Course: OPSEC Awareness for Military Members, DoD Employees, and Contractors

[NARRATOR:] Welcome to the OPSEC Awareness for Military Members, DoD Employees, and Contractors course.

[NARRATOR:] Protecting critical and sensitive information is essential to protecting the success of your organization and your missions, and to protecting the lives of U.S. service members, DoD employees, contractors, and family members. Select the Course Objectives button to read the objectives.

Incident Report

[NARRATOR:] The date is June third. At oh nine thirty, Air Force Col. James B. Stamburg receives word of an event he hoped would never happen. Stamburg is ready to act. He immediately places a call using secure communications equipment.

[COL. STAMBURG:] This is Delta Tango One Five. Priority URGENT. We have an extremely serious incident. A convoy of trucks carrying a store of weapons and explosives is under assault. The identity of the attackers is unknown. The convoy was being escorted by armored military vehicles. Initial reports from the scene indicate two personnel KIA, two WIA, and three MIA. Implement response plan echo-sierra-two. I repeat, implement response plan echo-sierra-two. Stand by for more. Over.

[NARRATOR:] Col. Stamburg has very little information about the attack. He orders an Explosive Ordnance Disposal, or EOD, team to the scene. He alerts the joint incident emergency response force. The colonel believes he has just 45 minutes to find the attackers and capture them. If he fails, the weapons and explosives will probably fall into the hands of terrorists.

Only an Exercise

[NARRATOR:] Fortunately, this incident wasn't real. It was an exercise planned by the joint incident emergency response force to test its plans for handling a real terrorist attack. No one was hurt. The convoy of trucks was carrying simulated weapons and explosive materials - not the real thing. The attack was staged. The joint incident emergency response force responded exactly according to plan. Col. Stamburg's EOD team recovered the simulated military weapons and explosive materials. In reality, the terrorists were military personnel playing a role. The joint incident emergency response force and federal law enforcement officers captured them as they boarded a helicopter in San Francisco to escape to a waiting ship. The whole exercise went quite well, except for one very big problem. The exercise was supposed to be kept secret, but a group of anti-government activists found out about it. They staged a massive protest at a small airfield that was the operations center for the exercise. The protest attracted spectators and television cameras. What should have been a secret exercise ended up as the lead story on the six o'clock news.

Investigation

[NARRATOR:] How did the protesters find out about the training exercise? In the days and weeks before the exercise, there was a breakdown in operations security, or OPSEC. Col. Stamburg ordered an investigation to find out how the OPSEC breakdown occurred. You're going to take part in that investigation. You'll hear

what these people knew in advance about the training exercise and examine what they did, or failed to do, to protect that critical and sensitive information. Along the way, you'll examine the OPSEC process. You'll discover how information that seems unimportant, even trivial, can help an adversary uncover critical information. You'll uncover the identity of security threats and adversaries, many of them closer to you than you might think. You'll find unexpected vulnerabilities that allow adversaries to exploit unprotected information. Most importantly, by the time you finish this course, you'll be able to identify ways to limit the significance of information an adversary can collect, and you'll be able to take appropriate steps to protect critical information.

Investigation, Part 2

[NARRATOR:] Here are some of the people who agreed to talk with investigators. None of them are accused of doing anything illegal, and none had access to classified information; however, they all had some advance knowledge of the training exercise. Listen to what they told investigators and rate each person on how well you think he or she protected critical and sensitive information about the training exercise.

[DANIEL, SERVICE MEMBER:] I did NOT tip off the protesters. I first heard about the exercise when I received a call with orders to report to the staging area in the desert. Right away, I canceled a planned birthday rafting trip with my son and his friends. My son was very disappointed. He had been talking about the trip with his friends for months. Once I arrived on location, I had a little free time, so I called home while I was off duty. I took a quick picture with my cell phone of myself and a couple of EOD buddies to send to my son. We weren't in uniform, and we weren't on duty. When I got home, I found my son had posted the picture to his social network page on the internet. He said he wanted to let his friends know I really did have to be someplace else. I didn't think he would post the pic on the internet and certainly not so soon. Maybe I should have warned him, but believe me, he'll know better next time. I don't think anyone saw the picture, but even if they did, they wouldn't have been able to tell where I was or what I was doing. I've made sure his page is password protected. Only his friends could have seen the picture. I didn't tell anybody about the exercise.

