David had left for the day, so I immediately took possession of the classified document and locked it in a GSA approved safe and contacted SIMP by calling 321 from the nearest Sandia phone.

When David came in the next day, I introduced him to our department Classified Administrative Specialist (CAS) and showed him our department GSA approved safe.
Great catch Andy!

A SIMP IO met with David and determined that he did not understand that Confidential was a classified marking and that leaving the document improperly secured resulted in an incident of security concern due to improper storage/protection of classified information.

I’ll be back in the studio with some best practices for the MOW.
To reduce the risk of improper storage, MOWs should:

Coordinate classified activities with your CAS to get your classified password and document to perform work at a designated classified kiosk, if available.

This method helps ensure classified matter is properly marked and stored at the appropriate level and category.
Great reporting as always Terry and great job Andy Atom. You saved the day, educated a fellow MOW and secured Sandia’s classified information. Here are some helpful resources for protecting and storing classified information.
Laboratory Policy (available on Sandia Restricted Network)
SS003 - Classified Matter Protection & Control (CMPC)

Helpful link (available on Sandia Restricted Network)
Classified Workstation Manual

Read the following handouts (available at the end of all modules):
Everything You Need to Know About Classified
Understanding Classification

After hours Classified information/matter storage assistance:
NM Protective Force: 505-844-4657
CA Protective Force: 925-294-2300
Security Connection: 321 from a Sandia phone or
505-845-1321 from a non-Sandia phone
Unauthorized Vehicle Gate Access
THIS JUST IN!

Live outside a vehicle gate is Chris Classified with Breaking News.
Chris Classified standing here outside the Limited Area where Annie Awareness, a Q cleared MOW badged in and was tailgated by an unknown driver in a personally owned vehicle.

That’s right folks, tailgated.

We were able to talk to Annie Awareness to see how she handled the situation.
Chris Classified with Sandia News, can you tell me what happened here today?
Sure. Today when I was approaching the security area gate, in our government vehicle, the signs made me aware that it was a Limited Area which requires my badge and pin.

I presented my badge, entered my pin and began to drive into the limited area and that’s when I noticed the vehicle following me in before the gate arm came down.
I knew the only thing to do was to stop my vehicle, to prevent them from going any further into the limited area. I called the Sandia Protective Force, gave a description of the vehicle and waited for help to arrive.

I didn’t want to be responsible for the vehicle getting inside the Limited Area.
Thank you Chris.

Great Work Protecting What is Ours Annie! Let’s go back to Sam for a discussion of the difference between tailgating, vouching and escorting?

Thank you Chris.
Way to be aware, Annie.

Back to Chris to review some definitions and share some best practices, helpful resources, and important numbers if you find yourself being tailgated into any security area at Sandia.
Vouching - Visually verifying the access authorization of another person for the purpose of granting them entry into a security area. The person being vouched is described as piggybacking.

Tailgating - Action taken by an individual to avoid established security protocols (e.g., badge reader) by following another individual into a security area without that individual’s knowledge.

Escorting - Action taken by an authorized individual to oversee and control people within a security area who do not have the proper NTK or access authorization for that area.
When entering any security area vehicle gate (PPA or LA), you must:

- Know what type of area you are entering
- Ensure you are complying with the area’s prohibited or controlled articles requirements
- Have the appropriate clearance level
- Follow all posted signs and local restrictions
- Verify the gate closes behind you and no other vehicles follow you in (tailgating)

When entering a LA vehicle gate, you also must:

- Disable Bluetooth and Wi-Fi in the vehicle, if applicable
- Understand and follow [SS008.1 Site Access](#) if escorting another vehicle

Back to you, Sam in the studio.
Unauthorized Vehicle Gate Access

Contact Pro Force:

• Use a cell phone or phone at the vehicle gate.
• Be prepared to provide information: your name, location, security concern.
• Unless instructed otherwise, remain in your vehicle and wait for help to arrive.

