Security in Depth

050213 Webinar

Welcome and thank you for standing by. All parties will be in a listen-only mode for the duration of today's conference call. Today's call is being recorded; if anyone has any objections, you may disconnect at this time. I would now like to turn today's call over to Mr. Danny Jennings; sir, you may begin.

All right, thank you. Before we get started please be aware the video portion of this webinar will be recorded, and once we receive the recording light we will begin. All right, I think we got the light. Good afternoon, I'm Danny Jennings. I am the Physical Security Curriculum manager here at CDSE and before we get started I want to thank you all for taking time out of your busy schedules to join us this afternoon. Some of our responsibilities are curriculum development, course instruction, curriculum review of all the physical security training here at CDSE. And today's topic for the webinar today is security in depth, we'll talk about security in depth today. Along with the webinar you're going to have, I think, its two posters, security posters that we made available for you to download. And you can actually use that part of the security education program. My producers for today is Sandy Vega, and Mr. Tim Sutton and at this time we're going to let Sandy, who is going to provide you some instructions on how to use the chat box and poll questions and how to navigate the other portions of the webinar. Sandy.

Thank you Danny. Let's take a quick tour of the DCO meeting room. In the bottom left-hand corner you'll find a notes box. This has the call-in number and other announcements as necessary. These notes will remain on the screen throughout the webinar for your reference. To maximize your view of the presentation, click the "full screen" button in the gray banner in the upper right corner of your screen. However, when poll questions appear, you must click the "full screen" button again to be able to respond to the poll. To the right is a Q&A box for entering questions and or feedback. As all participants' phones are muted this is your only way to communicate with us. Below the presentation you'll find a file/share box. You can download and save the files listed to your computer to record notes on today's presentation. During the webinar we'll be popping up some poll questions, select your answer and we'll provide feedback. Danny, the audience is all yours.

All right, speaking of poll questions, we're going to start today's webinar off with a poll question. What we want you to do is consider one asset at your installation or facility, how do you implore security in depth to protect that asset? As a matter of fact you can give me some examples of security measures that you protect your assets. Okay, looking at the feedback we got security officers; security guards; CCTV; safe for classified information; access control systems; alarms; 24-hour security guards; and those are all security measures we're going to talk about that during our webinar. First, let's look at the webinar objectives. Today we're going to define and list the purpose of security in depth. We're going to identify physical security measures that are used to actually implement security in depth. And we're going to see how those security measures are incorporated or integrated to get to the concept of security in depth.

Let's start with the definition. Security in depth is a determination by the senior agency official that a facility security program consists of layered and complimentary security controls sufficient to deter, detect, and document unauthorized entry and movement within a facility. The key words in this definition is "senior agency official's determination." Your job as a security professional is to understand the concept of security in depth, along with the regulatory guidance, and be able to apply it to security in depth. Understand senior agency officials or commanders are responsible for the particular assets. They need the flexibility to be able to provide those security measures and protection of these assets. So it's their determination that their security program meets that concept of deterring, detecting, and documenting unauthorized entry or movement within a facility. And what is it that we're protecting? We're protecting assets, correct. Now what do assets come in form of? They can be people, information, or operations. Use this acronym that we provided you: PIE-FAO. Some of you may be familiar with it, some of you may not, but as a baseline to actually help you to understand what it is you're in charge with protecting. People is your most important asset, you want to have a security program that actually safeguards the people. Also information, information may be classified or sensitive information. But your physical security program should have measures in protecting that information. What about equipment? Equipment could be weapon systems, computer systems, or research facilities. You should have a physical security program that enhances protection of that equipment. Also facilities. Facilities that are housing the people and information and the equipment. Physical security in depth to apply to that facility to protect that facility and the assets. Also activities and operations. What activities and operations do the people at that facility, what are they conducting? Maybe sensitive information, when you look at activities and operations . . . I want you to take OPSEC, that

critical activities that they're doing may not be classified, but it may need a form of protection. And how do we do this? We do it by safeguarding personnel; we do it by preventing unauthorized access to equipment, installations, and material and documents. We do it by safeguarding assets against espionage, sabotage, damage, and/or theft.