[CARLENE, SPOUSE:] I did NOT tell the protesters about the training exercise. I was at the library, and I got a call from my husband on my cell phone canceling our planned visit with his parents this weekend. He told me that I should keep quiet about this. I realized I shouldn't take this call in the middle of the library. So I asked one of the librarians if there was someplace I could take a private phone call. She let me into the staff break room. There were only a couple of other library employees in there. I could have called him back later I suppose, but he didn't have much time to talk. I worry about him so much when he's away and I don't know what's going on. He told me all about his travel schedule and asked me to get in touch with his parents to let them know we wouldn't be coming for the weekend. While I was still in the break room, I called his parents and gave them all the details. I didn't tell anybody else a thing.

[GERRY, AIRPORT FACILITY MANAGER:] I didn't tell anyone about the training exercise, especially not the protesters! Several weeks ago, when I first learned our facility was going to be part of the simulated terrorist incident, I sent out an email marked "Secret" to my employees, informing them about the special security precautions at the south entrance to the airport starting on June 1. My email explained that the south entrance would be closed to airport employees and the general public over those dates. I instructed all airport employees they would have to get here early on those days to avoid congestion. Some employees had to make special arrangements for kids and transportation, so I gave them plenty of advance warning. I also told them the staging area was off limits because there would be a lot of important officials involved, you know, Feds and Washington types and military. I instructed them to see me if they had to get into the staging area. We also had

to arrange for detour signs at the airport ramp from the highway, directing the general public to the east entrance. We know how to do things right around here. I didn't tell anyone else what was going on, just the people who needed to know… the airport employees.

[ELENA, CONTRACTOR:] Don't look at me. I didn't tell the protesters about the training exercise. What was I supposed to do? I had no choice. I got an order from the local Air Force base for 5,000 lunches and dinners: 2,500 for the 2nd; 2,500 for the 3rd. I had to order my supplies, deli meats, bread and rolls, potato salad, cookies, fruit, soft drinks, water, and that was just for the lunches. I had an even bigger order for the dinners. I also had to get extra help from the temp agency. It was a big job, and I didn't have much notice. I mean, we're here in the middle of a desert. Getting the food together for an event that big is a major project. It's not like we're in some big city with suppliers we can call in on a moment's notice. Look, I know my suppliers really well, and I can trust them. So I told them, "This is a big deal for the people at the Air Force base. Half of the Air Force is going to go hungry if you can't deliver on time. I can't let the Air Force down, and you need to make sure I can deliver these meals on the 2nd and the 3rd." Other than my suppliers, my employees, and the temp agencies, no one else knew what was going on. I sure didn't tell anybody.

[EARL, FEDERAL LAW ENFORCEMENT OFFICER:] Well, I sure didn't tell the protesters. But one person I did talk to about the exercise was a reporter. I knew her when she used to work for the TV station here, but now she's out in San Francisco. Somehow, she got wind of big things going on at the Port of San Francisco and the Alameda Naval Air Station. She connected the dots and figured out the base here was involved, so she gave me a call. I advised her to hold up on her story because the things she was about to report weren't really terrorist incidents. If I had let her go ahead thinking the training events were real, she would have had the whole city of San Francisco in a panic. She's like that. She's a typical reporter. But other than that, I didn't tell anyone, and I told her it was off the record.

OPSEC Process

[NARRATOR:] All of the people in these interviews are telling the truth. No one called the protest leaders and told them about the training exercise; however, any of these people, or all of them, may have contributed to the OPSEC breakdown during this training exercise. What is OPSEC? OPSEC isn't a set of rules that tells you what you should or shouldn't say. Instead, it's a process. It's a method of denying critical information to an adversary. Government and military officials at the highest levels of responsibility use the five-step OPSEC process to identify and protect critical information. Cost-effective OPSEC countermeasures should be incorporated into every operation. But OPSEC isn't just their job. It's part of everyone's job, including yours.