Laboratory Policy (available on Sandia Restricted Network)
SS008.1 Site Access

Read the following handouts (at the end of all modules):
Who & What Can Go Where

Helpful numbers
NM Protective Force: 505-844-4657
CA Protective Force: 925-294-2300
Security Connection: 321 from a Sandia phone or 505-845-1321 from a non-Sandia phone
Counterintelligence
And in World News, the Office of Counterintelligence would like to remind everyone of the importance of reporting.

Sam Seriously
Sandia Counterintelligence wants you to report:

- Substantive relationship with foreign nationals.
- Personal foreign travel to sensitive countries.
- Unusual interactions or questions about your work at Sandia.

You should also report:
Unsolicited emails targeted at you.

Sam Seriously
Counterintelligence defines substantive relationship: A personal or professional relationship that is enduring and involves substantial sharing of personal information and/or the formation of emotional bonds.

**Substantive contact:** includes contact through social media i.e., Facebook, Twitter, LinkedIn, etc., and associations which involve meeting and sharing SNL business information.

**I also want to share some Counterintelligence helpful resources.**
Laboratory Policy (available on Sandia Restricted Network)
SS012 Report Personnel Security Information and Security Incidents

Read the following handouts (available at the end of all modules):
CI Newsletter
DOE and Sandia Reporting Requirements

Counterintelligence Helpline:
NM & CA: 505-284-3878

Counterintelligence email:
CI-Help@sandia.gov
Security Updates
This chart represents recent security incidents and the stories we shared today contributed to these numbers.

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

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

We need to do better.
I’d like to share some important Security updates from programs around Sandia that help us protect our people, information, and national interests.

Vault Type Room Terms
Supply Chain Risk Management
Managing Metagroups
Protecting Your Badge
Vault Type Room (VTR) Terms

This year, VTR terms were updated to ensure proper access and escorting in VTRs.

Program Authorized User (PAU) is a person who:

• Has access authorization on the VTR access list or in WebCAT, as applicable,
• Has badge/PIN access to enter the VTR,
• Has unescorted access inside the VTR, and
• Has been granted combination privileges by the VTR manager’s or delegate’s discretion.

Escorted Visitor (EV) is a person who:

• Is NOT identified on the VTR access list or in WebCAT,
• Is allowed access to a VTR, and
• Is escorted at all times while inside the VTR.

For more information: contact Security Connection 505-845-1321
Supply Chain Risk Management

Use a valid vendor to avoid Suspect and Counterfeit parts.

- Conduct an internet search to validate the location. Is it a valid address and does the location make sense? If you are unable to locate basic contact information such as sales, location, address, phone numbers, etc. the company is likely not legitimate.

- If you can’t validate the company, don’t use them.

- Don’t just trust ratings, read the comments! Companies may skew ratings to be higher at 4 or 5 stars, but may leave the original negative comments about products.

For more information visit: Supply Chain Risk Management site (available on Sandia Restricted Network)
Email: sqasci@sandia.gov
Managing Metagroups

Metagroup owners/delegates should routinely review listed members to control access to the collaborative sites. This will ensure members:

- Meet access requirements and need to know for the information on the collaborative site (e.g., foreign nationals cannot be on the metagroup if OUO Ex. 3 information is going to be added to the site).
- Are removed when they leave the working group/organization.
- Working in a potentially classified subject area, do not add uncleared individuals.

Adding information to the collaborative site accessed by uncontrolled members could lead to the site now containing classified information which would automatically make this a high level security incident.

To review metagroups visit: Metagroup Utility site (available on Sandia Restricted Network)
Protecting Your Badge

With auto theft and property crime on the rise, it is important to use appropriate countermeasures to protect your badge. The badge gives the adversary information about you and our sites and could potentially give them access to our information, facilities, and assets.

Secure your badge!

Report lost or stolen badges immediately to Security Connection at 321 from a Sandia phone or 505-845-1321 from a non-Sandia phone.

