Counterintelligence and OPSEC Courseware

Module 1: Introduction

Lesson 1.0: Introduction

Welcome to the NSA's annual Counterintelligence, OPSEC, and Unauthorized Disclosure Refresher Course. Please allow yourself 45 minutes of uninterrupted time to complete this course.

Lesson 1.1: Opening Video

At any given moment, there are numerous countries spying against the United States – from our most dangerous enemies to some of our closest allies. They want our information. Our technology. Our deepest secrets. And while many of these threats come from the outside, perhaps the greatest security concern facing the nation today comes from within our most trusted circles. This concern is often – and correctly called… The Insider Threat. Millions of people are trusted with America's most important secrets. Vetted personnel who've made promises to protect this information at all costs. Millions of cleared people - but it takes just one person to undo it all. To waste years of research… to squander millions of dollars in technological innovation… to put thousands of people in harm's way. Our information is valuable and the economics of espionage are simple. Why spend billions developing a military program when you can spend a fraction of the cost to simply steal it? But beyond money, imagine how U.S. critical information could allow adversaries to exploit our weaknesses – discovering holes in our defenses…and providing those who would do us harm an increased advantage to steal the liberty and lives of our citizens and allies. Whether intentional or not, when someone fails to safeguard critical information or protect our computer networks from the ever-present threat, the impact can be felt for decades. It's your duty to protect the information you have access to. And if you believe someone else is placing that information – or themselves in danger – it's your job to say something. It only takes one person to betray a nation… or to save it.

Lesson 1.2: Objectives

At the conclusion of this training, you will be able to:

Define Operations Security (OPSEC) and describe the methodology. Identify types of threats. Identify targeting methods used by foreign intelligence services and characteristics that make you a target. Define Social Networking Sites (SNS) and identify risks associated with using them. Identify countermeasures for safer use of SNS.

As you look over the course objectives, remember that protecting sensitive information is a details game and there are two main pieces to this puzzle: our sensitive information… and you. This course focuses on your responsibility to protect CLASSIFIED and UNCLASSIFIED information.

OBJECTIVES

At the conclusion of this training, you will be able to:

Define espionage and identify key indicators. Describe the lifetime obligations associated with protecting sensitive information. Define unauthorized disclosures and describe the impact to national security. Identify employee responsibilities, accountability, and reporting requirements. Recognize consequences/penalties associated with not reporting.

Module 2: OPSEC

Lesson 2.0: OPSEC

In this module, we'll take a look at how the OPSEC methodology helps protect critical information. The movie you're about to watch will tell a tale of OPSEC gone wrong. Small mistakes that lead to catastrophe. At the end of the module, you'll see how the mission would have been successful – and lives could've been saved – if the simplest of OPSEC methods were employed.

Lesson 2.1: A Tale of OPSEC

Narrator: Shhh…quiet now…don't let the enemy hear you. We've got some good intel… there is a high value target inside. He's one of the bad ones—plotting attacks on our country, and doing violence in his. He's not gettin' away this time. Our boys will be here any minute…some of 'em probably already are. Troop 1 on Radio: He's not here! Troop 2 on Radio: They knew we were coming… Troop 1 on Radio, shouting: Get out, get out, get out, IED! Narrator: Back in Washington, folks are scrambling to find out what went wrong. You see, the infrastructure that makes the American military the most effective fighting force the world has ever known…is complex. It's interconnected, and many people have a part in making it work...and this time, some of those people talked. Oh, maybe they didn't mean to, maybe they thought the information they shared was small. Maybe it was small. It probably wasn't even CLASSIFIED. Overheard guy on phone: "Hello, Sue? You won't believe this new technology…it's incredible!" Narrator: But it was a piece of the puzzle. Someone let their guard down. The enemy was listening. And the bad guys were prepared. And now? Well, the terrorists got a PR victory. Remember that bad actor I told you about? He got out of dodge of course. But he made sure some innocent civilians were there in his place. Plays better on the news that way. And some of our Allies are questioning our intelligence sources and methods. But worst of all, some of our men and women—well, they didn't make it home. The tragedy is—this—all of this—could have been prevented. OPSEC practices exist for a reason. Use them.

Lesson 2.2: OPSEC Definition

OPSEC DEFINITION

Operations Security

Operations Security – or OPSEC – is a risk management methodology used to deny an adversary information concerning our intentions and capabilities by identifying, controlling, and protecting critical information associated with the planning and execution of a mission.

So, when we hear that OPSEC practices could have made a difference in this tragic tale – what's really being said? Well, the "clinical definition" is that OPSEC is a methodology for identifying, controlling, and protecting generally UNCLASSIFIED information. This information is critical – and can be incredibly damaging if it becomes known to an adversary and can be used against you or your organization. So OPSEC is wrongly understood when we view it as a checklist or a tool in our security toolbox. OPSEC covers everything – and all the time. In a sense it's about looking at everyday habits and procedures in a different way, being vigilant and constantly monitoring the world around you. Seeing things how an

adversary sees them may be a bit uncomfortable – but it's going to help you… and probably surprise you… to see just how much information you give away for free. What's your daily routine and what can a bad guy learn from it? Are you "predictable," and if so – does that make you vulnerable? What kind of information do you put on the Internet; if that info's not blatantly damaging, what kind of information can it lead me to – or "who" can it lead me to, that just might lead me back to your critical information? If you haven't done the mental math on this before… prepare to be shocked. We give away a lot.

Lesson 2.3: OPSEC Process

OPSEC PROCESS

OPSEC is a process for examining day-to-day activities from an adversary's point of view. The process can be adapted to any organization, program, event, or activity. While some OPSEC steps may naturally come before others, they are all related.

An "OPSEC outlook on life" – and a firm grasp of the OSPEC process – will help you examine your day-to-day activities from the adversary's point of view and can cover your organization, program, event, or activity. Most importantly, OPSEC is a cycle where even after vulnerabilities are assessed and countermeasures are implemented, evaluation can, and really has to, continue. It's like asking "when do you stop setting your home's alarm system?" – that answer would be "never…" right? Right. Now bear this in mind… OPSEC isn't a linear exercise – even if logic might seem to dictate that certain steps precede others… they interact with and share dependencies with one another. Understanding this might necessitate revisiting previous steps in the process from time-to-time to reach a comprehensive plan of action.

Section 2.3.0: Identify Critical Information

OPSEC PROCESS

Is this something that could help the bad guys? If the information was combined with other information, would it create vulnerability? Would the information assist the enemy in finding weaknesses?