[NARRATOR:] The OPSEC process consists of five steps. Each step provides the answers to some very important questions. Step 1 is identifying critical information. This step answers these questions: What information must be protected? Why does this information need to be protected? Step 2 is analyzing threats. Analyzing threats provides answers to these questions: Who is an adversary? What are the adversary's intentions, and what is the adversary capable of doing? Step 3 is analyzing vulnerabilities. This step answers the question: What weaknesses can an adversary exploit to uncover critical information? Step 4 is assessing risks. Assessing risks gives you answers to these questions: If an adversary exploits vulnerability, how will that affect the mission? What will be the overall impact of the adversary learning our critical information? Step 5 is applying OPSEC countermeasures. This step sums up the OPSEC process by answering this question: What will be done to protect critical information?

Step 1: Identify Critical Information

[NARRATOR:] Now let's take a step-by-step look at the OPSEC process. The first step in the process is identifying critical information, the information that is absolutely essential for the success of a mission. Critical information is information that must be protected by OPSEC. Critical information about a given mission or project includes specific facts about what our side can do and what we intend to do. In particular, critical information is any information an adversary can use to keep us from accomplishing the goals of a mission or harm us. Critical information isn't the same thing as classified information. Critical information is often unclassified. Critical information is sometimes revealed by information that's publicly available if you know where to look for it. Quite a bit of information about the training exercise was circulating before the exercise began. Many federal and state government agencies helped plan the exercise. If you looked at the public records kept by those agencies, you could have gathered information about the exercise before it happened.

Indicators

[NARRATOR:] Here's your first assignment as an investigator. Think back to the interviews you heard. Did you hear anyone admit to giving critical information to the protesters or telling them where they could find the training exercise? No one did that. All of these people knew that information about the exercise was sensitive and needed to be protected; however, all of these people provided an indicator to critical information. What's an indicator? An indicator is anything that draws attention to critical information or gives an adversary a clue about what's going on. Unusual activity or changes in routine are indicators that point to critical information. Here's an example: Suppose you're standing outside an office building around noon. If you see people walking out of the building in groups of two or three, you might guess that everything is normal and people are going to lunch. If you see crowds of people rushing out of the building all at once, you might guess there's a fire or other emergency situation. The behavior of people leaving the building is an indicator of what's going on inside. In short, indicators are clues that an adversary can interpret to uncover critical information.

Indicators - Interviews

[NARRATOR:] Indicators often reveal only a little information about a mission. They provide one piece of a larger puzzle. If adversaries collect and interpret enough indicators, they'll have a pretty good picture of the mission. The contractor who was called in to feed the surge of personnel involved in the exercise gave an indicator that called attention to the exercise.

[ELENA, CONTRACTOR:] I know my suppliers really well, and I can trust them. So I told them, "This is a big deal for the people at the Air Force base. Half of the Air Force is going to go hungry if you can't deliver on time."

[NARRATOR:] The contractor was exaggerating when she told her suppliers that half the Air Force would go hungry if she didn't get her job done. That exaggeration was an indicator that there would be a large number of military personnel in the area very soon.

The airport facility manager provided an indicator as well.

[GERRY, AIRPORT FACILITY MANAGER:] I sent out an email marked "Secret" to my employees, informing them about the special security precautions at the south entrance to the airport starting on June 1. I also told them the staging area was off limits because there would be a lot of important officials involved, you

know, Feds and Washington types and military.

[NARRATOR:] The email hinted at the presence of high-level officials and provided specific dates when they would arrive. Most of all, the email was marked "Secret" even though the information was not actually classified. That's a great big flashing neon sign of an indicator that tells an adversary, "This information is valuable."

Step 2: Threats and Adversaries

[NARRATOR:] The second step in the OPSEC process is analyzing threats. Threats to the success of a mission are caused by adversaries. Who is an adversary? An adversary isn't always who you might think. Sworn enemies, foreign governments, or terrorists are certainly adversaries. Adversaries much closer to home may pose threats as well. An adversary is any person or group with intentions and capabilities contrary to our own. Exercise planners wanted to keep the training exercise unnoticed. The training exercise was disrupted by unexpected adversaries with different intentions. A political group that opposes government military activities and weapons development wanted to call attention to the exercise, and it had the capability to do so. The protest group was an adversary, not because of its political beliefs, but because its intentions were contrary to the success of the training mission. Reporters also had contrary intentions and capabilities. They wanted to capture exercise activities on video and report them on the evening news. In this instance, the reporters were adversaries.