24/7/365
Conclusion
As we wrap up today’s news, it is important to remind ourselves of Dr. Younger’s message and understand that our information is threatened every hour of every day by companies and countries who want to know what we do, to gain a military or commercial advantage.

Security has to be a Top Priority with every conversation, email, document, and presentation.
On behalf of all us in the Sandia newsroom,

Stay Secure Sandia!

PROTECTING WHAT IS OURS!
The purpose of the Classification Program is to identify information classified under the Atomic Energy Act or Executive Order (E.O.) 13526, so that it can be protected against unauthorized dissemination.

Laboratory Policy SS002, Identify Classified Information, contains much of what you'll need to know when working with classified information at SNL. Below are some of the terms you'll hear regarding classified information.

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

**Classified Matter** — Any combination of documents and material containing classified information. Access is restricted to persons with appropriate access authorizations (security clearances) and “need to know.”

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

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

**Restricted Data (RD),** all data concerning the design, manufacture, or use of nuclear weapons; production of special nuclear material; or use of special 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 (SS003, Classified Matter Protection and Control)**

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 stand-alone system. Home computers are not approved for use, even with Sandia’s unclassified information.

Information processed on a classified computing system must be marked at the highest potential level and category for that information, or marked and protected at the highest level and category of the information resident on the computing system until it is reviewed by an authorized Derivative Classifier (DC).

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

#### Derivative Classifier (DC)
- An individual authorized to confirm that an unmarked document or material is unclassified or determine that it is classified as allowed by his or her description of authority. Only trained DCs determine whether documents and material are classified, and to what level and category. DCs are trained on specific technologies/programs—what is not classified on one technology may be classified in other circumstances. Be sure to choose the right DC.

#### 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.

#### Declassification Requirement
- 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/FTNI or DOE NSI equities.

You can find a DC or DD at the Jupiter website, or by calling 321 from a Sandia phone or 505-845-1321 from any phone.

### Classified Administrative Specialist (CAS)
- An individual trained to mark, store, duplicate, destroy, and mail classified material.

**Work with your manager to identify your CAS.**

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

**Work with your CAS or manager to address CMPC issues.**

### Classification Office
- Assists DCs and staff with classification decisions, and reviews information for public release. If you think a DC determination is incorrect, you have the right and are encouraged to challenge the classification status of information by contacting the Classification Office.

- NM (505) 844-5574
- CA (925) 234-2202

### DOE Office of Classification
- If a classification challenge cannot be resolved locally, Sandia’s Classification Officer will submit a challenge in writing to the Director, DOE Office of Classification. You also have the right to submit a formal written challenge directly to the Director. Under no circumstances will you be subject to retribution for making such a challenge.

**Request information from outreach@sandia.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 321 from a Sandia phone or 505-845-1321 from any phone.
WHEN SHOULD YOU HAVE A DOCUMENT REVIEWED?

Documents must be reviewed before they are finalized, sent outside of the organization or working group on which you are serving, or filed permanently. Prior to getting a review, you should protect and mark the document at the highest potential classification level, category, and caveat (Sigmas 14, 15, 18 and 20) of information that you believe is in the document.

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

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

WHO IS AUTHORIZED TO CONDUCT CLASSIFICATION REVIEWS?

As required by DOE Order 475.2B, Identifying Classified Information, only Derivative Classifiers (DCs) may conduct a review of information for classification.

DCs must:

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

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

Phone: 505-844-5574
Fax: 505-844-1977

E-mail: classificationdept@sandia.gov

Security Question?
Ask us!
Think. Assess. Protect.

Security Connection 505-845-1321 or 321 from a Sandia phone

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.

SAND2015-8385 O
WHAT INFORMATION IS CLASSIFIED?

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

The four categories are:

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

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

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

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

WHAT IS A CLASSIFIED SUBJECT AREA?