There are only so many hours in a day, so many resources to put towards protecting our assets, and so many ways to protect what we've got. So you need to identify what's "worthy" of your efforts. If you're not careful – you can spend all of your resources protecting things that aren't all that important while other things of greater value are neglected. It would be like the world's most sophisticated alarm system guarding costume jewelry, while the Hope Diamond has a "Please do not touch" sign on it. Silly, right? But we get distracted, and end up "majoring on the minors." Start by identifying your critical information. How could "this thing" help a bad guy and what weaknesses does it expose? Foundational to the OPSEC process is determining what information, if found in the hands of an adversary, would bring harm to an individual or their organization's ability to effectively carry out their mission. This is the kind of data that constitutes "critical information" – information that's central to the organization's mission or specific activities. Critical information is almost always UNCLASSIFIED, but if compiled, could quickly become incredibly SENSITIVE, or even CLASSIFIED.

Section 2.3.1: Analyze Threats

OPSEC PROCESS

Who might want your sensitive information or critical technology? What are their objectives? How could they get the information they seek?

After identifying critical information, you need to know the threat. Who wants what you've got and what are they willing to do to get it? Understanding why an adversary would want "this particular information" in the first place will help you to not only protect it – but build walls around similar information to protect it too. Knowing who your adversaries are and what objectives they have will also prove essential in determining what—among the information you possess – should be considered critical. In any given situation, there is likely to be more than one adversary who wants what you possess, and each might be interested in different types of information. So, an adversary's intentions toward your operations, coupled with their ability to collect, process, analyze, and use your information, has to be determined to truly analyze a threat.

Section 2.3.2: Analyze Vulnerabilities

OPSEC PROCESS

Are you aware of your weaknesses? How do you store, share, or destroy information? Are there indicators that could tip an adversary off – habits, methods, behaviors? Are all protective measures being implemented properly? Do you safeguard your information?

OK – the proverbial "chink in the armor" – you know… "you're only as strong as your weakest link…" This is never as true as when we're analyzing our vulnerabilities. It's one thing to be self-aware, and know what they are; it's another to actually do something about them. If you've discovered them, the adversary can as well. What do you do that would allow someone to collect and exploit your critical information? At times organizations release information through the web or in publication form that wasn't reviewed with OPSEC in mind. Other vulnerabilities occur as a result of "the way we do business." The adversary is always watching, and waiting for indicators that act as a tripwire for their plans. Once again: think like the enemy and assess your organization from his perspective.

Section 2.3.3: Assess Risks

OPSEC PROCESS

Is the risk great enough to take action? How would the loss of information affect you, your family, or your organization? What is the cost of losing or revealing the information? Does the cost of losing or revealing the information justify the cost and effort of protecting it?

So we've talked about analyzing threats and vulnerabilities – let's chat a little bit about "Assessing Risk." Everything has some sort of risk – right? But ask yourself: how "big" is the risk, how could it affect you or the people around you, and is it worth doing something to protect against it? This goes back to planning: how many resources do you put on any particular initiative. You wouldn't use all your bricks to fortify three walls, only to leave one side of your fortress completely exposed… and you can't do that with OPSEC planning and risk mitigation either. Vulnerabilities matched to specific threats help us to gauge the probability of losing information. When we add to our estimate the costs of an adversary to gather our information – measured in time, resources, casualties, or dollars – assessing risk demands a "so what?" answer, which becomes the basis for your forward-moving actions. Where the risk is great, a high priority for protection needs to be established and corrective action must be taken. Where the risk is low, we might simply choose to live with the potential risk in light of minimal consequences.

Section 2.3.4: Apply Countermeasures

OPSEC PROCESS

Limit the sharing of data, online and off. Follow your organization's security policies. Vary routines to avoid becoming predictable. Report instances in which security has been or is in danger of being breached.

Finally, taking the necessary steps to secure your information and our computer networks – and making sure those around you do as well is where the rubber meets the road. Countermeasures need to be established that reduce risk and are practically feasible – this is an important one… don't build a plan that you or your organization can't execute. The Countermeasures need to be effective and fit within budgetary restraints. Countermeasures can be just about anything likely to work in a particular situation. As an example, simply changing up your routine might prevent an adversary from predicting your activity and leveraging your location or patterns. Also, keeping business talk in confined areas instead of the local coffee shop can be an assertive and effective step toward preventing an adversary from eavesdropping in public areas. Eavesdropping at coffee shops isn't limited to what you say; it can be prime hunting ground for adversaries seeking to gain access to our computer networks. Using unsecure Wi-Fi can expose your critical information and give the adversary the needed foot in the cyber-door. But the Countermeasure is simple – don't use unencrypted Wi-Fi, use strong, unique passwords, and don't allow unauthorized people access to your computer.

Lesson 2.4: A Tale of OPSEC Retold

So we said we'd revisit the woeful tale of the military exercise gone wrong from the beginning of this course – let's take a look…

(Dramatic music) (gunfire) Soldier on radio: Alpha Team you're cleared to move to check point. (Noise; gunfire) Soldier: There he is. Soldier: We've got him. Soldier: Good work.
Narrator: Things turned out different this time. The five-step OPSEC process was followed at every step along the way. People didn't share information they weren't supposed to. Our adversaries were denied access to critical information…and the mission objective was achieved. Achieving the mission is about more than just short-term goals or even taking out the bad guys. It's about protecting our Nation and the American way of life.

Module 3: The Threat

Lesson 3.0: The Threat

This module is all about recognizing different types of threats.

Lesson 3.1: Define CI Insider Threat

DEFINE CI INSIDER THREAT

in•sid•er:

Any person with authorized access to any U.S. Government resource to include personnel, facilities, information, equipment, networks, or systems.

in•sid•er threat:

The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the U.S. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities.

Anyone who belongs to an organization is considered an insider, really. But an insider in the Intelligence Community is more specifically defined. Here, an insider is any person with authorized access to any U.S. Government resource to include personnel, facilities, information, equipment, networks, or systems. The insider threat, then, is the threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities. Simply paying close attention to a person's behavior and trusting your intuition can help you identify an "insider threat."

Lesson 3.2: Face of the Foreign Adversary

FACE OF THE FOREIGN ADVERSARY

Foreign adversaries may pose as many different types of individuals. Each of these individuals may work with someone inside a target organization to meet their goals.

Foreign agents, international terrorist organizations, and foreign intelligence services have two agendas. While an individual's job function may be legitimate for a foreign national, it's entirely possible that they may also be a foreign intelligence officer or the member of a Foreign Intelligence Service (FIS). They all pose a direct intelligence threat to us, but they also pose an indirect danger: by playing the part of an engineer or a student, for example. They may try to befriend us to sway our thinking. Foreign adversaries come in all shapes and sizes. And they don't wear name-tags to help you identify them. Be aware of their common disguises.

Lesson 3.3: Define Threat Types

DEFINE THREAT TYPES

Insider Threat:

The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the U.S. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities.

