

Parts of a Physical Security Plan Webinar  
April 4, 2013

Welcome and thank you for standing by. All participants will be able to listen only. Today's conference will be recorded; if you have any objections, please disconnect at this time. I would like to turn the conference over to Mr. Danny Jennings. Sir, you may begin.

Good morning and welcome to the Physical Security webinar. We would like to thank you for taking the time out of your busy schedules to join us today. My name is Danny Jennings; I am the Physical Security Curriculum Manager here at CDSE and I will be your host for today's webinar. Some of my responsibilities are design and development of the Physical Security curriculum. I am also responsible for course instructions and our curriculum review. The topic for today's webinar is going to be Parts of a Physical Security Plan. We're actually going to give you an overview of a physical security plan. At this time I would like to introduce my producers, Ms. Rachel Mongeau and Mr. Tim Sutton. Rachel is going to get us started on some instructions on how to navigate the tools and how to participate in the webinar. We've got some poll questions that we're actually going to have you guys participate.

Rachel: Thank you, Danny. As you can see here in the left hand corner, there's 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 on the full screen button in the gray banner in the upper right-hand corner of your screen. However, when poll questions appear, you must click on the "Full Screen" button again to be able to respond to the poll. To the right is a Q&A box for entering questions/feedback. Since all participant phones are muted, this is your only way to communicate with us. Below the presentation you will find a file share box. You can download and save the files listed to your computer and it's a way to record notes on today's presentation. You'll find a Word document containing the template we will be discussing today and a PDF file of today's slides. At the end of today's presentation we'll be giving you some poll questions. This shows you what a poll question looks like; all you'll need to do is provide your responses in the boxes as you can see indicated with a green arrow. To get us started we're actually going to have you respond to a chat question—and Danny, I'll let you take it from here.

Danny: Okay. In order to gauge your experience in dealing with physical security plans, we want to see what your experience is, and I want you to use your chat box down here to determine what has been your personal involvement in establishing a physical security plan. Want to kind of gauge the audience on this. Were you helping develop the plan, or you did it all by yourself, or you never had a chance to actually be involved in that? If some people had to develop a plan all by yourself—hey, my feelings go out to you. Looks like we have a variety of experience in developing a physical security plan. And I'll tell you for those that have been involved in this process, you understand that it was a huge collaborative effort on your part to actually get this done. And hopefully that you had a physical security plan that were already in existence that

you could use from, but if you start from scratch, I know that it was very challenging for you. And that lets us lead to this template we're going to provide to you. It's going to be a takeaway that if you're developing one you can use it as a baseline to help you do that and get you to where you need to go and you can curtail it to what your mission is. So that's one big take from this webinar.

Let's look at today's objective. Once again, we're going to provide an overview of a physical security plan and we're going to provide a definition and purpose of the physical security plan. We're also going to talk about physical security plan responsibilities; you as the security specialist and your commander. We're also going to talk about the components of a physical security plan.

What is the definition and purpose of a physical security plan? Bottom line, it provides guidance on how installation commanders and facility directors consider threats, assess the vulnerabilities, and plan for the protection of DoD assets and safeguarding badges. Now, a physical security plan may be for an installation or facility. Regardless of what size or what your mission is, all of the physical security plans should have three things in common. They are: a physical security plan should be practical, flexible, and responsive.

When we talk about they should be practical, have you ever, when you're doing this coordinating, developing plans, or writing policies, a lot of times you're sitting in your office and actually writing stuff on paper. But if you know as well as I do that a lot times you write stuff down on paper and it does not mean that it's practical. Bottom line, it looks good on paper but when you try to put it into effect, it does not actually go the right way. So you want to make sure your plan is practical. And how you ensure that your plan is practical when you're writing these policies and doing these coordinations, make sure you're out there talking to tenant units and other areas that are responsible for the support of the security of the installation and you're actually walking that installation, making sure that what you put on paper is practical and you can implement it. A lot of times talking to security officers, security guards, and security personnel will actually help you in that event.

The next part is we're talking about the flexible. Your plan should be flexible. Understand that your threat is going to change, your operational environment is going to change, so does maybe your agency mission. So you're going to make a plan that is flexible to those changes.

Also, a plan should be responsive. It has to be responsive to the needs of the commander's or the agency's facility director's intent. It has to be responsive; make sure that it actually can execute what the plan is documented for.