And also the insider threat. That is the key thing to remember. Security programs should have measures in place to safeguard against insider threat. As it pertains to physical security think about your access control procedures. Do you have people that come in, are bags checked going in? Are they checked going out? What systems do you have in place to help prevent the insider threat? Also, you want to control movement within the facility, and you do this through the integration of countermeasures. Which leads us to our first chat question — what are some examples of integrated countermeasures? Go ahead and enter your responses in the chat box: what are some examples of integrated countermeasures? Feedback is: census; spot checks; lighting; ram measures, that is, random antiterrorism measures; cameras; fences; guards; access control bag checks . . . those are good examples of integrated countermeasures, and what do they do for us? Integrated countermeasures are security measures employed to deter, delay, detect, and deny or prevent aggression or attacks on identified critical assets. If you look at your PowerPoint we have an access control system, you have a close circuit television monitoring system, and you have some type of barrier. Integrating these systems. Standing by themselves they provide some level of support, but when you integrate this system they stand to provide you better coverage of your areas. Establishing that multi-layer approach.

Let's talk about the multi-layer approach. Not only does it employ security aids like lighting, fences, and barriers, it also has a human aspect of it. Now let's look at our diagram. If you look at your diagram, looking at your asset is going to be on your most inner layer, that's where your asset belongs. If you look at all the other rings that's protecting your asset, you start with facility layout and construction. You also have visitor entry areas, IDS alarms, surveillance cameras, perimeter entry and checkpoints, fencing and site lighting and barriers. All of these working together in an integrated form to actually protect that asset. Security in depth concept also talks about employing active and passive complimentary physical security measures to ensure protection of DoD assets. What are active and passive complimentary measures? Let's look at an example. A perimeter fence would be considered a passive complimentary security measure. Really responsible for actually deterring a person or defining an area. Look at our AA&E storage facility. At an AA&E storage facility you might have an active barriers system. You also might have active patrolling of a security officer or security guard. Another concept I want to talk about is enclaving, which is a perimeter inside of a perimeter. And as you get

closer to the asset your restrictions get more stringent. Let's take a moment and talk about what happens during the detect, deter, delay, and deny process.

During the detect, deterrent phase of the process understand it's prevention through fear of consequences. Some of the security measures that we have available for us are fences, lighting, posted warning signs, posted signs saying this area is under security surveillance, military working dogs, active patrolling signs . . . all of those are part of the physical security concept of deterrence. Let's look at detection. Detection can occur through security forces, or some type of alert is going to happen, or some type of assessing the situation is going to happen, and it should provide evidence of unauthorized intrusion. We already said security forces, but you can also look at IDS systems. Your IDS system is an unauthorized intruder alerts the alarm, some type of assessment is going to occur with that alarm. It's going to tell you what type of alarm or where the alarm is located, and also it's going to be your first initial response or assessment by a security officer to determine what level of security needed to respond to the alarm. Delaying mechanisms, active and passive measures, like we talked about on a previous slide. Physical barriers, active vehicle barriers, security officers, active patrolling, is to slow and encumbered to the potential adversary, with your initial response. Talk about denying. Really deny is a combination of all security measures brought to better rest of the enemy in action. Understand it's — security officer is looking at your alarm is going off, hopefully that you have enough active and passive measures in place that you can send a response force and they can apprehend or detain the individual to make an arrest. Those are all in the concept to deter, detect, delay, and deny.

What I would like for you to do now is look at the physical security measures that are offered to you. One key point I want to make about physical security measures is that your operational environment is going to be different, whether it's an installation, in-CONUS, on installation, over-CONUS, overseas. It's going to be different between a leased government facility or a contracting facility. So you may use these security measures, you may not use all of these security measures. You might even have to add to these security measures, but it depends on your operational environment. Security in depth on an installation may be different between a security in depth with a leased facility, or a contracting facility. But understand that these measures are actually for your use. Let's talk about the barriers. We said the barriers actually define an area, has to provide some type of deterrence, and it may provide some type of support for vehicle entry. And actually, really, traffic control and vehicle control, a person and vehicle. Fencing, fencing does the same, it provides some type of deterrence, define an area. What about clear zones? We have special areas that require regulatory guidance to have clear

zones. Clear zones are for security officers and security guards, security personnel to have observation of the perimeter. Naturally you will not have a clear zone, maybe, possibly, at a leased government facility, maybe not, probably not.

