# Introduction

## Welcome to this year's SEC100

SAND2013-8270P

**The Threat is Real**
Each day at SNL, our information is threatened by cyber hackers, foreign adversaries, malicious insiders, or is subject to inadvertent release. The work that we do at SNL is cutting edge, and others want that information—whether classified or not. They can reap rewards from our bright minds without paying the price. This briefing gives you the tools you need to help keep our information safe and secure.

**What you can do: Think.Assess.Protect.**
Most security requirements, in one way or another, are about ensuring information and material are kept from those who don't have a need to know (NTK): both inside and outside SNL. By applying NTK and remembering to "Think.Assess.Protect.," you can help keep our nation's information safe and secure.

**Another Adventure with Sam.**
Last year, we helped Sam Seriously make good security choices during a day at SNL. This year, we'll follow Sam through several more challenges that often occur at the Labs. Unfortunately for Sam, not every challenge is easy. As we go through the briefing, you and Sam will have opportunities to apply some core security principles.

Click BEGIN below to start the modules.

*Module 1: Overview and tools*
*Module 2: Know your work*
*Module 3: Know your surroundings*
*Module 4: Who needs to know*
*Module 5: Seeking help*
*Module 6: Protecting export information*
*Module 7: Final tips*

# Module 1: Overview and Tools

## What is a national security laboratory?

DOE's 17 national laboratories grew out of the massive scientific endeavors of World War II. New technologies such as radar, computers,  proximity fuses, and the atomic bomb proved decisive for the Allied victory. After the war, the newly created Atomic Energy Commission took over the wartime laboratories, and cemented their existence. Additional "national laboratories" were created, each typically centered around one or more expensive machines (e.g., particle accelerators or nuclear reactors).

Today, DOE provides more than 40% of the total funding for physics, chemistry, materials science, and other technical fields. The national laboratories themselves, however, are managed by private companies or universities. As a system, the labs form an overarching and far-reaching component of what is known as the "iron triangle": military, academia, and industry. Our national laboratories also represent what may be the world's largest scientific research system.

**For these reasons, other nations and companies are very interested in the innovative work being performed at SNL.**

[redacted]

## Did you know?

### 1948: President Truman establishes civilian control of the U.S. nuclear arsenal

*"I do not want to have some dashing lieutenant colonel decide when would be the proper time to drop one."*

Separation of knowledge between the military and civilians is the foundation of compartmentalization; it helps ensure that no one has more information or power than they need. Civilians like you help maintain a proper balance.

## Security needs you

You are the first line of defense in protecting our nation's information. An easy way to do this is by applying the core principles of Operations Security, or OPSEC:

- **Think:** Recognize and acknowledge that you are at risk.
- **Assess:** Evaluate your routines and environment. Where are you vulnerable? Are you willing to accept those vulnerabilities?
- **Protect:** Adopt countermeasures. Make security part of everything you do. Protect our nation by protecting our information.

Let's see how this works in an "everyday" example. Driving to work, you can't remember whether you locked the front door of your house. What would you do? You might **THINK,** "Did I lock it or not?" You'd then **ASSESS** the risks (burglary, vandalism, etc.). Most likely, you'd choose to **PROTECT** your property by returning home to ensure the door is locked.

## You never need to guess

Remember, at SNL you never have to guess. Your manager, your Derivative Classifier (DC), and your Classified Administrative Specialist (CAS) are always available if you have questions. In addition, you may use one of the resources cited in the box on the right side of this page.

### There are lots of ways to get help!

- Call 3-2-1 from any SNL phone (505-845-1321 off site) to reach the Security Connection (get live assistance to address any security issue)
- Visit the Sandia Security website (get an answer to any security question)
- Visit the DC/UCNI RO database (find a DC or UCNI RO within your organization)
- Call the Security Incident Management Program (SIMP) at 505-283-SIMP (to report an incident of security concern or get help after hours)
- Contact your Classification Office (for assistance with classification-related issues)

## What causes mistakes?

Here are some reasons why good people make mistakes.

- **Being in a hurry:** Rushing causes us to lose focus. Slow down to stay safe and secure.
- **Not taking the risk seriously:** If you don't believe there's a threat, you won't implement protections.
- **Waiting to report/assuming everyone had gone home:** Delays in reporting only make the consequences worse. The sooner mitigating measures are put in place, the less information may be lost, if any. Report as soon as you suspect you may have made or seen a mistake.
- **Disruption in routine:** Establishing routines helps us, whether it's storing our personal electronic devices in the morning or locking our computers when we leave our offices. It's when we do something out of the ordinary that we make mistakes, such as rushing to an appointment and leaving classified unattended, or putting on a winter coat and forgetting there's an electronic gadget in one of the pockets. If you do something out of the ordinary, take extra care.
- **Being interrupted/distracted:** A coworker walking in to discuss an urgent issue or receiving an emergency call from home can cause us to forget what we were doing. Be careful if you are interrupted, and be mindful when you interrupt others.

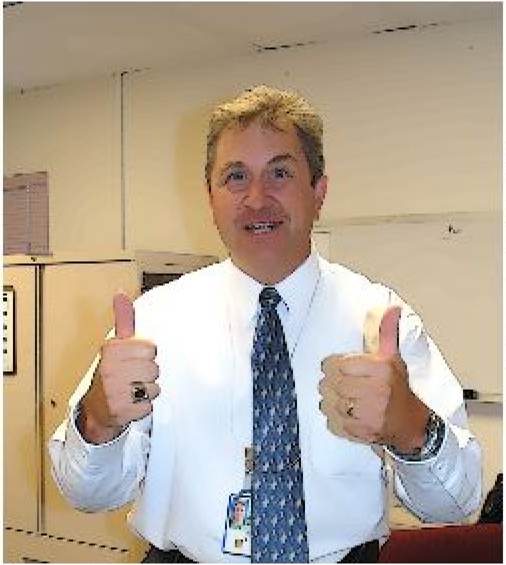
[redacted]

## Did you know?

**New Mexico** is a hot spot for spies. Counterintelligence expert Bruce Held says, "for many international intelligence operatives, the state's name is nearly synonymous with espionage."

According to the FBI, **Silicon Valley** (near Sandia's California campus) is also a hotbed of espionage. The valley is home to many of the estimated 3,000 front companies nationwide, set up by foreign countries to steal secrets and acquire technology.