Espionage:

Intentionally obtaining, delivering, transmitting, communicating or receiving national defense-related information not available to the general public that may be used to the advantage of a foreign power or contrary to the best interest of the United States.

Recent focus on the "insider threat" has been on the violent threat – specifically related to terrorism. However, the threat has existed for a long time. It is often more subtle but just as damaging. Crimes like espionage, subversion, sabotage, terrorism, sedition, and treason degrade our ability to complete our mission and protect our nation. Review the definitions of each of these crimes further.

Subversion:

Actively encouraging military or civilian personnel of the DoD to violate laws, disobey lawful orders or regulations, or disrupt military activities, with the willful intent to impair loyalty, morale, or discipline of U.S. military forces.

Sabotage:

An act with intent to injure, interfere with, or obstruct the U.S. national defense by willfully injuring or destroying any national defense or war material, premises or utilities, to include human and natural resources.

Terrorism:

The use of force or violence against a person or property for the purposes of intimidation, coercion, or ransom. Terrorists promote fear and the idea that the established government is powerless. They seek to gain publicity for their cause.

Sedition:

Knowingly or willfully advocating or teaching the duty or necessity of overthrowing the U.S. Government or any political subdivision therein by force or violence.

Treason:

Violation of the allegiance owed to one's sovereign or state; betrayal of one's country. Aiding or attempting to aid the enemy. Knowingly harboring, protecting or giving intelligence to, communicating or corresponding with the enemy.

Lesson 3.4: Learning Checkpoint - Identify Threats

LEARNING CHECKPOINT:

Identify the Threats

How well can you identify different types of threats? Listen to the stories below to learn more about why each person poses a threat.

Section 3.4.0: Karen Stone

Identify the Threats. Karen likes her job with the Agency, but she's quick to say that it's not what she lives for. Last year she found a social group called the Young Avengers. They're radical political activists with groups in America and across the globe. The Avengers ideology seems to have negatively influenced Karen's opinion of our government to the point that she now questions her support for U.S. policies. This weekend, some of the group's members are getting together to take a vocal, public stand against the government. One of the leaders of the group has even gone as far as to say that the members of the Avengers should be prepared to meet force with force. Karen has decided to stand with her new friends – regardless of what happens.

Karen Stone. Karen has joined a radical international group with a mission that runs counter to the principles of the U.S. Government. She's attending an event that the group's leader has suggested will turn violent; she's prepared to participate anyway. Can you define the threat?

Section 3.4.1: Hector Famosa

Identify the Threats. Hector moved to the United States with his family when he was a child. After high school, he enlisted in the Army to help pay for college. He was deployed to Iraq, but returned six months later after being injured by an IED. Hector was assigned a desk job at Headquarters. Part of his job includes monitoring potential foreign threats originating from a number of countries. In the course of his work, he's developed sympathy for a revolutionary faction in his home country. Intelligence the U.S. has collected on the ruling government would be very useful to them in their fight, and so, Hector is reaching out to contacts within the faction, emailing them information about CLASSIFIED satellite imagery and intercepted military cables he believes could help them overthrow the current regime.

Hector Famosa. Hector works at NSA headquarters and is privy to CLASSIFIED intelligence about his home country. Because he was born there, he feels a close tie to its people's struggles. As a result, he's decided to share the CLASSIFIED information he has access to with a rebel force that's fighting to overthrow the current regime. Can you define the threat?

Module 4: Methods of Ops

Lesson 4.0: Methods of Ops

In this module, we'll take a look at a variety of methods foreign adversaries use to target DoD personnel. Knowing how these methods are used should help you in standing against them, should you be approached or have your information exposed.

Lesson 4.1: Laying the Snare

LAYING THE SNARE

All it takes is a moment of weakness to ruin your reputation and unravel your organization's security.

Meet Erica Rock

Erica Rock is a language analyst and just learned that she'll be going TDY to Belgium next week. Excited, she can't help but tell her friends about it.

Putting Herself Out There

Having never been to Belgium, Erica tries to learn as much as she can about her destination. What to see… what to eat… where to have fun. She reads and comments on a few blogs, visits sites to learn more, and asks questions of people she meets on those sites who live in Belgium and the surrounding areas. Erica even shares information about her occupation and asks for recommendations on regions that will expose her to the Dutch, French, and German speaking areas of the country to feed her love of language and help her in her job.

Meet Dylan

Dylan is a citizen of Belgium and joins the online conversation, telling Erica about the top tourist sites in his country – and those off the beaten path. Dylan also volunteers to show Erica around when she gets to Flanders, his hometown.

They Meet

Erica has a wonderful time with Dylan. He tells her that he works for a non-profit in Brussels dedicated to spreading democracy. He's smart and attractive. They agree to see each other again. And again. Eventually their relationship becomes close and continuing.

All's Fair in Love & Elicitation

Dylan starts asking Erica about her job. While Erica is hesitant, she's not sure how she can keep information from Dylan, whom she is becoming closer to with every conversation. She tells herself, that he loves her, and his country is an ally – so what can it hurt? After all, we are all working to spread democracy.

The Trap is Set

Dylan and Erica begin making plans for a romantic evening out. Dylan quickly took over the coordinating, and tells Erica to meet him at a remote lodge near the coast. When Erica arrives, however, she's shocked. Instead of Dylan, it's two strangers, waiting for her. They have photos, video and audio of her with Dylan, sharing sensitive government information. Turns out that Dylan wasn't who he pretended to be… and isn't even a Belgian national.

Quid Pro Quo

The men and Dylan are from a foreign intelligence service. They tell Erica that if she doesn't cooperate with them they'll send an anonymous package to the U.S. Government exposing her actions. All they want, they assure her, is a bit of "harmless information." Erica puts her face in her hands. She's trapped… and she knows it.

What Now?

As hard as it is, Erica has to report the incident. While she's gotten herself into trouble, there's no way out but to contact U.S. security personnel for help, immediately.

Lesson 4.2: Methods and Techniques

METHODS AND TECHNIQUES

A foreign agent can employ a variety of methods and techniques to access potential recruits.

An adversary's job becomes much easier if they can find a partner in crime – especially if that partner is a trusted insider. There are a variety of methods and techniques that a bad guy can employ to gain access to a potential recruit. Sometimes they're subtle, other times – overt – and whether they're executed in-person, electronically, or by other means… these strategies have proven themselves effective.

Recruitment:

Exploit personal weakness, preferences or circumstances (such as shared ideology, addiction or financial problems) to lure victims into cooperating. Often involves praise or rewards.

Elicitation:

The subtle collection of pieces of information through face-to-face interaction or over the Internet. Over time, the information provides a complete picture. The goals of elicitation are to GET you talking and to KEEP you talking.