Threats - Interviews

[NARRATOR:] A response team member's wife discussed her husband's travel plans in the staff break room of the college library.

[CARLENE, SPOUSE:] I asked one of the librarians if there was some place I could take a private phone call. She let me into the staff break room. There were only a couple of other library employees in there.

[NARRATOR:] Little did she know, several library employees had close ties to campus activist groups that opposed U.S. military policies and took part in the protests. Although there were only a couple of employees in the break room, they may have been involved with groups that should be considered adversaries. The federal law enforcement officer had a long-standing working relationship with a reporter.

[EARL, FEDERAL LAW ENFORCEMENT OFFICER:] I knew her when she used to work for the TV station here, but now she's out in San Francisco. Somehow, she got wind of big things going on at the Port of San Francisco and the Alameda Naval Air Station. She connected the dots and figured out the base here was involved, so she gave me a call.

[NARRATOR:] Her intention to gather critical information about the exercise and her ability to make that information public made her an adversary and a threat to the mission.

Step 3: Analyzing Vulnerabilities

[NARRATOR:] The third step in the OPSEC process is analyzing vulnerabilities. A vulnerability exists whenever an adversary can collect an indicator that points to critical information about a mission. Interpret the indicator correctly to gain valid information about the mission and figure out what the indicator means in time

to do something with the information. The protest group clearly exploited one or more vulnerabilities. It was able to stage a big demonstration because it collected indicators that pointed to the travel plans of military and governmental personnel, including some high-ranking officials; interpreted the indicators correctly to find the date and location of the exercise; and learned about the exercise in time to bring several hundred protesters to the site.

Vulnerabilities – Interviews

[NARRATOR:] During his interview, the service member said:

[DANIEL, SERVICE MEMBER:] "I don't think anyone saw the picture, but even if they did, they wouldn't have been able to tell where I was or what I was doing. I've made sure his page is password protected. Only his friends could have seen the picture."

[NARRATOR:] The service member analyzed vulnerabilities, but he was a bit late in doing so. He recognizes that social networking sites on the internet provide a way for an adversary to collect valuable indicators about future missions. Anyone with access to his son's site could collect and interpret information about his travels.

[CARLENE, SPOUSE:] "I realized I shouldn't take this call in the middle of the library. So I asked one of the librarians if there was some place I could take a private phone call. She let me into the staff break room. There were only a couple of other library employees in there."

[NARRATOR:] This woman took the time to analyze vulnerabilities. She recognized that a public phone conversation might be overheard. She took steps to address that vulnerability by looking for a private place to take the call; however, she continued her call in the presence of library employees in the break room. She shared travel plans with everyone in the room and potentially with anyone who intercepts her phone call.

Step 4: Risk Assessment

[NARRATOR:] Step 4 of the OPSEC process calls for assessing risks. Military commanders, agency officials, and operational planners will make formal risk assessments using a formula that considers the value of assets, the nature of existing threats, known vulnerabilities, and the potential impact of loss of critical information to an adversary. On a personal level, you must act responsibly. It's up to you to carefully weigh the consequences of your actions. Will something you do or say create a vulnerability that can be exploited by a potential adversary? Are you about to provide an indicator that may expose critical information? How would an adversary take advantage of that indicator? What would be the possible effect on the mission if an adversary learns the bit of information that you know? Finally, what's the cost of avoiding the risk? What's the downside of doing what it takes to protect critical information? In most cases, the cost of protecting the information is very low. Sometimes, you simply need to choose not to talk about something.

Risk Assessment Example

[NARRATOR:] The contractor did not take any steps to assess risk. Recall what the contractor said in her interview:

[ELENA, CONTRACTOR:] I know my suppliers really well, and I can trust them. So I told them, "This is a big deal for the people at the Air Force base. Half of the Air Force is going to go hungry if you can't deliver on time. I can't let the Air Force down, and you need to make sure I can deliver these meals on the 2nd and the 3rd."

[NARRATOR:] Her focus was on getting her suppliers to help her deliver meals to the training exercise participants. She talked quite openly about her preparations for the training exercise and assumed that the information she shared with her suppliers wasn't a risk. The airport facility manager also made an effort to assess risk. In his interview, he said this:

[GERRY, AIRPORT FACILITY MANAGER:] "I instructed all airport employees they would have to get here early on those days to avoid congestion. Some employees had to make special arrangements for kids and transportation, so I gave them plenty of advance warning."