Some of the responsibilities—the overall responsibility lies with the commander or the agency's head or the facility director. A person who is responsible for the protection of DoD assets. Your role as a physical security specialist—or physical security manager or officer—you have different titles but the same responsibilities. Your job is going to be to develop and prepare the

plan. You're also going to be responsible for coordinating the effort. You're going to be doing all the work for it, and you're also going to be responsible for making recommendations on physical security measures that are included inside your plan. So really you're actually doing the legwork for the commander, but the commander has the overall responsibility for the physical security plan.

You want to treat your plan as a living document. Meaning that you should be updating and checking the plan constantly according to how many changes that are current within your operational environment. You've got to understand the agency's threat, mission, and operational environment is going to change, never going to be constant, and so should your plan. If you do not look at your plan, you look at my friend here on the right, your plan will become extinct, become ineffective. At a minimum, it is recommended that you should review your plan annually. So when you actually help develop this plan, I tell you, if you ever have to work on one, you develop it, you're glad that it's finished, you do not put it on a shelf, you have to go back and revisit it cause things change.

Now for an installation, there is normally one overarching physical security plan that is probably going to be supplemented by tenant units, subordinate's unit plan, and it's going to depend on how large your installation is if you're going to have one overarching plan. If you have a physical security plan for a facility or an agency, you may not have an overarching plan. But understand, this plan on an installation, you got one overarching plan—supplemental units will have responsibility for developing their own plan, and actually it's implemented by standard operational procedures or general post instructors for security personnel.

What are some of the basic components of a physical security plan? Well I'm going to tell you, depends on, it's going to be based on really, your component's guidance. And if you don't have component's guidance, you're going to have to base it on your size and installation and your unit's mission. Now I'm going to tell you I thought this claimer out there, that these are some of the basic components that we feel that were important, but like I said, get with your component's guidance that they have regulatory guidance that they want you to follow and ensure that you follow these guidance. But at a minimum we want, we thought that is was important that a plan should have a purpose. Should have a responsibility section, should have a policy section, and we should have access control measures. We're going to talk about security aid and we're going to talk about annexes to a plan. But once again, this is a just a recommendation, get with your component's specific guidance if you have it to actually go by. But if you don't have component's specific guidance, that's why we're going to give you this template to actually get you started. Like a baseline to help your curtail that plan if you're developing one for your benefit.

The first one we're going to talk about is the purpose. Now what we've done here is we've taken a portion of a job aid or the template and we're going to actually use it in a slide. The purpose: when you're setting a purpose, that's going to be a commander's or director's intent. It's going

to state the purpose of the plan. And we list an example here. This plan identifies the physical security policies and procedures for securing and safeguarding the assets of a specific facility and/or installation. You want the commanders' intent, or I think in some CONUS, it might be called the executive summary, but you have to state the purpose—very important. Also in that purpose you might want to include a brief summary of describing installation and a tenant organization.

Alright, this area we want to talk about is responsibilities which is also important. It's important that you list the agencies, directorates, offices, and the titles of the responsible people that are responsible for the security and supporting your agency's or installation's operations. Some of these examples could include installation commander, the director of law enforcement, director of information management, and your director of maintenance or whoever is supporting the infrastructure of the installation, your security manager officer, antiterrorism officer, your intelligence/counter intelligence officer, and commanders/directors of tenant units. They need to understand what their roles and responsibilities in support of the installation physical security plan and identify the agency.

We also included a policy section and we think that it's important that you define how you're going to provide area security. Meaning, how is the commander going to establish and define the areas of the buildings and other structures consider critical and establish priorities their protection. What the commander is charged to do, he has to go through a risk management process, identify his critical areas and determining their priorities, and establishing a security level to protect those assets. Some of the examples that we list are Category 1—if you look to the right, will probably be your Maximum Level Security, Category 1 is probably going to be considered your priority category, your most critical asset and whatever maximum level security requirements are, that's how the assets are going to be protected. Category 2 would be Advanced Level Security, and Category 3, Intermediate Level Security. Just some examples.

It is also important that you want to actually document on how you're going to control access to your installation or facility. How are you going to control your people, material, and vehicles. At a minimum you probably want to break it down to personnel access, material control, and vehicle control. You can get more specific if you want, but for personnel access you want to think about authority for access, what's the criteria for access, how you're going to get your visitors on post, what about your permanent employees, what type of badge systems are you using, how are they going to be vetted—things to think about.

What about material control? What types of materials are coming in, what type of mail is coming in? Depends on what type of facility that you have, but you want to have a plan that is going to acknowledge incoming material and outgoing material. Also, you might want to include vehicle control; what policy do you have if you have to search government vehicles versus POVs? If you're not searching vehicles, what are the parking regulations that's going to be enforced? What critical assets or restricted areas that you have on that installation or facility

that are going to require special parking? What kind of controls for interest to restricted areas and administrated areas? Some things you want to consider, once again, guys, this is just a template—it's not all inclusive—you can use this to curtail it to whatever your needs are.