# Meet Sam...

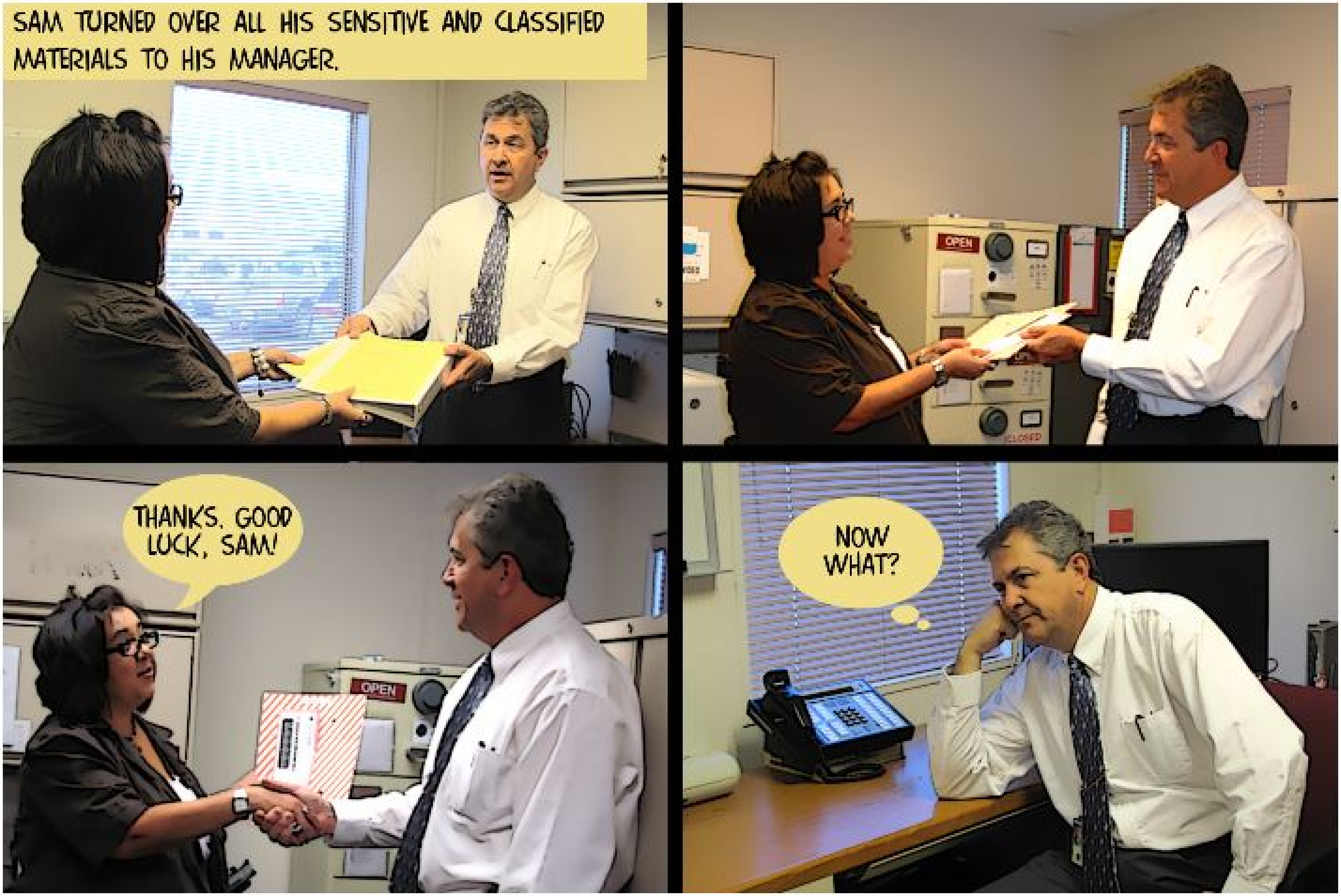


Sam is a seasoned engineer who has been working at SNL on the Super-Secret Ray Gun (SSRG) project for the past 8 years. He has a Q-clearance and currently works inside a Limited Area.

Given Sam's experience with the SSRG, his manager recently tasked him with supporting another organization conducting R&D on an unclassified trigger component. The new component is being designed for multiple applications, including those for the SSRG.

# Module 2: Know your work

Sam started his new job today. Sam transitioned his classified and unclassified sensitive work on the SSRG to his previous manager.


SAM TURNED OVER ALL HIS SENSITIVE AND CLASSIFIED MATERIALS TO HIS MANAGER.
OPEN
CLOSED
THANKS, GOOD LUCK, SAM!
OPEN
NOW WHAT?

What Should Sam Do?

Familiarize himself with the websites and staff of his new organization.

Contact his new manager to see if there is anything he needs to know before beginning work.

**Your Answer:** Familiarize himself with the websites and staff of his new organization.

*Close but, Security Ed has a few reminders...*

Getting familiar with your new organization's staff, mission, and tools before starting work is always a good idea. Sam should also talk to his new manager to ensure he understands the sensitivities of his new work.

If Sam understands what needs protection, and the risks associated with its loss, he can implement measures to protect it.

It's as simple as remembering the Operations Security concepts and adopting a mindset to **Think.Assess.Protect!**

**Your Answer:**

Contact his new manager to see if there is anything he needs to know before beginning work.

*Good job, this is what Security Ed suggests...*

By talking to his manager, Sam now understands the sensitivities of his new work. Of course, it would also be valuable to understand the mission, tools, and staff of his new organization.

If Sam understands what needs protection, and the risks associated with its loss, he can implement measures to protect it.

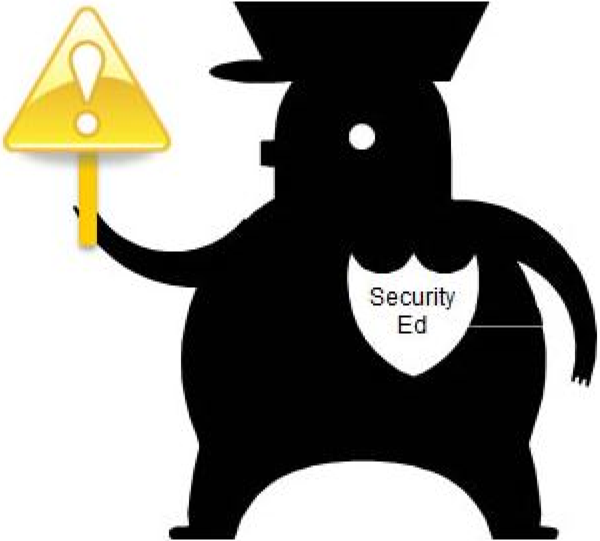
It's as simple as remembering the Operations Security concepts and adopting a mindset to **Think.Assess.Protect!**

## Security Ed says...

When you start new work, be sure you understand:

- What is sensitive or classified in your new subject area.
- What may be subject to export controls.
- Who can help.
- Know your Derivative Classifier (DC), Classified Administrative Specialist (CAS), manager, and subject matter experts (SMEs).
- What could be an indicator or pathway.
- Do budgets, customers, or schedules provide information that an adversary could use?

When you're in doubt or new to an activity, ask questions. It's better to be safe than sorry.