[NARRATOR:] The facility manager recognized the need for secrecy as he prepared for the training exercise. As he planned for the influx of visitors, he also weighed the costs of protecting critical and sensitive information. He realized that his preparations would require some airport employees to change their routine, so he shared information early. Unfortunately, by marking his email to employees "Secret," he called attention to sensitive information.

Step 5: OPSEC Countermeasures

[NARRATOR:] The fifth and final step in the OPSEC process is choosing and applying countermeasures to protect critical information. OPSEC measures protect critical information in one or more of the following ways: minimizing predictable patterns of behavior; sudden changes to established routines may alert an adversary to information about a mission; concealing indicators when they can't be avoided; hide unusual activities or changes in routine by pairing them with meaningless changes; providing an alternative interpretation for an indicator. An adversary can't make use of an indicator if he doesn't interpret it correctly. The most effective OPSEC measure may be simply to refrain from saying anything.

Countermeasures - Examples

[NARRATOR:] The service member and the spouse made attempts to apply OPSEC measures. The service member took a couple of precautions. Here's one:

[DANIEL, SERVICE MEMBER:] I took a quick picture with my cell phone of myself and a couple of EOD buddies to send to my son. We weren't in uniform, and we weren't on duty.

[NARRATOR:] Here's another one:

[DANIEL, SERVICE MEMBER:] I've made sure his page is password protected.

[NARRATOR:] The photo he sent home didn't show his uniform or his credentials. That reduced the chances that anyone who saw the photo would connect it to the training exercise. On the other hand, the service member might have thought he was applying an OPSEC countermeasure by making his son add password protection to his social networking website. A password can't provide much protection when the password is freely

shared. His son gives the password to everyone he accepts as an online “friend.”

The spouse applied one very basic OPSEC countermeasure.

[CARLENE, SPOUSE:] I asked one of the librarians if there was some place I could take a private phone call.

[NARRATOR:] Unlike many people you see every day, she didn’t treat a cell phone call she received in a public place like a private conversation. Once she got to the staff break room, she slipped.

[CARLENE, SPOUSE:] While I was still in the break room, I called his parents and gave them all the details.

[NARRATOR:] She could have avoided giving an indicator by keeping her remarks short or going home before relaying the message. If that wasn’t possible, she could have made up a cover story to explain her change of plans.

Investigation Review

[NARRATOR:] Have you changed your mind about any of the ratings you gave to the people interviewed by investigators? Think about how well each person applied the five steps of the OPSEC process. Which steps did each person perform well? Which steps were missed? Click the images to listen to the interviews again. You may change your ratings using the scale under each image.

[DANIEL, SERVICE MEMBER:] I did NOT tip off the protesters. I first heard about the exercise when I received a call with orders to report to the staging area in the desert. Right away, I canceled a planned birthday rafting trip with my son and his friends. My son was very disappointed. He had been talking about the trip with his friends for months. Once I arrived on location, I had a little free time so I called home while I was off duty. I took a quick picture with my cell phone of myself and a couple of EOD buddies to send to my son. We weren’t in uniform, and we weren’t on duty. When I got home, I found my son had posted the picture to his social network page on the internet. He said he wanted to let his friends know I really did have to be someplace else. I didn’t think he would post the pic on the internet and certainly not so soon. Maybe I should have warned him, but believe me, he’ll know better next time. I don’t think anyone saw the picture, but even if they did, they wouldn’t have been able to tell where I was or what I was doing. I’ve made sure his page is password protected. Only his friends could have seen the picture. I didn’t tell anybody about the exercise.

[CARLENE, SPOUSE:] I did NOT tell the protesters about the training exercise. I was at the library and I got a call from my husband on my cell phone canceling our planned visit with his parents this weekend. He told me that I should keep quiet about this. I realized I shouldn’t take this call in the middle of the library. So I asked one of the librarians if there was some place I could take a private phone call. She let me into the staff break room. There were only a couple of other library employees in there. I could have called him back later I suppose, but he didn’t have much time to talk. I worry about him so much when he’s away and I don’t know what’s going on. He told me all about his travel schedule and asked me to get in touch with his parents to let them know we wouldn’t be coming for the weekend. While I was still in the break room, I called his parents and gave them all the details. I didn’t tell anybody else a thing.