False Flag:

An agent can misrepresent him/herself as a citizen of a friendly country, nation, or organization in order to lessen suspicion and foster trust. This is referred to as the false flag approach.

Job Seeking:

Job seekers often learn a great deal about a potential employer. Seeking employment with a targeted organization can provide an adversary direct or indirect access to sensitive information and installations, providing first-hand access to targets or targeted information.

Leveraging Official Channels:

Foreign liaison officers, foreign exchange officers, or other high-ranking foreign nationals can gain access to important information on official visits. An adversary may use an official visit to an embassy, installation, or a base to gain access to a location, and, by default, information such as the names and titles of personnel and facility layouts.

Brute Force:

An adversary may use intimidation or coercion of individuals or third party nationals who have access to data, facilities, or personnel to gain access to critical information. Coercion is also used when a target has relatives that live in a hostile foreign country.

Online Research:

Gaining access to data through web and social networking sites provides a very low-level, low-risk way for an adversary to gain knowledge of personal interests, employment information, and proximity. This data can be used to manipulate individuals into service.

Old Fashioned Profiling & Observation:

As simple as it seems, an adversary can learn a lot about a potential target or organization by standing back and observing behaviors and habits. In doing so, a foe can identify where a target's personal interests lie, then disarm them by inserting themselves into a seemingly "safe" environment, like fitness classes, church congregations, or as fixtures in the local hang out.

Blog Watching:

Just like online research, scrubbing blogs for valuable personal information and leaks related to mission-related tasking have become a low-risk, easy way to gain valuable information.

Phishing & Online Scams:

An adversary may try to identify and recruit a target by soliciting information through deceiving emails. This technique may be another way to check for gullibility and test willingness. Intercepting the transfer of valuable information through commonly used email channels is another rather easy way to gain information.

Lesson 4.3: What Makes You a Target?

WHAT MAKES YOU A TARGET?

Vulnerabilities can include a variety of things such as:

Location Assignment Access Financial Problems Disgruntled Indebted

Substance Abuse Loneliness Ideology Adventure Seeking Ego Personal Problems

Once an adversary has targeted you, they will devise a strategy to entice you into service for them. They look for details about you… ways to gain your trust and befriend you… or vulnerabilities that they can use to exploit you. While your personal traits will not automatically make you a target, they can make you more interesting to an adversary.

Lesson 4.4: Protecting Information

PROTECTING INFORMATION

Important guidelines for protecting sensitive information:

Make sure your computer networks are protected from intrusions. Make sure your organization has clear and concise policies in place. Ensure your privacy settings are enabled and optimized when online. Consider the information you have and who could have access to it. Limit your communications to the most essential details only.

Whether it's physical or virtual security we're talking about, there are a number of ways to protect your information. Take a few minutes to review these important guidelines.

Important guidelines for protecting sensitive information:

Be aware of your surroundings. Know whom you're talking to, and who might be listening. Only share information on a need-to-know basis. Monitor the proper storage and disposal of physical information and data. Avoid routines and other behaviors that make you predictable to the adversary.

Module 5: Social Networking

Lesson 5.0: Social Networking

In this module, we'll focus on understanding Social Networking Sites, the risks associated with using them, and how to apply countermeasures for safer use.

Lesson 5.1: SNS Defined

DEFINED

Social Networking Sites (SNS):

Sites designed to allow for the easy exchange of information, both privately and publicly, with friends and strangers alike.

These sites are devoted to connecting users with similar interests, backgrounds, and experiences. Users generally have searchable profiles containing information about themselves, indexed for search by others looking to connect with them. Social networking sites are designed to allow for the easy exchange of information, both privately and publicly, with friends and strangers alike. Popular social networking sites include Facebook, Twitter, LinkedIn, FourSquare, Pinterest, and Flickr.

Lesson 5.2: Cyber Threat

CYBER THREAT

What are the risks associated with the social web?

Posting personal information or uploading photos to the Internet is becoming more and more common, and it's easy to make mistakes. Publishing photos while at certain locations can be incredibly detrimental to mission safety and success. You might not expose CLASSIFIED information, but an adversary who's able to put little details together can glean huge amounts of information.

Viruses, Malware, Spyware

They not only foul up system performance, they can trick your network into giving up its biggest secrets.

Malicious Links

The delivery method of choice for many hackers looking to introduce viruses or malware into your network.

Phishing and Online Scams

No hacking. Just good old-fashioned deception to steal your passwords, PINs, and other sensitive information.

Electronic Elicitation

Getting you to willingly give up information without you even realizing it.

Online Dating

A match made in heaven can quickly become a nightmare when you realize the person on the other end isn't who they say they are.

Virtual Gaming

The perfect place to subtly troll for information or observe real-world military strategies in action.

Lesson 5.3: Adding Up the Threat

ADDING UP THE THREAT

The math of aggregating critical information is deadly.

Having sensitive – or just embarrassing – information fall into the hands of the adversary can do some serious damage to your family, your career, and your organization. Remember that small pieces of data add up to give people – especially the wrong people – a more complete picture of you. And, this can make you vulnerable. While data mining isn't directly tied to national security, it should get you thinking about your personal data and what it's being used for. Don't forget that online information is immortal and never goes away!

Lesson 5.4: SNS Countermeasures

SNS COUNTERMEASURES

Protect your critical information.

In order to better protect your critical information, think about how to apply the OPSEC thought process to your online activities.

Remember Computer Security

Know the tools that you are using and set them up to be secure. Don't share passwords, or give out your passwords. Don't log into one site using credentials from another or use the same passwords across all of your accounts. Add your friends manually instead of letting a site into your address book.

Computer security. Know the tools. Know what files do. An adversary or attacker will usually try to attack the computer first. So use best practices; things that apply to email security apply when using SNS too…don't download executable files or install applications from unknown sources. And don't share your passwords with anyone – no matter how nicely they ask.

Before posting personal information or other data to the web or an SNS, research who owns the site/company that published the site; who are their partners; where is the site hosted; and, who has access to the data?

Consider All the Players

Before you go anywhere online, use caution. You never know who owns the site, where it's hosted, and who can get at their data.

Modify Your Search Profile

Even if you lock down your profile, you may still be visible to searches. Try searching your own name while logged out or from a friend's profile. Carefully scan all settings and controls to find those often-overlooked options.

Those online profiles of yours? Time to take the scissors to them and do some heavy cutting. Take out any info that could share too much about you and your family.

Remain Reasonably Suspicious

Con artists or potential foes often start to connect with a target by social engineering—becoming your friend to gain your trust, or using some other similarity to "get in." Maintain a healthy suspicion when

strangers “click” with you too quickly—they like what you like, hate what you hate and understand you like no other. Be cautious on dating sites. Adversaries can get data about you before they “meet” you— from yearbooks, your posts/profile and other Internet sources. Verify that you are friends before you accept a request. Verify that folks are who they say they are… Do not trust add-ons, such as games or services that share information (i.e. what you are reading, who your cousins are, etc.).