You also want to list security aids and what is a security aid; security aids are those security measures that you use to implement security protection of your DoD assets. Some examples are your protective barriers, do you have a protective barrier plan, how are your fences going to be listed, what type lighting systems are going to be required for special areas or general areas? Do you have emergency lighting listed, those types of things you want to look and how they are going to be implemented or employed in physical security plan? You also want to list your IDS systems. You want to list what type of system it is, who will be monitoring it, do you have coordination for response forces with the monitoring on that, is going to be on the installation, off the installation, are you responsible for the maintenance on it, who's responsible on the maintenance of it, how it's going to be implemented, that type of stuff.

We also want to talk about annexes. Depending on how you chose to structure your plan, you may have several annexes that may be separate, separate from the physical security plan or actually a part of the physical security plan. And I'm going to tell you, if it's going to be separate from the physical security plan, depending on your operational structure, a lot of times you might want to separate an annex from your security plan and in fact it may be classified. One thing to remember if it is classified—or if it's not part of that physical security plan—you want to make sure that you indicate the location of the annexes.

Now, we have several possible annexes, once again, this list is not all inclusive—let's take a look at that, some of them you might be familiar with, some you may not. And we list the annexes from A-R on your template and in the body some short examples of what they would entail. Now we're going to go through some of these that most are familiar with you and give you some examples.

Guys, it's going to be important that you list all DoD Component or specific guidance and regulations applying to the physical security of the installation or agency—and these references could come in the form of directives, regulations, instructions, manuals, and etc. But it's very important that you list all the references that you used that are part of enforcing that security and providing that policy for security of the installation or facility.

It is very important that you list installation's threat statement, and this annex is going to provide current intelligence threat information pertaining to terrorists, criminal, civil disturbance, and other threats. And understand you're getting this from your threat assessment and your threat assessment is going to drive protection efforts of your risk management process. It's really going to dictate how you're going to execute your protective measures securing your assets. This is very important that you have that, this statement in your plan. It's going to give you the reason why you're protecting your assets.

You also want to include your bomb threat plan. You want to have procedures addressing your bomb threats with guidance on control of the operation, evacuation, search, who's responsible for responding to bomb threats, have you coordinated with DoD, or is it on installation or off installation, how you're going to evacuate the personnel—and each unit should have a bomb threat check list and you should have an example of that actually inside your plan. You also probably also want to include an after action review or a report on your actions of the bomb threat plan, especially if you actually rehearse that.

It's also important to have a natural disaster plan. It's important that you address natural disasters in your plan that is coordinated with local law enforcement agencies and emergency operations. Understand that you need to have a liaison with local emergency communities that support that type of effort, and that you have a plan in place, that is going to assure you're going to shelter and place evacuation, what are your communications, you have alternate communications in this plan, are you coordinating on how you're going to protect that asset. It may be classified material; do you have an evacuation or recovery plan for that? You think live personnel and then property. Make sure your natural disaster plan is actually in line with the area that you're with, cause we've seen in recent history that we have a lot of earthquakes, monsoons, a lot of hurricanes, and stuff like that so this is very important.

Another plan we want to talk about is your resource plan. How are you allocating resources? Need to have a plan that is going to address your equipment, funding, personnel—at a minimum you should have contact numbers and services for the services of the people that ask you those type of support elements. How are you actually going to resource you're existing, or if you have a contingency plan that may require a upscale of security? What type of resource plan do you have to fund those requirements and how they're going to be executed? Just something to think about.

It's also important to have a communication plan, one that's going to address requirements to include systems and networks and the infrastructure to support command and control. You want to have a communication plan and an alternate plan in case of natural disasters. You might have a separate plan that is going to address your networks and communication systems, but also your wireless, cellular, and mobile radio systems. What type of plan do you have—it's very important to address your communications plan.

We also listed intrusion detection system plan. You also want to have an annex that is going to address the type of IDSs that you're going to require around your critical infrastructure, the type of maintenance that is going to be required, the type of who to call in case that your point of contact—especially on your critical assets—who's going to be the point of contact for that, who's going to be point of contact for the maintenance. Also, you may want to list maybe the alarm rates, the false nuisance rates, inside the plant what type of sensors is going to be on the assets. It's very important that you address your IDS systems.