## Know your work

Something that doesn't seem like a big deal to you could be the last piece of the puzzle for an adversary. Ask yourself:

- What parts of my work might be useful to an adversary?
- Who has need to know (NTK) for my program's information?
- Whom do I ask if I need help?

## Think like an adversary

Some common indicators that could lead an adversary down a pathway to more information:

- Increased program activity that can be seen by the public (e.g., movement of vehicles, shipments, increase in staffing).
- Information in presentations, articles, research papers, and journals.
    - Remember, **all** information intended for release outside of SNL must go through Review and Approval, even open source or unclassified.
- Information in waste streams (recycle bins, trash cans).

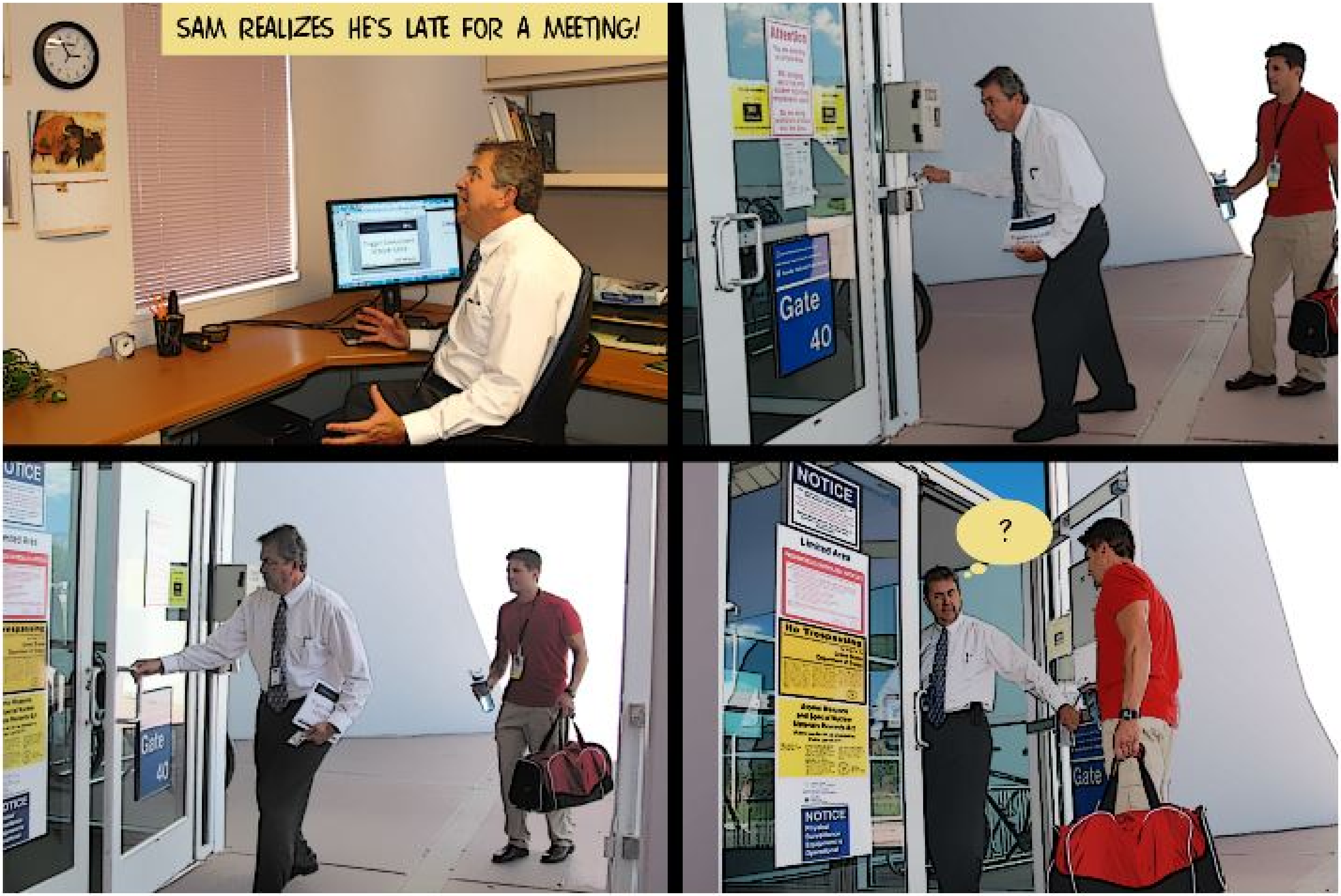
## Recycle diligently

All of SNL/NM's white paper collected for recycle has to be sent to an approved domestic mill for witnessed recycling/destruction due to UCI being incorrectly placed into the recycle bins.

Be aware of what you put in recycle bins. And if in doubt, shred it with an approved shredder. Remember, **Think.Assess.Protect!**

# Module 3: Know your surroundings

Sam is off to attend his first project meeting with his new team, but he got lost and now he's a little bit late. Sam badges in and hurries through the door. Meanwhile, another employee, who is busy checking the time on his Polar Heart Rate Monitor watch, grabs the door behind him and attempts to enter the building without badging in.