Don’t assume people you meet online are who they say they are. Even if they seem to be friends. Same goes for software, apps, and files too.

Watch Your Friends

Be sensitive to what your friends post about you—photos, locations, etc., and educate them on Internet safety. Be adamant about them protecting your data.

Also, make sure your friends don’t get you into trouble. Put them on notice to keep you out of their online conversations and photos.

Treat Links and Files Carefully

Verify links and attachments before clicking or downloading. Malware and damaging files can be distributed via SNS just as in email.

Treat links and files like the bomb squad treats a strange package. Maybe they’re OK. But maybe they’re not. Approach carefully.

Question the Utility of an SNS

If you feel that SNS are helpful to you and pose a benefit, do your homework. Understand how to protect yourself and your information and employ best practices and safety measures. If they are worth using, then they are worth understanding. Note that security is not inherent to all tools.

It seems like everyone’s on some social network these days. But ask yourself, is it really worth the risk? Do I really NEED to be on here? If the answer’s no, then reconsider it.

Think Twice Before Using Apps That Share Your Location

Sharing your location over the Internet can reveal more than just where you are and where you’ve been. It can provide insight into your habits and patterns, leaving you vulnerable. Be careful how much you share, and how often. Tweets, photos, check-ins, and status updates from your friends can reveal information about your whereabouts, too. Ask friends and family to use discretion when including you in updates on their networks. Photos taken with mobile devices and some digital cameras share the location of where they were taken (geo-tagging).

Anytime you share your location, you’re opening yourself up to a world of potential headaches. And before trying a new online, social, or mobile utility know whether or not it defaults to broadcast your position. When you share photos that contain GPS coordinates online, an adversary can easily extract location information from the photos. Taking a picture at home, work, or while deployed can lead them right to you.

Be Careful of the Information, Photos and Other Media You Post

Watch backgrounds and reflective surfaces. Be careful of what images will reveal about your personal life, locations and others in those photos. Once it’s out there, you can’t get it back. Be cautious about details that

you discuss. Avoid talking about work or details about work. Avoid the same for spouses, significant others and family members. Do not post information that the public should not know.

Use a little common sense when posting. Every update or photo may unintentionally give up details you don't want people to know.

Pay Attention to Browser Alerts, Prompts, and Information

While most browsers will automatically prompt users when an update is available, it's a good idea to perform a manual check for updates on a regular basis. Look for secure logins (i.e., https) when logging on to any site and make sure it's enabled the entire time – from login to logout. Do not let sites remember you, and do not depend on SNS to provide appropriate security. Login to all your mail and social sites with one browser (i.e. Internet Explorer) and surf the Internet with a different one (i.e. Firefox). If you don't use multiple browsers, log into your accounts one at a time before browsing or you may fall victim to what's called a Cross Site Scripting Attack.

Be smart with your browser. Keep it updated, listen to it when it throws up red flags, use secure logins, and diversify. Use different browsers for different things.

Lesson 5.5: Learning Checkpoint - FaceSpace Page

LEARNING CHECKPOINT:

Identify Responsible Social Media Usage

The web's become one of the most popular ways to keep up with our friends and family. Nothing wrong with that, but as an NSA affiliate, you must be more aware of what you're doing, who might be watching, and how it can affect you, your family, and national defense. For starters, never accept friend or follow requests from people you don't know. Assume anything you post online can be seen by anyone. Also be aware that adversaries can use seemingly innocuous information about you to gain your trust or gain access to your online accounts. Take a moment to review Joe Talker's Facespace page. Decide whether each item Joe posted is Secure or Unsecure.

Section 5.5.0: A: Travel Plans

Name: Joe Talker

Current status: "My fortune says I will be TDY in Beijing from the 11th-21st."

Refrain from detailing your travel plans before you leave. This can make your home and/or family a target. Also, using government specific terms, such as TDY, identifies you as a government employee – a potential asset to a foreign adversary. In this case, traveling to China identifies your interest in China and could make you a target while traveling there.

Section 5.5.1: B: Locations

Updates shared on Facespace: "About to leave work. Hope the B/W Parkway isn't too backed up."

Detailing your immediate location, or the fact that you are not home, makes you vulnerable. Also, the fact that you work off of the B/W Parkway put together with other information could identify you as a NSA affiliate.

Section 5.5.2: C: Kids

"So proud of my daughter. Her recital tonight was beautiful – not sure where she got her gift of music, but it wasn't from me." [photo shows daughter tagged]

Everyone wants to brag about their kids. But if someone is able to gain access to your posts, do you want them to know who your children are, what they look like, and what their interests are?

Section 5.5.3: D: Polygraph

"Polygraph, passed. Glad I don't have to get hooked to one of those things for another five years."

You might as well just post that you work in the U.S. Intelligence Community and have a TOP SECRET clearance.

Section 5.5.4: E: Hobbies

"Chesapeake Bay Car Show this weekend. Can't wait for retirement, so I can spend my days restoring the '66 'Cuda I bought a few years ago."

Sharing your hobbies is part of what makes social media fun, but just be aware that adversaries can use the information to elicit trust. For instance, someone might send a friend request and say, 'Hey, I hear you have a '66 Cuda. I am working on restoring one now. Would love to talk about where you get your parts.' Who's to say who that account really belongs to?

Section 5.5.5: F: Alma Mater

"'Terps made it to the Final Four! Gotta love my alma mater!"

Social media is a wonderful way to connect with old classmates – kind of an ongoing, virtual reunion. Again, be aware that the more information you share gives an adversary that much more information to make a connection.

Section 5.5.6: G: Travel Plans 2

"Back from vacation. I miss you already, Hawaii."

Posting your travel activities after they happen is much preferred to posting them before or during. This allows you to share your experience without making you vulnerable.

Section 5.5.7: H: Birthday

Information Section

Birthday: 4/14/1967

Including your month and day is fine – after all, don't we all love the numerous wall posts on our birthday, but omit the year. Besides, birthdates are often used to verify identity; best to keep the year offline.

Section 5.5.8: I: Relationship Status

Information Section
Married to: Ruth Talker

Well, I think you better claim your spouse on any social media sites, but, again, be aware that linking someone to you can make them more of a target if you become a target for an adversary.

Section 5.5.9: J: Alma Mater 2

Information Section
Studied at: University of Maryland; University of Chicago

You went to college and studied hard for that piece of paper, so go ahead and let folks know where your March Madness loyalties lie, but if someone tries to connect with you from your alma mater and you don't remember them, or you don't really like them, don't be afraid to 'ignore' it.