Talk about contingency plans, like contingency plans is going to be all the other plans that actually coordinate with all the continuing operations in case of natural disasters, or a national disaster, such as a large terrorist threat or incident. What are your contingency plans for that? Really it's going to be your plan B; what are you actually going to do. Now your contingency plan will—actually should be in line with your COOP plans, your higher continuing operations plan are some things you might want to look at.

We also want to address your post orders. Guys, at a minimum your physical security plans should have standard operational procedures for your security personnel, meaning the people that are responsible for the protection of your critical assets. We're talking about your security officers, your security police, security guards, security personnel to have post orders establishing their responsibilities of their post. You need to include that in your plan.

And this is going to lead us to our I think our next, first poll question, right Rachel,?

Rachel: Yes.

Danny: It serves as a review, you'll see the poll question on the screen now. Asks you to think about in which section of a physical security plan would you find information about gaining access to a facility. Would that be in the purpose, responsibilities, or access and control measure section? Alright we're looking at it, alright, we're getting here, it seems like the majority, well, here we go, we have 100 percent. Majority picked the access and control measures, which is absolutely right on target, right on point. Understand that you want to address your access control to your facility and or installation. You want to break that down as a minimum. Okay, you want to address your personnel, material control, and how you're going to have vehicle control. Good job everyone.

Next poll question. Here we're asking who has overall responsibility for the physical security of an installation and/or facility? Would that be the physical security manager, antiterrorism officer, or commander or facility director? Who has the overall responsibility? Alright, you're still responding, believe it or not. Okay, you just finished and majority of you, about 98 percent said the commander or facility director, which that would be correct. Understand the key word in this is overall responsibility. As a physical security specialist, manager, officer you're responsible for coordinating, making recommendations, and actually developing a plan, but the commander or agency director, a facility director is going to have the overall responsibility for that, and you're actually going to be executing—coordinating those efforts and actually helping develop that plan for that commander or agency, director, or facility director, so good job.

Next question. In what section of the PSP would you find supplemental plans? Would that be the security aids section, the annexes, or in the references section? Alright, we're at a 100 percent, almost a 100 percent, one person. Okay, it's going to be annexes, and actually it's going to be where you put all your supplemental plans—understand any of your annexes may be part of your physical security plan, or it may be separate. And for operational purposes a lot of times if

a plan may be part of your annexes, some of your annexes may be classified, it would have to be separate from your physical security plan. Alright good job, great job guys.

Next question. True or false, plans need to be practical, flexible and responsive. Alright a 100%, you're absolutely correct, that is a true question. Plans have to be practical, flexible and responsive. Has to be practical in the fact if you got to be able to execute your plan, have to be responsive to your protection of your installation, got to be executable and has to be flexible to change.

Alright next slide. Okay, guys, we're coming to the end of this webinar, hopefully you enjoyed it. So real quick high overview, so understand when you're talking about physical security plans, understand that the risk management process has to be implemented early in your physical security planning. Physical security planning needs to be integrated throughout all the other disciplines. So some level of physical security is going to exist in information, personnel, industrial or COMSEC, any other disciplines and/or special categories. You've got to have physical security planning implemented in that. We talked about the definition of purpose of physical security plan, we talked about physical security plan and responsibilities. We also listed the basic components of a physical security plan and we also said seek your agency's or component's guidance for the component of a physical security plan. But if you don't have one, please use that template that we provided for you and to help to get you started. If you want to learn more about physical security planning, please try our eLearning courses: Introduction to Physical Security, Physical Security Planning and Implementation and Physical Security Measures. We also have an instructor-led course; it's a 5-day course which we talk about physical security planning. The name of it is Applying Physical Security Concepts Course, 5-day course and we actually take the risk management process and we break it down step by step along with physical security planning. It's a great course, next iteration August 5-9 and hopefully we'll see a lot of you there.

Now here at CDSE we're always interested in what you think and any questions that you may have; if you have topics that you want us to do in physical security as it pertains to a webinar, please email us at [physicalsecurity.training@dss.mil](mailto:physicalsecurity.training@dss.mil) and we would be happy to look at what your requirements are. Naturally, we have to get it vetted first and see if we can actually do it, but if there's something else out there you want us to actually deliver a webinar on, please let us know, don't hesitate.

Well, that's going to wrap it up guys, as you see here is some more contact information—we're on Facebook and YouTube. Once again on part of CDSE and the Physical Security team want to thank you for coming out and joining us today, and we really appreciate your time and attendance and hopefully you'll have something to take away and we appreciate it. Thank you.