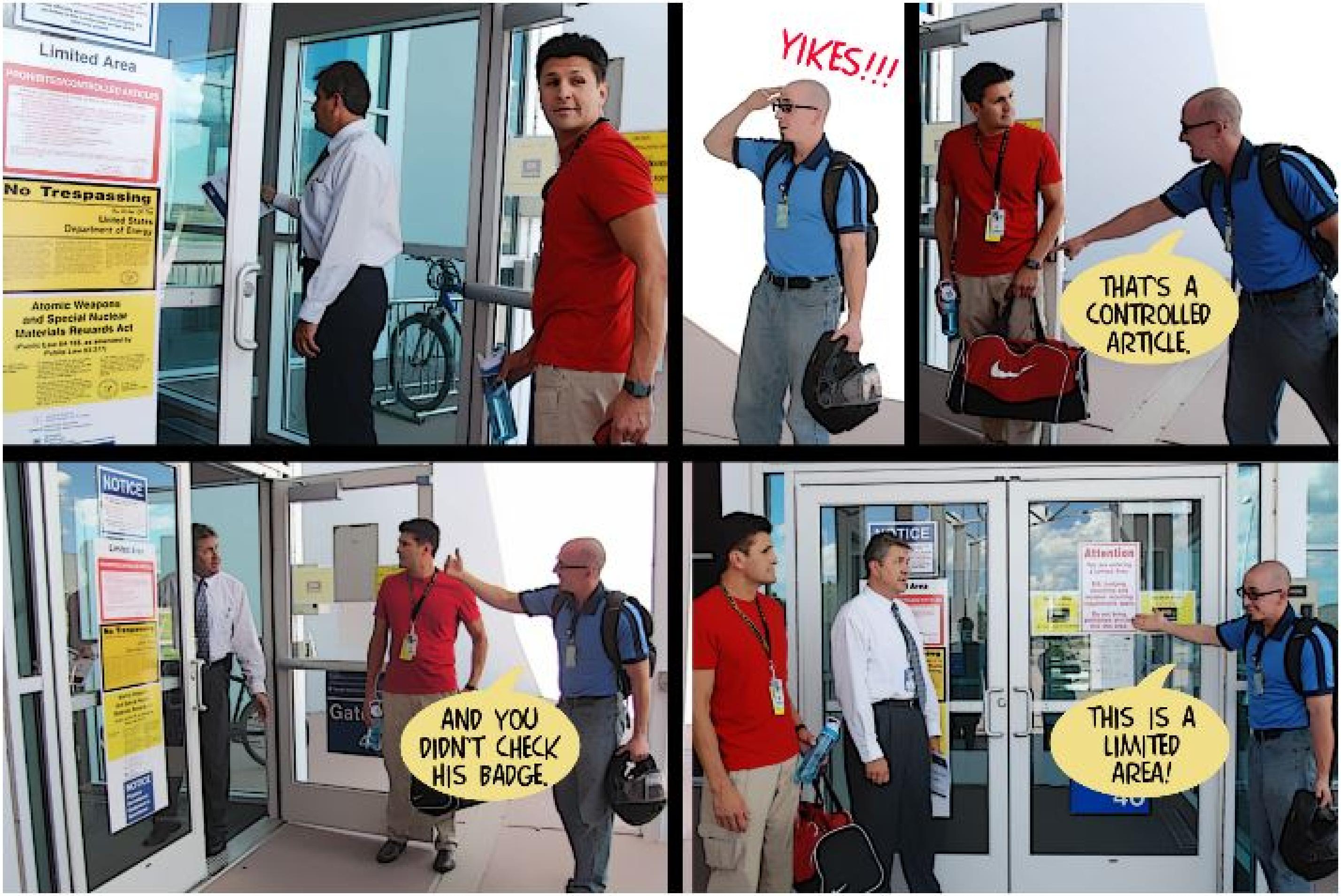


**What Should Sam Do?**

Continue on to his meeting. The individual has a badge and obviously works at SNL. Sam is in a hurry and this is probably a new coworker he'll meet soon.

Stop the individual and tell him that he needs to badge in separately.

**Your answer:** Continue on to his meeting. The employee has a badge and obviously works at SNL. Sam is in a hurry and this is probably a new coworker he'll meet soon.

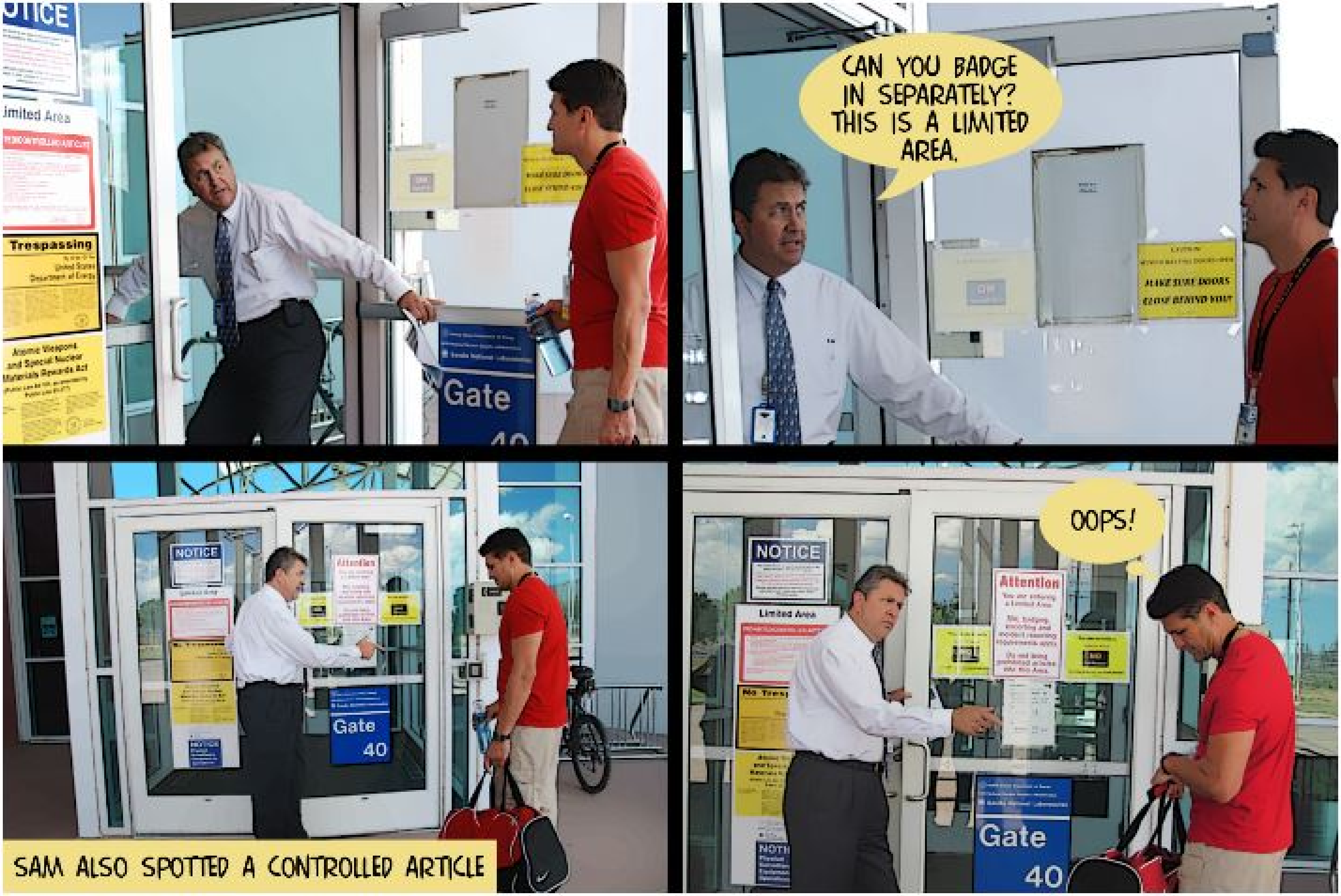

Limited Area
No Trespassing
United States Department of Energy
Atomic Weapons and Special Nuclear Materials Rewards Act
YIKES!!!
THAT'S A CONTROLLED ARTICLE.
NOTICE
AND YOU DIDN'T CHECK HIS BADGE.
Attention
THIS IS A LIMITED AREA!

*Oh no, Sam. Security Ed has a few reminders…*

By doing this, Sam puts himself at risk of accepting responsibility for someone he does not know and for any controlled or prohibited items that that person may be carrying, such as the Polar Heart Rate Monitor watch, which is a controlled article*. Luckily, another employee stopped the individual with the watch and pointed out that such devices are not allowed in Limited Areas. The employee also reminded Sam that it's a wise practice to ask unknown individuals to badge in separately.