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

At Sandia, common classified subject areas include:

**Areas Related to Weapons**

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

**Areas Related to Security**

- Intelligence/Counterintelligence
- Transportation Safeguards System
- Safeguards and Security

**Weapon Programs**

- W76-0.1
- W80-1
- W84
- W88
- B61-7
- B61-12
- W78
- W80-4
- W87
- B61-3/4/10
- B61-11
- B83-1

WHAT ARE SOME “RED-FLAG” INDICATORS?

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

- Neutron generator (NG) design and performance details (NG timing, etc.)
- Timer/drive design and performance details
- Firing set design and performance details
- Gas transfer system design and performance details
- Fuzing/Height of Burst (HOB) design and performance details
- Weapon use control features
- Data and photos from lab or flight tests
- Critical weapon association concerns (including part and MC numbers)
- Unique materials used in weapon application
- Unfavorable statement about a component or a weapon
- Weapon performance or quality details
- Production issues or concerns
- 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 control
- Configuration of components within the weapon
U.S. Department of Energy  
Washington, D.C.  

September 23, 2014

CLASSIFICATION BULLETIN

GEN-16 Revision 2: "NO COMMENT" POLICY ON CLASSIFIED INFORMATION IN THE OPEN LITERATURE

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

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

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

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

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

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

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

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

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

V. PRINCIPLES.

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

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

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

VI. GUIDANCE.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Andrew P. Weston-Dawkes  
Director  
Office of Classification  
Office of Environment, Health, Safety and Security
Who and What Can Go Where?

At Sandia and throughout the DOE complex, Tech Area or Technical Area is used to designate certain geographical areas, typically (but not always) enclosed by a fence. A Security Area refers to a physically defined space (identified by posted signs and some form of access control) containing special nuclear material, classified matter or property.

<table>
<thead>
<tr>
<th>WHO</th>
<th>General Access Area</th>
<th>Security Area</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Public</td>
<td>Non-Public</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q-cleared individual</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>L-cleared individual</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Uncleared individual w/SNL LSSO badge</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Children</td>
<td>✓</td>
<td>Only during certain special events with prior permission</td>
</tr>
<tr>
<td>Friend (uncleared)</td>
<td>✓</td>
<td>Only during certain special events with prior permission</td>
</tr>
<tr>
<td>Uncleared foreign national</td>
<td>Only in areas listed on their Foreign National Request Security Plan (FNR SP). For additional guidance contact your Center Security Coordinator or the Foreign Interaction Office (FIO).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WHAT</th>
<th>General Access Area</th>
<th>Security Area</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Public</td>
<td>Non-Public</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non Gov't-owned Portable Electronic Devices (PEDs) (includes laptops)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sandia-owned PEDs (blackberry w/credential, iPad, and iPhone)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AM/FM radio</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Electronic medical device</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sandia-owned camera</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Personal weapons/fireworks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alcohol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marijuana (medical, extracts such as CBD, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Someone else’s prescription medication</td>
<td>Prohibited Article — If your drug test indicates the presence of a prescription medication, and you cannot produce a valid prescription in your name, you will be subject to disciplinary action (e.g., termination of employment).</td>
<td></td>
</tr>
</tbody>
</table>

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

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

SCI and SAP facilities have their own rules and restrictions. Contact the POC for that facility for more information.

*Government owned laptops may be allowed in VTRs under certain circumstances. Contact the VTR POC for more information.
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>
</tr>
</thead>
<tbody>
<tr>
<td>Applications of new technology</td>
</tr>
<tr>
<td>Capabilities and limitations</td>
</tr>
<tr>
<td>Communication methods, user name/passwords</td>
</tr>
<tr>
<td>Critical job details, roles, and responsibilities</td>
</tr>
<tr>
<td>Current and future operations</td>
</tr>
<tr>
<td>Dates, times, locations, and events (tests, exercises, etc.)</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).
CI TOPICS

Sponsored by The SNL Office of Counterintelligence Newsletter #85 October 19, 2018

CIA helicopter that landed in Afghanistan after 9/11 joins 'best museum you'll never see'

Seventeen years ago, on Sept. 26, America began to hit back.