Section 5.5.10: K: Home Address

Information Section
Home Address: 212 My House Ct, Springfield, MD

There is no good reason to put your home address online.

Section 5.5.11: L: Job Title

Information Section
Job Title: East Asia Analyst

Do not put your job title online.

Section 5.5.12: N: Likes

Information Section
Likes: Muscle cars, family, anything University of Maryland, Redskins, playing basketball, Ocean City, our freedom, sushi, Dr. Pepper, and classic rock (especially the Eagles)

Again, don't know how often I need to stress this, but sharing online can make you vulnerable. It can be fine, but be aware. Those extra security questions sites often use to verify your identity, like: 'What is your favorite band? What is your favorite sports team? In what city were you born?' - adversaries can use information you post online to guess the answers. Next thing you know, they're sending emails brimming with malware from your account or purchasing 15 iPads with your credit card.

Section 5.5.13: O: Movies

Apps Section
NetMovies - *The Fast and the Furious; Battlefield Earth; The Thin Red Line; 27 Dresses; This is Spinal Tap; Enemy of the State*

So, you're the other person that watched Battlefield Earth. Seriously, though, if you think your friends want to know what you are watching, share away but use good sense.

Section 5.5.14: P: Apps

Apps Section
Places – Displays a map with points around Ft. Meade visited.

Sharing your actual location is a serious operations security violation. Be aware of location-services, such as Facebook Places, Foursquare, etc. Also, know that photos taken with phones, PDAs, and many cameras contain GPS coordinates that can easily be viewed with free software or are used to share locations – often without you knowing. So, next time you break out your camera at a work-related function, be careful of who might see the picture.

Running GPS – Shows his last jogging route on a map, including total distance run, duration, and avg. pace; and total distance and time logged on Running GPS.

Come on. You should at least make an adversary work for the information. Don't make it this easy.

Module 6: Espionage

Lesson 6.0: Espionage

In this module, we'll focus on how to identify key indicators of espionage.

Lesson 6.1: What is Espionage?

WHAT IS ESPIONAGE?

Espionage is a unique crime because it almost always requires a personal connection between an Insider Threat and a foreign adversary. It typically involves mutual benefit from a transactional relationship. According to Title 18 and Espionage Statutes, there are various penalties depending on the type of espionage: STATUTE 793 prohibits the gathering, transmitting or loss of defense information.

Penalty: 10 years in jail and/or fines

Espionage almost always requires a personal connection between an Insider Threat and a foreign adversary. It's simple… one has something that the other one needs – money, information, access… And just like we've seen… those partnerships can be devastating.

According to Title 18 and Espionage Statutes, there are various penalties depending on the type of espionage: STATUTE 794 prohibits the gathering, transmitting, or delivery of defense information to representatives of a foreign government.

Penalty: Lifetime in jail during peacetime, or the death penalty during time of war

According to Title 18 and Espionage Statutes, there are various penalties depending on the type of espionage: STATUTE 798 prohibits unauthorized disclosure of a cipher, code, cryptographic system or communications intelligence activities of the United States to any foreign government. This includes inadvertently or mistakenly divulging information to someone who should not have access to it.

Penalty: 10 years in jail and/or fines

Lesson 6.2: Espionage Motivators

ESPIONAGE MOTIVATORS

So what drives people to commit espionage? Analysis on many of today's cases reveals that ideology or a person's personal beliefs play a big role. Let's take a look at some of the common reasons.

Ideology:

When a person's personal, philosophical or religious beliefs conflict with their duties, they could be more likely to make a decision that could hurt national security or the safety of their colleagues.

Ana Montes

Ana Montes is a former DIA senior analyst, charged with spying for the Cubans. In 1984, Montes held a clerical job at the Department of Justice in Washington, during which time she often spoke openly against the U.S. Government's policies toward Central America. Cuban officials played to her political motives and recruited her to spy for them. In order to assist Cuba, she actively sought positions in the U.S. intelligence community, and, in 1985, she was hired by DIA, where she worked at the Cuba desk, helping shape U.S. policy towards Cuba. Once arrested, Montes acknowledged revealing the identities of four American undercover intelligence officers working in Cuba.

Revenge:

Those with a bone to pick could use their access to CLASSIFIED information as an opportunity to do it.

Earl Pitts

Earl Pitts, a former Supervisory Special Agent with the FBI, became embittered toward the FBI due to his perceived poor treatment as an employee. Seeking revenge, in 1987 he decided to spy for the Soviets to "pay them [FBI] back" and to dig himself out of a financial hole. He contacted the KGB and spied for them until 1992, receiving over $224,000. Pitts revealed personal medical, family, and CLASSIFIED information about fellow FBI agents and suggested strategies on how to use that information to convert them to double agents. He also released the FBI's comprehensive listing of every Soviet official in the U.S. and their connection to the intelligence community. When the KGB handler later defected to the U.S., he identified Pitts to the FBI, prompting an undercover operation wherein Pitts began spying again for what he believed were Russian agents. He was sentenced to 27 years in prison. At his sentencing he said, "What I did was wrong, pure and simple."

Ego:

Certain people believe they're above being caught and participate in illegal activities for the sheer thrill or personal validation.

Robert Hanssen

Robert Hanssen was charged with selling U.S. secrets to the Soviets and, subsequently, the Russians. A veteran FBI counterintelligence official, he used his training, expertise, and experience to avoid detection for over 20 years. Hanssen was motivated by ego and greed – receiving an estimated $1.4 million in cash and diamonds for his information, and his betrayal led, in part, to the death of at least two double-agents for the U.S. Hanssen is considered one of the most damaging spies in U.S. history.

Financial:

Dire financial straits can make some people desperate and willing to do anything to improve their fortunes.

Brian Patrick Regan

Brian Patrick Regan, a former Master Sergeant in the United States Air Force, was charged with two counts of attempted espionage and one count of gathering national defense information. Regan was strapped with a whopping $117,000 in credit card debt and began to collect CLASSIFIED information from NRO -- the National Reconnaissance Office – ultimately removing an 8 foot tall stack of TOP SECRET documents (15,000 pages), in addition to CD-ROMs and videotapes. He then offered to sell the materials to Saddam Hussein for $13 million and made similar offers to Libya and China. Regan was arrested on August 23, 2001, at Dulles Airport before boarding a flight to Germany – and before selling the information. His actions could have cost many soldiers their lives, but, thankfully, he was apprehended and arrested before any information was released. Brian Regan was tried and convicted in 2003. While prosecutors sought the death penalty, he was ultimately sentenced to life imprisonment without the possibility of parole.

Romance:

A fresh love can cause feelings of euphoria and excitement, making it difficult to make logical decisions.