We also have signage and lighting. If you look real close we also talk about doors and windows. Which, your doors and windows at a facility, that's going to be your most vulnerable areas. We'll go more in depth with some of these security measures. Right now we're going to do a poll question. How do security measures, we just talked about and listed, what is considered the most valuable countermeasure you can use? Is it access control system, intrusion detection system, or security personnel? We're about at 85 percent says security personnel, couple people are saying and choosing detection system, and some people are saying access control systems. Okay we're going to go ahead and end it there, we got about 83 percent that's going to say about security personnel. And I'm going to actually agree with security personnel, is going to be your most valuable countermeasure. Let's see why. Understand that the security force provide the enforcing element of physical security program. Security force may consist of military police, federal government police, that's the old 83 series, security guards 085, contract security guards, and possibly K9 teams. And understand their focus is going to be on law enforcement, crime prevention, physical security, critical assets, and sometimes protection of high-risk personnel and access controls. Security officers are also going to be the ones that monitor your IDS systems and response forces. Understand that the other security measures or physical security measures are just training aids or pieces of equipment. They are not going to take the place of a live person that's trained in security, who actually are helping to augment your program. So that's going to be your most important element, security personnel.

Access control systems. Access control systems ensure that only authorized personnel gain access to controlled areas. Understand that they can be manual or automated. If they're manual it's going to require a security officer checking or verifying credentials and personal recognition. If it's going to be an automated system, they're going to consist of electronic locks, card readers, biometric meters, alarms, and other computer systems to monitor access control. If it's an automated system the individual's credentials compared against a database, once approved, systems sends out input signals allowing authorized personnel to pass through the controlled portals. What happens is there's some type of verification and authentication that occurs in these systems. One thing to note that if you think about your automated systems, you look at biometric readers, is going to be your more expensive type of automated system. And understand when you start looking at biometric readers, the data input of the individual

information that has access to your area is going to actually take a lot longer, and more expensive. Depending on your asset depends on how you want to secure it.

Closed Circuit Television System. CCTV systems integration of cameras, recorders, switches, keyboards, and monitors to allow viewing and recording during security events which are utilized for alarm assessment and surveillance. If you're going to use a CCTV monitoring system, you can hook it up to your IDS system, where if an IDS sounds an alarm that monitoring system will actually view to where the alarm is. Or if you have a person looking at a TV monitoring system, you can use it as an alarm assessment. It also can be used as a surveillance system. For instance, if you look at the recent events with the Boston marathon bombing, surveillance video used from surrounding areas were utilized too, actually, and resulted in an arrest of one of the subjects. So depending on what your area and what your requirements are you can actually employ a CCTV system in this type of environment.

Physical Barriers: Physical barriers are utilized to deter and delay a physical barrier, define a perimeter, establish a physical and psychological deterrent to adversaries; it may delay and disrupt an attack, channel a flow of personnel and vehicles through designated areas, and understand it can be natural or manmade.

Signs: Signs are used to deter an individual, provide warning of restricted areas. Signs should be positioned to assist in controlling authorized entry, deterring unauthorized entry, precluding accidental entry. Signs should be clearly displayed and legible, bilingual for areas where multiple languages are spoken, and depending on your location or specific program you're working with, is going to depend on how far your sign should be spaced out. And it should be visible from any approach to the perimeter from a reasonable distance.

Security lighting: Security lighting can be used to deter, detect, and delay an aggressor. Security lighting should discourage and deter entry attempts, make detections likely, prevent glare for guards — understand we're talking about preventing glare for guards when you're positioning your security lighting, it should not come as a hindrance to your security personnel that is monitoring your perimeter or your access control point. It may be also used to incapacitate a person temporarily; for instance, if you ever have approached a military installation at night trying to gain access, if you pull up on to the installation you know that the

lights are positioned outward. At some moment you kind of lose a little bit of your vision. This actually enables the security officers to determine your location and able the security officer for him to approach your vehicle. Understand that security lighting should not impede CCTV or other automated monitoring systems. If you're going to use security lighting, you have a CCTV system in place, make sure that they augment each other. A lot of times if you're looking at night at security lighting and it does not give you the picture that you're looking at, it actually has blind spots, your color differation is off, make sure that it compliments your CCTV system.