Just 15 days after the U.S. mainland was attacked by al Qaeda terrorists on 9/11, a team of seven CIA paramilitary operatives and a three-man flight crew landed in Afghanistan's Panjshir Valley to prepare for the assault that would topple the Taliban regime by December.

The CIA liaison team – codenamed JAW-BREAKER – flew into Afghanistan on a Russian-made twin-turbine Mi Mi-17 helicopter and began to coordinate with the Northern Alliance rebels who controlled roughly a quarter of the country's territory.

Now, that aircraft, which flew 510 missions in Afghanistan, is being enshrined in the agency's headquarters in Langley, Virginia, at the CIA Museum – a place agency employees jokingly refer to as "the best museum you'll never see."

For the full story, click the link: CIA helicopter that landed in Afghanistan after 9/11 joins 'best museum you'll never see'

'Five Eyes' and tech giants closely watch Australia's spyware bill

In the UK last month accused murderer Stephen Nicholson was jailed for refusing to hand over his Facebook password to the police.

He had been convicted under electronic surveillance laws introduced in 2016 which Australia is now enacting with legislation introduced to parliament by the Minister for Home Affairs, Peter Dutton, just weeks after Nicholson was handed his 14-month sentence.

UK authorities had good reason to gain access to Nicholson's account under the Regulation of Investigatory Powers Act, dubbed the Snooper's Charter, which expands the electronic surveillance powers of police and intelligence services.

He had been arrested in July on suspicion of murder, and had communicated with the victim, 13-year old Lucy McHugh, via Facebook the day of her murder.

For the full story, click the link: 'Five Eyes' and tech giants closely watch Australia's spyware bill

Inside this issue:

EARLY EDITION: A double agent at the newsroom door

French Fears Iran Intelligence Assets to Sign Of Worthing Escalations

U.S. spies see new threats from global rivals, and say it may be Cold War 2.0

Interesting Reads

Movies to Watch

SAND2018-11655 O
EARLY EDITION: A double agent at the newsroom door

The only real spy I’ve ever met didn’t look anything like James Bond.

One day in 1997, I was working in the publisher’s office at the Ottawa Citizen when my assistant informed me that an elderly man had arrived and insisted on seeing me. The visitor was short, had prominent ears and a wicked grin. He was wearing a T-shirt and shorts topped by a baseball cap. He appeared to be in his 70s.

“You’ve printed a story that isn’t correct,” he said. He pulled a clipping out of a plastic shopping bag. It was a story the Citizen had published a few days earlier about spy cases from the Cold War.

One of the stories was about a Soviet double agent, code-named Gideon. The story included a blurry photo of him taken in the 1960s. Gideon had disappeared in the Soviet Union more than 40 years previous and was presumed dead.

“How do you know the story isn’t correct?” I asked. He pointed to the photo of Gideon. “That’s me.” I looked closely at my visitor, saw the identical prominent ears in the old photo, and knew immediately that he was telling the truth.

“My God,” I said. “Please sit down.”

For the full story, click the link: A double agent at the newsroom door.

France Freezes Iranian Intelligence Assets In Sign Of Worrisome Relations

France says it has frozen the assets of Iran’s Ministry of Security and Intelligence, as well as two Iranian men thought to be members of the country’s intelligence service, in a sign of deteriorating relations between the two countries.

The French government made the announcement in its official gazette on October 2, identifying one of the men as Assadollah Assadi, the same name as an Iranian diplomat who has been arrested over an alleged plot to bomb an Iranian opposition group in France in June.

The asset freeze also applied to Saeid Hashemi Moghadam, said to be the deputy minister and director-general of intelligence, and to the interior security directorate of the Intelligence Ministry.

For the full story, click the link: France Freezes Iranian Intelligence Assets In Sign Of Worrisome Relations.