Sharon Scranage

Sharon Scranage worked as a secretary for the CIA in Accra, Ghana and became romantically involved with Michael Soussdoudis, an agent for the Ghanaian Intelligence Service and a cousin of the then-Ghanaian head of state, Jerry Rawlings. Soussdoudis used the relationship to recruit her to spy for Ghana. She provided the identity of CIA officers and agents and compromised intelligence on communications, radio, and military equipment.

Coercion:

While seldom a motive to initiate espionage, subtle pressure from handlers and fear of detection if they stop, have been powerful sustainers of continued espionage activity.

Ronald Pelton

Once involved in espionage, many offenders have reported a coercive effect generated by their own fears that there is "no way out". A good example is Ronald Pelton, a former communications specialist with the National Security Agency for 14 years, who admitted to offering his services to the Soviets in 1980, within

one year after his resignation from NSA. Initially motivated by financial need, he continued contact for more than five years, until he was arrested, out of "fear of what they could do." During that time he attempted to break contact by failing to complete scheduled communications. He even went so far as to change residences and phone numbers twice. On each occasion they re-contacted him at his new residences on his unlisted phone numbers and requested meetings. While they never made overt threats, the fact that they could always find him generated such fear that he always complied with the request. This same coercive effect has also been reported by other convicted spies, including David Barnett and Earl Pitts. They attributed their fears to the relentless pursuit of Soviet handlers when they tried to end involvement or missed scheduled meetings. In the end, Pelton was arrested in Nov 1985 and reported receiving approximately $35,000 for his cooperation. Pelton was sentenced to three life terms plus 10 years to run concurrently.

Lesson 6.3: Indicators of Espionage

INDICATORS OF ESPIONAGE

There are a variety of leading indicators to espionage. Taking them into account while remaining observant to individual behaviors, you should be able to recognize and more importantly, report potential problems. Review each indicator in detail.

Frequent or Unexplained Travel

Unusual travel to foreign countries. Travel that seems inconsistent with person’s interests or financial means.

Unusual Work Behavior

Working unusual hours. Attempting to gain unauthorized access to CLASSIFIED areas or information. Copying or downloading of sensitive material.

Financial Matters

Unexplained affluence or paying off large debts. Lavish displays of wealth or free spending. Explanations of wealth absent of facts or support.

Disregard for Security Practices

Discussing CLASSIFIED information in public. Removing security markings from documents. Attempting to expand access to CLASSIFIED information. Bringing restricted items, such as removable storage devices, into CLASSIFIED spaces. Posting the wrong level of CLASSIFIED materials on the wrong network.

Foreign Influence or Connections

Unapproved contact with foreign government officials. Unreported foreign assets or business connections. Unreported monetary transactions with foreign nationals or governments.

Solicitation

Unexplained money or extravagant gifts. Attempts to coerce co-workers into illegal situations. Leveraging personal, trusted relationships to target co-workers.

Module 7: Reporting

Lesson 7.0: Reporting

This module reviews your reporting responsibilities.

Lesson 7.1: Lifetime Obligations

LIFETIME OBLIGATIONS

Safeguard protected information. Seek pre-publication review. Report unauthorized disclosures.

Protecting CLASSIFIED information is a lifetime obligation. Sure, you'll retire one day, but our adversaries never do. So as long as our nation has enemies, you have an obligation to protect its secrets. You are required to get approval to publish documents, resumes, white papers, articles, and the like through pre-publication review. This ensures that you don't inadvertently disclose information that could damage national security. This applies to any and every form of published communication…. print, on the web – and even TV. Remember – in this case, it's always better to ask for permission than forgiveness – the stakes are just too high. President Obama's 2009 Executive Order 13526 defined an unauthorized disclosure as "a communication or physical transfer of CLASSIFIED information to an unauthorized recipient." To be considered an authorized recipient, an individual must obtain eligibility for access, sign a Non-disclosure Agreement, and possess a "need to know" for that specific information. Anyone who doesn't meet these three criteria is considered an unauthorized recipient. If you or a colleague commit or identify an instance in which information of any kind was provided to an unauthorized recipient … you've got to report it – right away. This is not about punishing inadvertent disclosure. This is about giving your organization the ability to avoid the potential consequences that could occur as a result.

Lesson 7.2: Unauthorized Disclosures: Damage

UNAUTHORIZED DISCLOSURES: THE DAMAGE

An unauthorized disclosure can have a wide range of negative consequences, each more serious – and potentially deadly – than the next.

Damage to Sources and Methods:

Adversaries gain insight into how the U.S. gathers information.

When CLASSIFIED information ends up in the hands of unauthorized recipients, it can cause damage to our sources and methods by giving adversaries insight into the ways the U.S. collects information. The adversary can then use this knowledge to thwart our collection efforts or, perhaps worse, take advantage of them by attempting to hide their true capabilities or intention from the U.S.

Distorting Public Perception:

The public may get an incomplete picture, leading to misperceptions.

In almost every case of unauthorized disclosure, the public only sees some of the information. As a result, it can lead people to draw incorrect conclusions. In fact, because the information is incomplete, the public

may actually become less informed about how the government acts on their behalf. Unfortunately, it's a catch-22: to clarify the situation for the public would require disclosing additional CLASSIFIED information, which is highly unlikely – and even more dangerous.

Effect on International Alliances:

An atmosphere of distrust develops between allies.

Unauthorized disclosure can lead to distrust between the U.S. and its foreign allies. In addition, it can also damage relationships between the IC and allied intelligence services, ultimately leading to a reluctance to share important and potentially life-saving information with each other.

Financial Costs:

Hundreds of millions of dollars are lost.

Damage from an unauthorized disclosure extends beyond secrets. It can also mean a significant financial impact. According to the UNCLASSIFIED WMD Commission Report, unauthorized disclosures have cost the American public hundreds of millions of dollars.

Impact to Foreign Policy:

Leaders' ability to develop and carry out approved international policies is inhibited.

U.S. foreign policy is complex. An information leak can complicate it even further by directly – and very negatively – affecting officials' ability to shape and implement approved policies.

Potential Loss of Life:

Several deaths have occurred as a direct result of unauthorized disclosures.

Intelligence collected from human sources is especially vulnerable to damage from unauthorized disclosure. Tragically, information leaks through the media have been directly linked to the deaths of several people.

Lesson 7.3: Your Reporting Responsibilities

YOUR REPORTING RESPONSIBILITIES

You have a responsibility to report behavior that may lead to an unauthorized disclosure:

Report a suspected unauthorized disclosure immediately. The Associate Directorate for Security and Counterintelligence (ADS&CI) guidelines and your Security Officer can provide you with reporting information. Remain alert – especially online. You may be the only one who notices a harmful disclosure.

