Parts of a Physical Security Plan

Welcome

[Narrator] Welcome to the Parts of a Physical Security Plan Short.

Introduction

[Narrator] To protect Department of Defense, or DOD, assets, installation commanders and facility directors need a structured method to consider threats, assess vulnerabilities, and plan for protection of DOD assets.

A Physical Security Plan clearly defines an installation or facility's protective measures.

By the end of this Short, you will be able to identify the importance of each part of a Physical Security Plan in protecting DOD assets.

What Does a Physical Security Plan Do?

[Narrator] The Physical Security Plan is the blueprint for protection of DOD assets. Most importantly, the Physical Security Plan must be practical, flexible, and responsive.

A practical plan is one that personnel can implement, versus a theoretical plan that may not be possible to execute. For example, a plan to search vehicles at the installation's entry gate can only be implemented if the facility has proper equipment and personnel to do the searches.

A flexible plan can change as needed based on the environment. For example, if an event on the installation requires more personnel at the entry gate to search vehicles, a flexible plan will identify sources for the additional personnel and allows for an additional gate to be available for entry.

A responsive plan is both practical and can change quickly to deliver the intended end result. For example, during a severe weather event, the plan may require personnel who guard an installation to stay on the installation during the weather event so that security can be maintained.

The Physical Security Plan could be classified, controlled unclassified information, also known as CUI, or unclassified. It must be protected accordingly.

Role of the Physical Security Plan

[Narrator] Developing a Physical Security Plan, or PSP, requires coordination with multiple offices and is referenced for a variety of reasons. The PSP is the responsibility of the Commander or Facility Director.

The Physical Security Manager prepares the PSP in coordination with other offices and support agencies. The PSP is a living document that is edited or updated as needed. PSPs for installations and facilities are usually one overarching plan that may be supplemented by local, command, or facility directives.

PSPs are often implemented by standard operating procedures, or SOPs, and Post Orders. PSPs are reviewed and updated as needed or, at minimum, annually.

Knowledge Check 1

A Physical Security Plan outlines how a facility or installation will _____ DOD assets.

- hold
- assign
- protect
- interpret

Meet Mr. Jansen

[Narrator] Meet Mr. Jansen. He is a Physical Security Manager at Fort Delta.

[Mr. Jansen] Good to meet you. Glad you could join me today. One of my responsibilities as Physical Security Manager is to develop a PSP. I'll share with you what I have been learning.

The PSP can have six parts:

- Purpose of the Plan
- Responsibilities
- Policies
- Access Control Measures
- Physical Security, and
- Annexes

To help me write the plan for Fort Delta, I have been looking at a Job Aid, the Physical Security Plan Template, from the Center for Development of Security Excellence, or CDSE.

I also have been looking at two PSP models from fictional military installations. One is from Fort Bravo, and another is from the National Defense Center, or NDC. Let's see how we can use these resources to write a plan that truly captures how to implement physical security measures here at Fort Delta. As we review each part, you'll see a writing tip you can use when you're working on your own plan.

Part 1: Purpose

[Mr. Jansen] Part 1 of the PSP helps us understand the purpose of the document. Part 1 is also called a commander's intent or executive summary. It may include a brief summary describing the installation or facility and tenant units. It may state the installation or facility's mission. Reading this excerpt from the Fort Bravo PSP helped me understand the importance of the plan and components I'll need to include. I highlighted sentences that best describe the plan's purpose.

Model from the Fort Bravo PSP

Proper physical security protective measures, when implemented, can have a significant deterrent effect on terrorists, criminals, and insider threats. Even if not completely effective in deterring an act, these measures can serve to limit and mitigate damage and save lives. **Physical security measures or countermeasures** implemented on Fort Bravo create the backbone of the installation's efforts and **serve as the first line of defense against threats and attacks**. The Fort Bravo Physical Security Plan is built based on mission assurance, critical assets, identified threats, vulnerability, and risk analyses. The PSP incorporates an integrated approach that employs security-in-depth, or SID. These measures are complemented by asset-specific measures and Force Protection Condition, or FPCON, measures tailored to Fort Bravo. **This PSP outlines the layers of defense needed to protect Fort Bravo, Maryland, facilities and personnel from identified threats and attacks.**

Based on what I've read, the PSP outlines defense countermeasures needed to respond to various threats and attacks. Defense countermeasures include FPCON measures, asset-specific measures, and layers of defense. Threats and attacks could come from terrorists, criminals, and insider threats. The PSP outlines defense countermeasures needed to respond to various threats and attacks.

Defense countermeasures	Threats and attacks
• FPCON measures • Asset-specific measures • Layers of defense	• Terrorists • Criminals • Insider Threats

[Narrator] It may be best to write Part 1 last after you've become familiar with all the plan details and are ready to summarize them in broader terms.