*Controlled articles include electronic devices that can record, capture, or store information.

**Your Answer** Stop the individual and tell him that he needs to badge in separately.


NOTICE
Limited Area
Trespassing
Atomic Weapons and Special Nuclear Materials Rewards Act
Gate 40
CAN YOU BADGE IN SEPARATELY? THIS IS A LIMITED AREA.
MAKE SURE DOORS CLOSE BEHIND YOU
Attention
SAM ALSO SPOTTED A CONTROLLED ARTICLE
OOPS!

*Good job, Sam. This is what Security Ed suggests...*

By asking the individual to badge in separately, Sam ensured that the individual did indeed have access authorization.

It's important for Members of the Workforce to take the time to properly badge in, enter their PINs, ensure that they are not carrying prohibited or controlled articles, and ensure that the doors close properly behind them.

Sam also reminded the individual that his watch is a controlled article* and suggested that the device be stored outside the Limited Area.

*Controlled articles include electronic devices that can record, capture, or store information.

## Security Ed says...

Don't let being in a rush or making assumptions stop you from asking someone you don't know to badge in separately. That person could have been terminated, lost their clearance, or not even work here! Take access controls seriously; don't let unauthorized people into SNL.

Remember that there is a difference between escorting and vouching.

**Escorting** - Situation in which a cleared individual is responsible for an uncleared individual at all times, ensuring that the uncleared person does not access classified or sensitive information, or areas that may have safety hazards for which the individual is not trained.

**Vouching** - Situation in which one properly badged individual allows another properly badged individual into an area (i.e., without requiring the other person to badge in separately). To vouch, you must check the other person's badge photo and expiration date. Vouching should be used in rare cases, such as when a trusted coworker is carrying a large package.

Don't let people sneak in behind you without making sure they should be here.

# Understanding prohibited and controlled articles

**Prohibited articles** are typically things that can hurt you, such as guns, fireworks, or illegal drugs. They are not allowed on **Sandia-controlled premises.**

**Controlled articles** are typically thought of as "anything that can record, store, or transmit data." Because of these capabilities, they are not allowed where classified processing occurs: Limited Areas and more restricted areas. Aside from cell phones and cameras, this includes, but is not limited to, GPS watches and any type of pedometer other than SNL's Virgin Health Miles pedometer.

All Sandia-owned items that meet the controlled articles criteria (see IM100.1.2, Manage Controlled Electronic Devices and Media) must be registered.

## But wait, there's more!

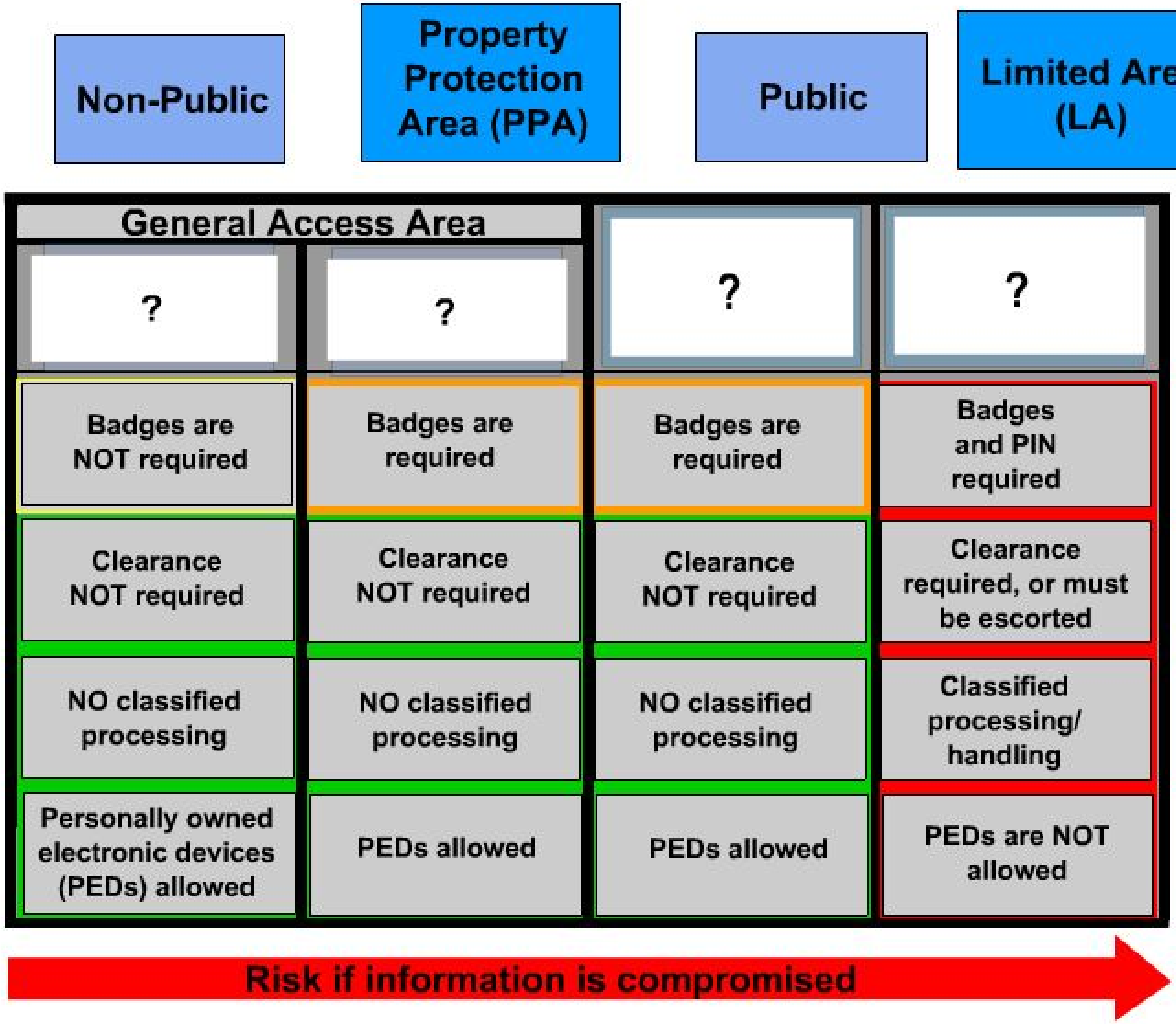
**Additional information and assistance**

- IM100.1.2, *Manage Controlled Electronic Devices and Media*
- ISS100.5.1, *Manage Controlled and Prohibited Articles*
- ISS100.5.2, *Conduct and Report Technical Surveillance*
- ISS100.5.3, *Control Site Access*
- Sandia Security website

## Protection is based on risk

Each area is designed with risk in mind: Public Areas, have open access, while Limited Areas require two-factor authentication (badge in and PIN) because of classified processing. As the desirability/sensitivity increases for the information in the area, so do the security controls. That's why not all areas at SNL are Limited Areas. In other words, let the security area fit the work.