[GERRY, AIRPORT FACILITY MANAGER:] I didn’t tell anyone about the training exercise, especially not the protesters! Several weeks ago, when I first learned our facility was going to be part of the simulated terrorist incident, I sent out an email marked "Secret" to my employees, informing them about the special security

precautions at the south entrance to the airport starting on June 1st. My email explained that the south entrance would be closed to airport employees and the general public over those dates. I instructed all airport employees they would have to get here early on those days to avoid congestion. Some employees had to make special arrangements for kids and transportation, so I gave them plenty of advance warning. I also told them the staging area was off limits because there would be a lot of important officials involved, you know, Feds and Washington types and military. I instructed them to see me if they had to get into the staging area. We also had to arrange for detour signs at the airport ramp from the highway, directing the general public to the east entrance. We know how to do things right around here. I didn't tell anyone else what was going on, just the people who needed to know ... the airport employees.

[ELENA, CONTRACTOR:] Don't look at me. I didn't tell the protesters about the training exercise. What was I supposed to do? I had no choice. I got an order from the local Air Force base for 5,000 lunches and dinners: 2,500 for the 2nd; 2,500 for the 3rd. I had to order my supplies, deli meats, bread and rolls, potato salad, cookies, fruit, soft drinks, water, and that was just for the lunches. I had an even bigger order for the dinners. I also had to get extra help from the temp agency. It was a big job, and I didn't have much notice. I mean, we're here in the middle of a desert. Getting the food together for an event that big is a major project. It's not like we're in some big city with suppliers we can call in on a moment's notice. Look, I know my suppliers really well, and I can trust them. So I told them, "This is a big deal for the people at the Air Force base. Half of the Air Force is going to go hungry if you can't deliver on time. I can't let the Air Force down, and you need to make sure I can deliver these meals on the 2nd and the 3rd. Other than my suppliers, my employees, and the temp agencies, no one else knew what was going on. I sure didn't tell anybody.

[EARL, FEDERAL LAW ENFORCEMENT OFFICER:] Well, I sure didn't tell the protesters. But one person I did talk to about the exercise was a reporter. I knew her when she used to work for the TV station here, but now she's out in San Francisco. Somehow, she got wind of big things going on at the Port of San Francisco and the Alameda Naval Air Station. She connected the dots and figured out the base here was involved so she gave me a call. I advised her to hold up on her story because the things she was about to report weren't really terrorist incidents. If I had let her go ahead thinking the training events were real, she would have had the whole city of San Francisco in a panic. She's like that. She's a typical reporter. But other than that, I didn't tell anyone, and I told her it was off the record.

Investigation Results

[NARRATOR:] Here's how you judged the five interviews. Now you can compare your judgements with those of Col. Stamburg's investigators. Compare your ratings with those in the investigation team's report.

Example of Vulnerabilities

[NARRATOR:] This course showed many examples of possible vulnerabilities. Examples of vulnerabilities that you should be aware of include: discussions and phone calls in public places; telephone and cell phone calls that can be intercepted; email messages that can be intercepted; social networking sites, blogs, and other postings on the internet; printed or written information that can be taken out of your trash; disclosing too much information about your mission to family and friends; and unauthorized disclosure of official information to the press.

Examples of Ways to Protect Critical Information

[NARRATOR:] Examples of easy, inexpensive steps you can take to protect critical information include: disclose information about your mission and organization judiciously and on a need-to-know basis; do not discuss your work in public places; do not discuss critical information on unencrypted telephones; do not include critical information in unencrypted email messages; do not reveal critical information, indicators, or personal information on the internet; shred paper documents before placing them in the trash; and refer all inquiries from the press to your organization's public affairs office.

Summary

[NARRATOR:] The investigation is complete. The investigators identified critical breakdowns in following OPSEC procedures that allowed the protesters to find out about the training exercise. The investigators made a recommendation: provide training to help people understand the five-step OPSEC process. Col. Stamburg accepted that recommendation. Congratulations! You have completed the colonel's training course.