It's up to you to notify your agency if you suspect an unauthorized disclosure. Your agency provides guidelines for the proper reporting channels, and it's important that you become familiar with them. If you have additional questions, talk to your Security Officer. Next, stay alert – especially online. There are millions of blogs, journals and other media outlets – each a potential platform for a harmful disclosure. If you notice something's not right, don't assume others have noticed it, too. It's up to you to say something.

Remember: it's everyone's responsibility to report the actions of another employee whose behavior could lead to unauthorized disclosure, whether you have access to CLASSIFIED information or not.

Lesson 7.4: Reporting Foreign Contact/Travel

REPORTING FOREIGN CONTACT/TRAVEL

Before You Go:

Submit Unofficial Foreign Travel (UFT) request (Form K2579) 30 days before your leave date. Submit via:

NSANet – 'go uft' Fax: 301.688.2284 Mail: Director, NSA; ATTN: Q34; Suite 6321, 9800 Savage Rd.; Fort George G. Meade, MD 20755-6000

If you plan to go on vacation or conduct Unofficial Foreign Travel, otherwise known as UFT, or take UFT in conjunction with Official Foreign Travel, OFT, you must submit a UFT request 30 days prior to the date you expect to leave.

While You're There:

Report the following:

Reporting contacts with foreign nationals is a requirement you agreed to when you were indoctrinated. You must report close and continuing association with non-U.S. Citizens; any contact with an employee or representative of a foreign government, even a one-time meeting with a diplomat or attaché; visits to foreign embassies; sexual contact with a non-U.S. citizen, even if only one time; and any unusual or suspicious contacts or incidents with foreign nationals, either in person, by phone, or over the Internet.

Where to Report:

If you're a civilian, report to CI Awareness and OPSEC or appropriate SSO or PSO. If you're a contractor, report to your CSSO and contact CI Awareness and OPSEC or call Contractor Clearances at 410.854.6036. If you're a military assignee, report to Military commanders via service SSO with a copy to CI Awareness and OPSEC.

Lesson 7.5: Consequences of Not Reporting

CONSEQUENCES OF NOT REPORTING

Liability

You could have stopped a crime before it happened.

Culpability

You could be considered an accessory to the crime and receive administrative or legal action. Military affiliates can be prosecuted under the UCMJ.

Tragedy

You could be responsible for lost lives.

As part of your oath to protect our nation's sensitive information, it's also your responsibility to report whatever you've heard or seen. Besides any administrative or legal ramifications for not reporting, there can be even larger impacts. Information lost. Weaknesses exposed. And lives put at risk.

Lesson 7.6: Learning Checkpoint - Identify Reportable Indicators

LEARNING CHECKPOINT:

Identify Reportable Indicators

How well can you identify reportable indicators? Listen to the stories below to see if you can identify what to report.

Fred Walters.

Fred used to be very social and it wasn't uncommon for him to talk frequently with coworkers about work and non-work related subjects. Lately he's quiet and distant. When asked to join his colleagues for lunch, he declines telling them that he's trying to save money. Twice in recent weeks, his wife called to ask if he's at work on days that he has scheduled off. Colleagues ask him if everything's okay, but he's become very defensive. The other day a coworker spotted Fred off base with a very attractive Asian woman who was not his wife. The coworker also noticed that the car they got into had diplomatic plates.

Can you identify Fred's reportable indicators?

Fred's recent changes may indicate that he has something on his mind and his involvement with another woman may all be unusual, but they are most likely not reportable. Make an effort not to over think changes in behavior that do not indicate a violent threat. Fred's suspicious behavior coupled with the fact that he and his mysterious friend got into a car with diplomatic plates may indicate a problem. Suspicious activity and unexplained connections to foreign entities should be reported.

Ellen Chang

Ellen is an Intelligence Analyst. Over the past months, she's bragged about an expensive trip that she took to the Bahamas. She's also purchased expensive jewelry and a new BMW. When asked by friends how she could afford these things on a government salary, she said that her husband had recently made some good investment choices. But just a few months ago Ellen was complaining about a significant amount of debt that she and her husband had acquired.

Can you identify Ellen's reportable indicators?

The change in her financial situation is puzzling. Despite admitting she was significantly in debt, she is purchasing things that are beyond her means, and that's a red flag. While it may be that she did

have some good investment decisions, the situation appears reportable. Remember, an investigation does not mean someone's guilty.

Dave West

Dave's a COMINT analyst. Recently he's mentioned to a number of colleagues that his workload has increased, and while he's come in early and stayed late at the office, he's admitted that he sometimes falls behind in his tasks. One day, while in a rush to photocopy a report he'd been working on for an important presentation, Dave dropped a file box full of documents on the floor of the copy room. A coworker helped him pick up the materials, but noticed that Dave was less than meticulous in putting the files back together. Later that evening as Dave packed up to leave, the coworker noticed him place a pile of disheveled papers in his briefcase.

Can you identify Dave's reportable indicators?

While Dave may be trying to catch up, the extra hours he's working, compounded with his seemingly haphazard handling of security documents could indicate that something's not right. Dave may simply be stressed and absent-minded, but his behavior appears to be reportable. An inadvertent security breach is still a breach.

Module 8: Conclusion

Lesson 8.0: Conclusion

If you see something, know something, or even suspect something: report it.

Lesson 8.1: Call To Action

CALL TO ACTION

What Can You Do?

Follow NSA's protocols and procedures and practice good OPSEC. Exercise sound judgment. Report. Report. Report.

So now you have good perspective on how to recognize an insider threat and report suspicious activity. You have known that Good OPSEC helps you evaluate your information and its vulnerabilities (and the security of your organization) from the bad guys' point of view. Our adversaries don't wait to exploit huge gaps in our security… they use the combined weight of numerous small details or mistakes to break through our information defenses. If you're careless in your everyday activities – it'll spill over into your work. And it can become a red flag for anyone who's looking to exploit you, your family, your friends, or your mission. And remember – always be vigilant. You may be the only one standing in the way of the adversary and our nation's security. If you see something, know something, or even suspect something: report it. America's counting on you.

Lesson 8.2: Contact Information

CONTACT INFORMATION NSA/CSS ADS & CI

Avenues of Reporting:

Staff Security Officer, Contractor Special Security Officer, Military Staff Security Officer, Security Operations Command Center (SOCC) – 301-688-6911 US Embassy/US Consulate Local FBI Field Office

You can report an incident in a number of ways.

Avenues of Reporting:

Counterintelligence Awareness and OPSEC 9800 Savage Road OPS 1, 1S079, Suite 6321 Fort George G. Meade, MD 20755 301-688-6535 (b) / 301-688-2284 fax (b) / 963-3273 (s)

Lesson 8.3: Congratulations

You have completed the NSA's annual Counterintelligence, OPSEC, and Unauthorized Disclosure Refresher Course.

CONGRATULATIONS!