Which leads us to our next chat question, number 3. What physical security measures could be used to safeguard this facility? What I'd like you to do is actually send me the number. Write down on your piece of paper, but send me the number of physical security measures that you'll utilize to secure our facility here and we'll match it up to what we have. All right, I'm looking at four to seven. I think the highest number I got is seven. Unlike last iteration — I think we had somebody with fifty-four and I think we had — he was developing a bunker, I think, to secure his area. Okay, we got a twelve. All right, we're going to go ahead and see the results. Here's our solution. About barriers, we just talked about barriers, sight lighting, security personnel, fencing, signage, access control systems, video surveillance system. Now if you got more than that, and I'm sure that they're more than that, like fence spacing in between the fence, could be like a delay mechanism, but you're doing good, appreciate it. One key point I want to do before we wrap up here is to actually — we talked about security in depth a little but we want to talk about more physical security planning. Not only is security in depth important but physical security planning is important, that you integrate physical security planning with other security programs and/or disciplines, such as law enforcement. We already talked about the importance of law enforcement in your physical security planning. Law enforcement is going to be your response force that's going to enforce your procedures, it's going to provide security for you, it's going to be your folk that monitor your IDS systems, and law enforcement can also be used to test physical security equipment. You want to integrate OPSEC into your physical security planning. Information may not be classified but it still may be sensitive enough that you do not need anyone else to share that information. Classified information, information security. Physical security planning should be integrated with your information security program, protecting that classified information. Also, personnel security. The security planning should be incorporated in your personnel security program. How you're going to verify the people coming into your installation, who is authorized, who is not. How you're going to conduct your access control, in and out of your installation. Are you checking people going out? How are you vetting people coming in? Also COMSEC, COMSEC equipment. If you have a security program that has COMSEC equipment, the security planning on how you're going to protect that equipment. Intel and counterintelligence, that information should be coordinated

with your physical security planning, should integrate counterintelligence information. Vulnerability, your threats and antiterrorism goes hand-in-hand with physical security. Vulnerability assessments, criticality assessments, you use antiterrorism doing those types of assessments, actually coming down looking at your area from a terrorist standpoint. And the ultimate goal is an integrated and coherent effort.

Physical security planning got to be integrated with your other security discipline. In summary, we define and gave the purpose of security in depth with identified physical security measures and we actually engage some examples of incorporating physical security and how to obtain security in depth. And if you want to learn more please go to our eLearning courses . . . . we have several that are online, "Introduction to Physical Security," "Physical Security Measures," "Physical Security Planning and Implementation," "Physical Security Virtual Environment Assessment." And we also have an instructor-led course, five-day course, "Applying Physical Security Concepts." Next iteration is 5-9 August 2013 here at Linthicum, Maryland. This course is built off the Risk Management model where they go in and actually conduct a risk management, go through the five-step process identifying assets, vulnerability assessments. And also we look at it from a physical security manager's standpoint, where you actually look at countermeasures, where you go through the analysis process. You actually have to write statements of work and actually procure equipment. That's a real good course, so we have slots available and invite you to come out. If you have any questions about this webinar and others, please visit us at PhysicalSecurity.Training@dss.mil, that's PhysicalSecurity.Training@dss.mil. And if you have any comments or questions about the information pertained in this webinar please visit us at the below locations. We're always interested in your comments on what else can we actually train on for a VI Webinar. If you have any suggestions or anything you would like to see us train you on, visit us at PhysicalSecurity.Training@dss.mil. Once again it's been a pleasure, thanks for you coming out and joining us today. Make sure you download the 2 posters that we have for it and we will have this presentation available for you online, I believe by next week, that you can actually download the presentations. Once again thank you for your time.