U.S. spies see new threats from global rivals, and say it may be Cold War 2.0

As the intelligence community shifts its primary focus from counter-terrorism to threats from Russia and China, some leaders voice a sense of déjà vu and even eagerness at the challenge.

“It has been a sort of reawakening of times of old, I will say,” said Deputy Director Justin Poole of the National Geospatial-Intelligence Agency, one of the 17 agencies and offices that make up the U.S. intelligence community. “It’s a little more cold war-y.”

President Donald Trump singled out China this week for what he said was an intent to interfere in upcoming midterm elections. In separate speeches, the national intelligence director and the CIA director also emphasized the shift in strategy toward China and Russia, both of which seek to rival the United States on the global stage.

For veteran intelligence officials, the refocusing evokes the more than four decades of the Cold War when intelligence analysts and spies pooled back the capabilities of the Soviet bloc and sought to decipher how it intended to use its weaponry.

For the full story, click the link: U.S. spies see new threats from global rivals, and say it may be Cold War 2.0.
Interesting Reads


The history of espionage is far older than any of today's intelligence agencies, yet the long history of intelligence operations has been largely forgotten. The codebreakers at Bletchley Park, the most successful World War II intelligence agency, were completely unaware that their predecessors in earlier moments of national crisis had broken the codes of Napoleon during the Napoleonic wars and those of Spain before the Spanish Armada.

Those who do not understand past mistakes are likely to repeat them. Intelligence is a prime example. At the outbreak of World War I, the grasp of intelligence shown by U.S. President Woodrow Wilson and British Prime Minister Herbert Asquith was not in the same class as that of George Washington during the Revolutionary War and leading eighteenth-century British statesmen.

In this book, the first global history of espionage ever written, distinguished historian Christopher Andrew recovers much of the lost intelligence history of the past three millennia—and shows us its relevance. (amazon.com)


On August 7, 1998, three years before President George W. Bush declared the War on Terror, the radical Islamist group al-Qaeda bombed the American embassy in Nairobi, Kenya, where Prudence Bushnell was serving as U.S. ambassador. Terrorism, Betrayal, and Resilience is her account of what happened, how it happened, and its impact twenty years later.

When the bombs went off in Kenya and neighboring Tanzania that day, Congress was in recess and the White House, along with the entire country, was focused on the Monica Lewinsky scandal. Congress held no hearings about the bombings, the national security community held no after-action reviews, and the mandatory Accountability Review Board focused on narrow security issues. Then on September 11, 2001, al-Qaeda attacked the U.S. homeland and the East Africa bombings became little more than an historical footnote.

Terrorism, Betrayal, and Resilience is Bushnell's account of her quest to understand how those bombings could have happened given the scrutiny bin Laden and his cell in Nairobi had been getting since 1996 from special groups in the National Security Council, the FBI, the CIA, and the NSA. Bushnell tracks national security strategies and assumptions about terrorism and the Muslim world that failed to keep us safe in 1998 and continue unchallenged today. In this hard-hitting, no-holds-barred account she reveals what led to poor decisions in Washington and demonstrates how diplomacy and leadership going forward will be our country's most potent defense. (amazon.com)

Movies to Watch

Ronin. 1998.

A freelancing former U.S. Intelligence Agent tries to track down a mysterious package that is wanted by the Irish and the Russians. (imdb.com)
### Other Reporting Requirements