**Drag & drop the column headings. Incorrect placements will bounce back.**



Non-Public

Property Protection Area (PPA)

Public

Limited Area (LA)

| General Access Area | | | |
|---|---|---|---|
| ? | ? | ? | ? |
| Badges are NOT required | Badges are required | Badges are required | Badges and PIN required |
| Clearance NOT required | Clearance NOT required | Clearance NOT required | Clearance required, or must be escorted |
| NO classified processing | NO classified processing | NO classified processing | Classified processing/ handling |
| Personally owned electronic devices (PEDs) allowed | PEDs allowed | PEDs allowed | PEDs are NOT allowed |

# Module 4: Who needs to know

Since it is Sam's first day with his new team, his teammates invite him to join them for lunch at the Sandia cafeteria.

During lunch, Sam's teammates attempt to get to know him by asking him questions, such as where he went to school, how long he's been at Sandia, and details about the type of work he did for the SSRG project.

Sam knows that the SSRG project is classified.

GRILL
SAM'S NEW COWORKERS TAKE HIM TO LUNCH.
SO, TELL US ABOUT THE SSRG...
WELL...

What Should Sam Do?

Answer their questions. After all, Sam was asked to join his new team because of his SSRG experience. Plus, his teammates are all Q-cleared and they're having lunch on Sandia-controlled premises.

Express concern that they do not have a need to know (NTK) for the SSRG project and move onto another topic.

Your Answer: Answer their questions. After all, Sam was asked to join his new team because of his SSRG experience. Plus, his teammates are all Q-cleared and they're having lunch on Sandia premises.

THE SSRG WAS GREAT!!!
OH BOY! SSRG INFO!
SAM'S COWORKER STOPS HIM. THIS IS A PUBLIC AREA! WHO KNOWS WHO MAY BE LISTENING!

*Oh no, Sam! Security Ed has a few reminders...*

Sam is talking to other cleared employees on Sandia-controlled premises but he shouldn't share information with others unless he is sure they have a need to know (NTK). Even people who work in the same subject area or department might not have the same NTK.

Luckily, one of Sam's new colleagues pointed out that SSRG is a classified project and should not be discussed in a public area.

**Your Answer:** Express concern that they do not have a need to know (NTK) for the SSRG project and move onto another topic.

UM...
PLEASE GO ON!
SORRY...
SAM REMINDS THEM THAT THEY MUST HAVE NTK, AND THEY ARE IN A PUBLIC AREA. THEY CHANGE THE TOPIC TO SPORTS.

*Good job, Sam. This is what Security Ed suggests...*

Sam knows that people who work in the same subject area or department might not have the same NTK. He is correct to not share information, even though they have clearances and are working on a related component.

Since he's new, he's uncomfortable sharing information until he verifies NTK.

Plus, the topic is classified and they're in a public area.

# Security Ed says...

It's important to remember that someone may have the appropriate clearance to discuss classified information, but they must also have NTK.

In addition, the Sandia cafeteria may be on Sandia-controlled premises, but it is a Public Area, which means it is open to anyone, cleared or not. Therefore, discussing classified information in such a place is prohibited.

Be mindful of what type of area you are in before discussing classified or sensitive subjects. Classified conversations must be held in Limited Areas or more restricted areas.

[redacted]

## Think about where you are and what information you have...

Apply NTK to all of your work, not just classified. Sensitive information, or Unclassified Controlled Information (UCI), must also be protected.

Each type of UCI (shown in the graphic) has different protection strategies (marking, handling, and disposal) based on the risk to the nation if it were to be compromised. Learn more about the different types of UCI by consulting IMI100.2.5, *Identify and Protect Unclassified Information*.

[redacted]

### Remember...

Compromise of some UCI, like Export Controlled Information (ECI) or Unclassified Controlled Nuclear Information (UCNI), whether intentional or not, constitutes a security incident and violates federal law. Compromise can also subject SNL to fines by the State Department or Department of Commerce.

# Module 5: Seeking Help

Later in the week, Sam is tasked with developing a presentation for a new trigger component for an internal customer.

Sam's new teammates provide the necessary information via e-mail, which Sam then compiles into a presentation. Sam is told that all of the various pieces of information are unclassified since they were gathered from open sources (e.g., the external web) or unclassified project information. However, Sam remembers the catchphrase "**Think.Assess.Protect.**" and decides to get the presentation reviewed by a Derivative Classifier (DC), just to be sure.

Unfortunately, Sam can't find the DC for his new organization, and his deadline is fast approaching.

SAM USES THE INTERNET AND EMAILS FROM PEERS TO CREATE A PRESENTATION ABOUT THE TRIGGER COMPONENT.
Trigger Component
SCSQJR-SARJE
Sam Seriously
Goog
I NEED A DC REVIEW, BUT THE DC ISN'T HERE.

What Should Sam Do?

Ask the DC from his old organization to review the presentation.

Contact the Classification Office.

Your Answer: Ask the DC from his old organization to review the presentation.

SAM VISITS THE DC FROM HIS OLD PROJECT...
SORRY, SAM. THIS ISN'T MY SUBJECT AREA. CLASSIFICATION CAN HELP.
LATER, AT THE CLASSIFICATION OFFICE, THE PRESENTATION IS REVIEWED.
YOU'RE GOOD TO GO, SAM.

*Close but, Security Ed has a few reminders...*

Sam did the right thing by deciding his presentation needed to be reviewed by a DC; however, not all DCs are interchangeable. DCs have specific subject-matter expertise, which means that Sam must request a review by a DC who is knowledgeable in the area which he or she is authorized to derivately classify.

The DC he contacted recognized the subject matter as being outside his area of expertise and referred Sam to the Classification Office.

Your Answer:

Contact the Classification Office.

SAM RUSHES TO THE CLASSIFICATION OFFICE...
Gate 2
1108
CAN YOU REVIEW THIS?
GETTING A PROPER REVIEW WAS THE RIGHT THING.
YOU'RE GOOD TO GO, SAM!