<table>
<thead>
<tr>
<th>Incident</th>
<th>Reporting Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents of Security Concern (i.e., Security Incidents)</td>
<td>Report immediately, but do not provide details over the phone. NM: Security Connection (321), CA: Security Connection (321) or DIM (925-294-2600), TTR: Central Alarm Station (702-296-8285) Note: Contractors must also report incidents to their Facility Security Officers.</td>
</tr>
<tr>
<td>Waste, Fraud, &amp; Abuse (WFA)</td>
<td>Report incidents of WFA and criminal matters to Ethics Advisory &amp; Investigative Services (925-845-9900) 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>Counterfeit/Counterfeited Items</td>
<td>Upon discovery of suspect or counterfeit items, report the circumstance or submit questions to <a href="mailto:sqaasci@sandia.gov">sqaasci@sandia.gov</a>, or via <a href="mailto:counterfeit@sandia.gov">counterfeit@sandia.gov</a>.</td>
</tr>
<tr>
<td>Theft of Property</td>
<td>Immediately report any theft of Sandia or U.S. Government property to Property Management (<a href="mailto:loststolen@sandia.gov">loststolen@sandia.gov</a>). 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>Wrongdoing</td>
<td>Report incidents of wrongdoing to Ethics: 925-845-9900. Note: * Incidents of wrongdoing are not limited to items listed elsewhere herein. * You may also report directly to the Office of Inspector General information about wrongdoing by DOE employees, contractors, subcontractors, consultants, grantees, other recipients of DOE financial assistance, or their employees.</td>
</tr>
<tr>
<td>Drug Use</td>
<td>Report the following to Ethics at 925-845-9900: * Positive drug test results (regardless of source [e.g., court system and military testing]) * Incidents of illegal drugs in the workplace. This includes trafficking in, selling, transferring, possessing, or using illegal drugs. Note: * Illegal drugs are prohibited on Sandia-controlled premises and KAFB property. * The use of illegal drugs—or legal drugs in a manner that deviates from medical direction—is a serious offense and could result in termination of your clearance and your employment, as well as arrest.</td>
</tr>
</tbody>
</table>

### Managers

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

### Remote Sites Personnel

Report to SNL/NM, unless otherwise indicated.

### SCI- and SAP-Briefed Personnel

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

---

**DOE and Sandia Reporting Requirements**

**What You Need to Know About Your Reporting Responsibilities**

---

Revised: October 25, 2018

"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
<table>
<thead>
<tr>
<th>Concerns of Personnel Security Interest</th>
<th>Report to...</th>
<th>By this date...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are approached or contacted by ANY individual seeking unauthorized access to classified matter or special nuclear material (SNM).</td>
<td>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 personal security interest.</td>
<td>NM – Ethics Advisory and Investigative Services (505-845-9900), CA – Clearance Processing (925-294-2061)</td>
<td>Immediately.</td>
</tr>
<tr>
<td>Note: Such information must be reliable and relevant, and create a question as to the individual's access authorization eligibility.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Legal</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Are arrested; subject to criminal charges (including charges that are dismissed); receive citations, tickets, or summonses; or are detained by federal, state, or other law-enforcement authorities for violations of the law within or outside the U.S.</td>
<td>NM – Ethics Advisory and Investigative Services (505-845-9900), CA – Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and in writing within the next 3 work days.</td>
</tr>
<tr>
<td>*File for bankruptcy, regardless of whether it is for personal or business-related reasons.</td>
<td>NM – Ethics Advisory and Investigative Services (505-845-9900), CA – Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and in writing within the next 3 work days.</td>
</tr>
<tr>
<td>*Have your wages garnished for ANY reason. Examples: divorce, debts, child support.</td>
<td>NM – Ethics Advisory and Investigative Services (505-845-9900), CA – Clearance Processing (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and in writing within the next 3 work days.</td>
</tr>
<tr>
<td>*Change citizenship or acquire dual citizenship.</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>*Are a foreign citizen who changes citizenship.</td>
<td>NM – Foreign Interactions (505-844-8263), CA – Foreign Interactions (925-294-2061)</td>
<td>Orally within 2 work days of occurrence, and in writing within the next 3 work days.</td>
</tr>
<tr>
<td><strong>Marriage</strong></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 EF 2730-NCR).</td>
</tr>
<tr>
<td><strong>Foreign Travel</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have personal foreign travel to a sensitive country.</td>
<td>CounterIntelligence (505-284-3878)</td>
<td>Prior to travel or as soon as practicable.</td>
</tr>
<tr>
<td>Note: Although 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></td>
<td></td>
</tr>
<tr>
<td><strong>Interaction</strong></td>
<td></td>
<td></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>Foreign National Contacts Reports (online application)</td>
<td>Note: You can find this site by searching “contactreports” (one word) in Technet.</td>
<td></td>
</tr>
<tr>
<td>Note: “Substantive contact” refers to a personal or professional relationship that is enduring and involves substantial sharing of personal information and/or the formation of emotional bonds (does not include family members). At SNL, substantive contact includes associations that involve meeting and the sharing of SNL business information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are employed by, represent, or have other business-related associations with a foreign or foreign-owned interest, or with a non-U.S. citizen or other individual who is both a U.S. citizen and a citizen of a foreign country.</td>
<td>NM – Ethics Advisory and Investigative Services (505-845-9900), CA – Personnel Security (925-294-2061)</td>
<td>Immediately.</td>
</tr>
<tr>
<td>Have an immediate family member who resides 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></td>
<td></td>
</tr>
</tbody>
</table>
China’s Trade Practices and Your Procurements

By Gabrielle Holcomb

If you have been reading, watching, or listening to the news you may have heard all the commotion surrounding the recent trade tariffs regarding section 301 if the Trade Act if 1974. Under this section, the United States Trade Representative or USTR, initiated an investigation (reference Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer; Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974-March 22, 2018) to determine if China had acted in a discriminatory or unreasonable manner in relation to technology transfer, intellectual property, and innovation that would burden or restrict US commerce. The investigation found the following:

- China requires or pressures US Companies to transfer technology to them by use of joint venture requirements, foreign investment restrictions, and administrative review and licensing processes.
- China deprives US companies of the ability to set market-based terms in licensing and other technology related negotiations.
- China directs and unfairly facilitates the systematic investment in, and acquisition of, US companies, and assets generate and gain large-scale technology transfer.
- China conducts and supports cyber intrusions into US commercial computer networks to gain unauthorized access to commercially -valuable business information. (Reference Section 301 Investigation Fact Sheet June 2018 from USTR)

How does this affect you?

- Well, in response to these trade violations, the US has decided to impose a 25% tariff on approximately $50 billion of products from China that are strategically important to, and benefit from, the “Made in China 2025” program and other Chinese industrial policies. See the current list of products that are and will be affected by these tariffs here.
- With the trade tariffs in place, the rise in counterfeit products will only increase as individuals and companies in the US seek cheaper products, unfamiliar with why their products prices have gotten so expensive. The balloon effect for counterfeiters will be enormous and full of opportunity. This is a scary thought, which means many of us at the laboratory must be vigilant for these dangerous items.

What can you do?

- Be aware of the fact, that items on the list of products will now have this tariff, so the price will increase soon, if it hasn’t already. Plan for this.
- Try to work with US companies as much as possible.
- Be vigilant for suspect and counterfeit items. These will increase over the coming months. If you have questions or need to report an item visit our webpage at counterfeit.sandia.gov or email us at sgasci@sandia.gov
- Engage in Supply Chain Risk Management! Know your QLI Visit the SCRM webpage to learn more.
After reading all the modules of SEC100, complete this form and send it via email to securityed@sandia.gov or via fax to 505-844-7802 to receive credit.

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

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

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

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

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

Security+ YOU

Think. Assess. Protect.
SEC100 Feedback form

Your feedback is important to us. Please complete this evaluation and send it to us via email at securityed@sandia.gov or via fax at 505-844-7802.

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

The ease of use for this learning. 1 2 3 4 5
The organization of the information presented. 1 2 3 4 5
The usefulness of the information presented. 1 2 3 4 5
Your level of knowledge related to this topic BEFORE using this tool. 1 2 3 4 5
Your level of knowledge related to this topic AFTER using this tool. 1 2 3 4 5

Enter feedback below.
What was the most valuable about this learning tool?

Does any information need to be clarified? Please explain.

What could be done to improve or enhance this learning tool?