*Good job, Sam. This is what Security Ed suggests...*

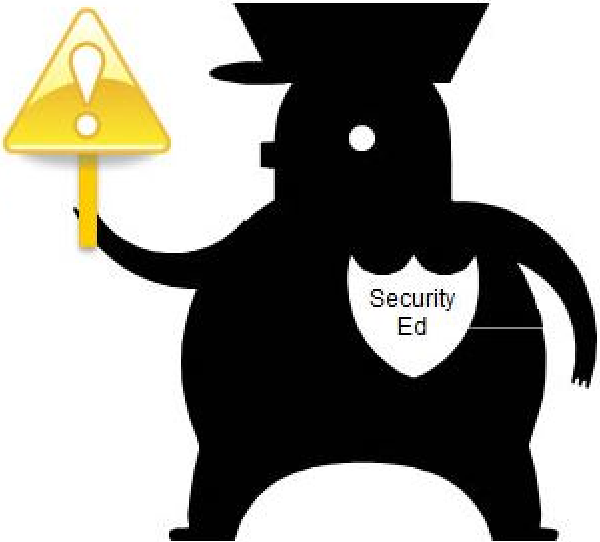
Since DCs have specific subject-matter expertise, Sam's best option is to contact the Classification Office rather than going to a DC outside of his new organization. Sam realizes that the DC for his old program may not have the necessary expertise to make a qualified determination about his presentation.

## *Security Ed says...*

Even though information may start out as unclassified, associating it with other unclassified information—known as "compilation"—may result in the combined information being classified.

If you work in a classified subject area, you must have your DC review any new information you create. However, it's a good idea to get a DC review anytime you're in doubt—whether you work in a classified subject area or not.

For questions or additional information, contact your Classification Office.



## Why we classify

- Classification is the identification of information that needs to be protected. By classifying information, we establish additional protections while allowing its use by individuals with the appropriate access authorization, clearance, and NTK.
- If you release classified, whether intentionally or not, that constitutes a security incident and violates federal law. Protect yourself by using the resources available to you, including DCs, the
- Classification Office, your CAS, and the online Review & Approval process. Ignorance is not an excuse for failing to protect our nation's information.

## No comment! Think before you speak.

- Accidental or unintentional release of classified information by others does not mean that the information has been declassified. If you see something you know is sensitive/classified, don't say anything.
- DOE's "No Comment" policy requires that you neither confirm nor deny public statements concerning potentially classified information, whether online (e.g., chat rooms) or in person. When in doubt, refer inquisitors to Media Relations.

## Disagree or need to downgrade?

- If you believe that information has received an incorrect classification determination, you may challenge it. The Classification Office can help you resolve concerns.
- If you need to declassify or downgrade existing classified matter, be aware that all such determinations require a review by a Derivative Declassifier (DD) in the Classification Office. Consult your DC to begin either process.

## But wait, there's more!

### Online resources

- CLA102, Classified Programs Initial Awareness Briefing
- ISS100.1, Perform Classified Work
- ISS100.1.1, Identify Classified Information
- ISS100.4.4, Control Classified Visits Involving Cleared Foreign Nationals
- Subject-Matter-Related Classification Briefings
- Sandia Security website
- DC/UCNI RO database

# Module 6: Protecting Export Information

Now that Sam's presentation has been properly reviewed by a DC, he's ready to brief his internal customer.

Twenty minutes before the meeting, Sam's customer informs him that two Australians, who are visiting SNL, would like to sit in on the meeting. The Australians are aware of the new trigger component, and it could be of value to them as well. The customer assures Sam that both foreign nationals are cleared, but Sam knows that if he proceeds with the briefing, he may commit an export violation.

SAM'S CUSTOMER WANTS HIM TO MEET SOME PEOPLE.
RED BADGES!
THEY'RE FOREIGN NATIONALS...
SAM, THEY'D LIKE TO SEE YOUR PRESENTATION.

**What Should Sam Do?**

Request that the Australians not be present during his briefing.

Proceed with the briefing as scheduled. Sam trusts his customer.

Your Answer: Request that the Australians not be present during his briefing.

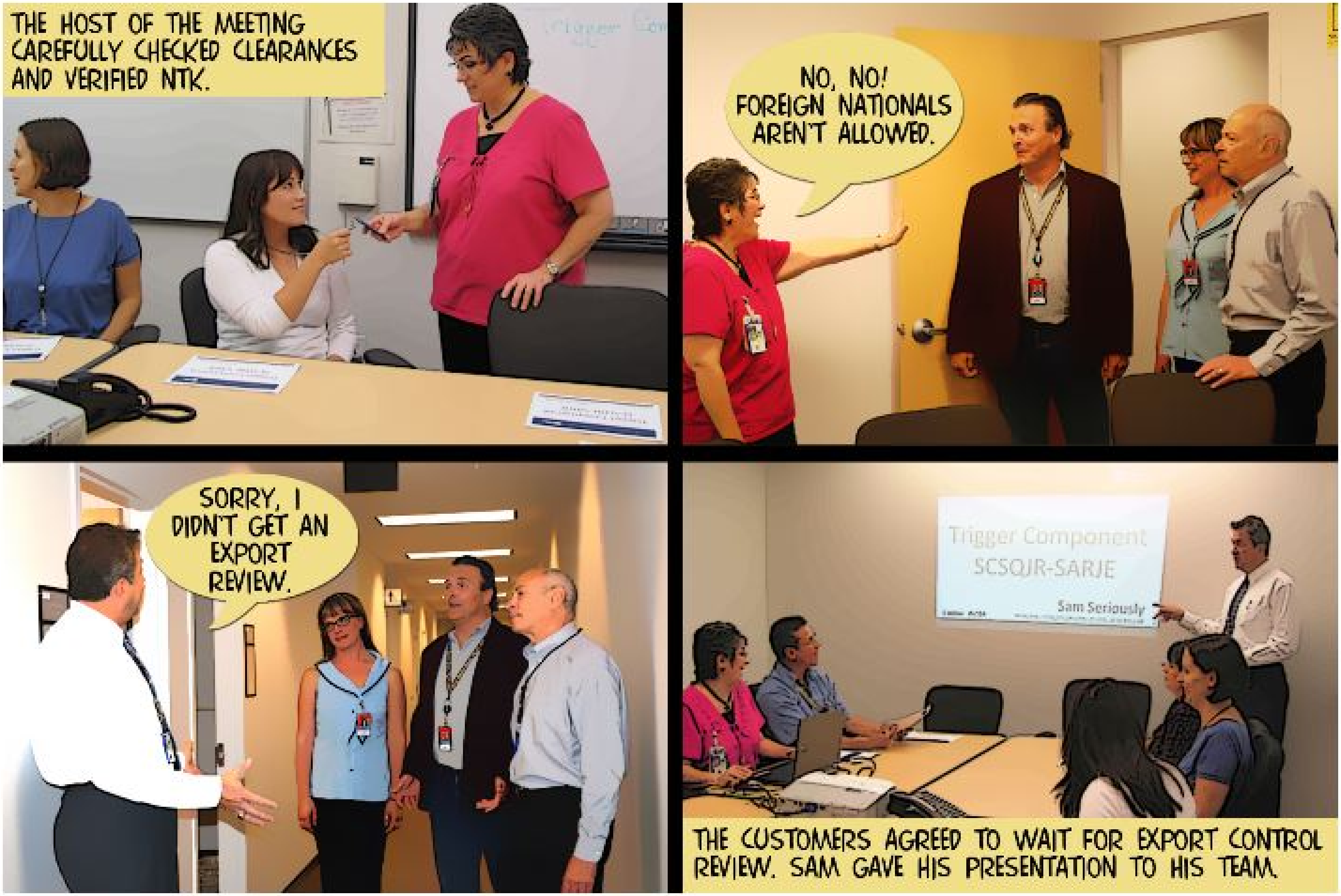
I'M SORRY! I CAN'T...
MY PRESENTATION WASN'T REVIEWED FOR EXPORT CONTROL.
THAT'S TOO BAD!
EVERYONE UNDERSTOOD AND AGREED TO WAIT FOR THE RIGHT REVIEWS.

*Good job, Sam. This is what Security Ed suggests...*

Although Sam's presentation was reviewed by a DC for a classification determination, the presentation also needs to go through Sandia's **Review and Approval process** before it can be released to any external persons or agencies, including foreign nationals.

Since there isn't enough time to submit his presentation through Sandia's Review and Approval process before the meeting, Sam should not disclose any presentation material to the Australians.

Your Answer: Proceed with the briefing as scheduled. Sam trusts his client.


THE HOST OF THE MEETING CAREFULLY CHECKED CLEARANCES AND VERIFIED NTK.
NO, NO! FOREIGN NATIONALS AREN'T ALLOWED.
SORRY, I DIDN'T GET AN EXPORT REVIEW.
Trigger Component
SCSQJR-SARJE
Sam Seriously
THE CUSTOMERS AGREED TO WAIT FOR EXPORT CONTROL REVIEW. SAM GAVE HIS PRESENTATION TO HIS TEAM.

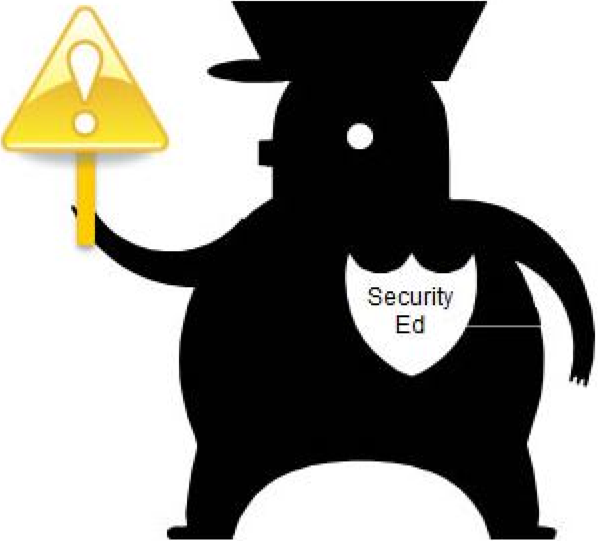
*Oh no, Sam. Security Ed has a few reminders... ...*

Luckily, the host of the meeting checked all participants' clearances and need to know (NTK) before beginning the presentation. Noting the presence of foreign nationals, the host also asked if Sam's presentation had been cleared through Sandia's **Review and Approval process.**

Since it had not, the Australians couldn't attend the presentation. They understood, as they were familiar with export-control protocols.

## *Security Ed says...*

Regardless of a foreign national's clearance level, you must control all scientific or technical information as export-controlled information (ECI) unless it has been legally released into the public domain or has been determined to be Unclassified Unlimited Release (UUR) information.



# Collaboration with foreign nationals

Working with foreign nationals provides a great opportunity for collaboration and new points of view. However, don't forget that:

- A Foreign National Request Security Plan (FNR SP) is necessary for every foreign national at SNL. These plans outline where the foreign nationals may go, what hours they can be in those areas, and who can escort/host them. If you're not listed as an escort on an applicable FNR SP, do not take responsibility for escorting. An FNR SP must also be in place even if you are having business interactions with a foreign national off site.
- Anyone who will work with foreign nationals, either at SNL or off site, needs to take the course EC100, *Export Control*.

## Learn more about export controls

**Additional information and assistance**

- Fact sheet: What Do I have To Do with Export/Import Control?
- EC100, *Export Control Awareness Training*
- ISS100.4.3, *Comply With Export/Import Controls*

# Module 7: Final Tips

## Security incidents at SNL this year....

In addition to recognizing contributing factors, SNL's Security Incident Management Program (SIMP) also notices trends. Here are trends we've seen this year:

- Starting classified discussions, especially in offices, before verifying that there are no SNL BlackBerries or iPhones present. Always verify that there are no cell phones, and that everyone has the right clearance and NTK before beginning a potentially classified discussion.
- Compilation of information in email, especially in attachments and replies. Be careful when email strings get long. Start a new email, call, or have a meeting.
- Using open source material SNL documents that is later found to be classified. Open source should not be assumed to be unclassified.
- Working from home on classified subject areas, which has resulted in classified on unapproved systems.
- Classified being sent to large distribution lists or located on server/SharePoint sites with large access lists.

[redacted]

An **incident** is a **potential** violation of security requirements, which...

- Must be investigated.
- Can result in the damage to national security.

***... in other words, information may have been compromised.***

Willful or grossly negligent behavior, not reporting an incident timely, or failure to cooperate with an inquiry will result in an **infraction.** If the individual's behavior was not negligent, the incident will not result in infraction.

## Meanwhile, in your real life...

Sam has had a busy week! He narrowly avoided some tricky issues. But things happen outside of work too. If you get in trouble with the law, get married, change your name, travel internationally, have problems with debt, seek help with substance or alcohol abuse, or a variety of other things, you report to SNL.

The reason for this type of reporting is to ensure that you are trustworthy and an acceptable risk. In addition, reporting these circumstances helps mitigate the potential that you can be targeted or blackmailed.

The DOE and Sandia Reporting Requirements pamphlet provides a complete list of "concerns of personnel security interest," all of which are reportable within specific time frames.

[redacted]

## But wait, there's more!

**Additional information and assistance**

- ISS100.3.1 *Report Personnel Security Information; Security Incidents; and Waste, Fraud, and Abuse*
- DOE and Sandia Reporting Requirements
- Sandia Security website

# Farewell!

Thanks for sticking with Sam as he began his new project. We hope you go forward with new tools and a **"Think.Assess.Protect."** mindset.

Always be willing to ask questions. When in doubt, or if something doesn't feel right: Consult your manager or team lead.

Talk to your Derivative Classifier (DC) or Classified Administrative Assistant (CAS). Call 3-2-1 (505-845-1321 offsite) for help.

With these resources, there's no reason to guess or assume.

**Remember:** You are our best defense. Help protect our nation every day by staying alert and aware.

**Think • Assess • Protect**

*Keep Sandia Secure* security.sandia.gov