Knowledge Check 2

Part 1 of the PSP outlines the purpose of the document. Based on the Fort Bravo model, what is most important to communicate in this section?

- Needs for emergency responses
- The impact of threats and attacks
- Hazards within a facility or installation
- The role of defense countermeasures

Part 2: Responsibilities

[Mr. Jansen] Part 2 lists people responsible for physical security and what their specific responsibilities are related to the physical security of the installation or the facility.

These are roles you could include:

- The Installation Commander or Facility Director
- Director of Law Enforcement
- Director of Public Works or DPW
- Physical Security Manager
- Antiterrorism Officer or ATO
- Intelligence and Counterintelligence Officer
- Commanders and Directors of Tenant Units

[Narrator Tip] It may come naturally for you to write the description of your own responsibilities first and use that as a model for writing the responsibilities of others.

[Mr. Jansen] Let's look at a model from the National Defense Center, or NDC.

The NDC Physical Security Manager will:

- Manage the NDC Physical Security program for the Director of Law Enforcement and Physical Security, or DLEPS.
- Coordinate and facilitate the Physical Security Council and Force Protection Council.
- Organize physical security plans with agency and tenant unit security managers.
- Author and maintain the NDC physical security plan.
- Coordinate with Department of Public Works, or DPW, and contractors to install and maintain physical security equipment such as intrusion detection systems, or IDS, closed-circuit television, or CCTV, barrier systems, and other equipment and countermeasures associated with physical security.

This model shows the Physical Security Manager interacts with, at a minimum, the Director of Law Enforcement and Physical Security, agency and tenant unit security managers, and the Department of Public Works.

This is a good model for me to begin outlining my own responsibilities. I'll also need to contact others at Fort Delta with physical security responsibilities and work to accurately document their roles.

Part 3: Policies

[Mr. Jansen] Part 3 defines the areas, buildings, and other structures considered critical and establishes priorities for their protection.

[Narrator Tip] First, generate a list of critical items on the installation. Then categorize them by security level.

[Mr. Jansen] On our installation, these are some assets needing security. They include chemical storage, media equipment, an Automated Teller Machine, or ATM, a Communications Security, or COMSEC vault, and a Sensitive Compartmented Information Facility, or SCIF. Next, think about the impact if any of these items were compromised. Our template and the NDC model describe four levels.

Assets	**Building #**
Chemical Storage	12
Media Equipment	5
Automated Teller Machine (ATM)	5
Communications Security (COMSEC) Vault	54
Sensitive Compartmented Information Facility (SCIF)	23

[Narrator] Category I (Maximum Level Security): This level of security is required for an area containing a security interest or defense resources. Its compromise or loss would have an immediate effect on the defense potential or capability of the United States.

Category II (Advanced Level Security): This level of security is required for an area containing a security interest or defense potential or capability of the United States. The total security effort for these areas should provide a high probability of detection and assessment or prevention of unauthorized penetration or approach to the items protected.

Category III (Intermediate Level Security): This level of security is required for an area containing pilferable material or sensitive items that have an attraction for the intruder in addition to monetary value. These areas may contain equipment necessary for the continual functioning of the activities, but not necessarily a part of the immediate or near-term mission or defense capability. These areas should be provided physical protection through isolation, barrier systems, IDS-CCTV, and access control or a combination of these. The total security effort for these areas should provide a reasonable probability of detection and assessment or prevention of unauthorized penetration, approach, or removal of the items protected.

Category IV (Basic Level Security): This level of security is established to protect pilferable items or for the principal purpose of providing administrative control, safety, or a buffer area of security restriction for areas of higher security category. The items within the area are essential to continue base operations and should be afforded additional security or consideration during increased FPCONs.

[Mr. Jansen] Based on these definitions, we could categorize our assets at Fort Delta as follows: Chemical storage and the SCIF both need maximum level security and are in Category 1. The COMSEC Vault needs advanced level security and is in Category 2. Media equipment needs intermediate level security and is in Category 3, and the ATM, requiring basic level security, is in category 4.

Assets	Building #	Category
Chemical Storage	12	I
Media Equipment	5	III
Automated Teller Machine (ATM)	5	IV
Communications Security (COMSEC) Vault	54	II
Sensitive Compartmented Information Facility (SCIF)	23	I

In the PSP, I will also include descriptions of the protection we currently use on each asset. Here you can see I have ordered the assets by category. The assets needing maximum security, which are chemical storage and the SCIF, have multiple layers of protection. Assets not requiring maximum security, including the COMSEC vault and the media equipment, have fewer layers of protection. The ATM, requiring a basic level of security, has one layer of protection.

Asset	Building #	Category	Protection
Chemical Storage	12	I	Fencing/Lighting IDS/CCTV
Sensitive Compartmented Information Facility (SCIF)	23	I	IDS/Access Control 24-hour security
Communications Security (COMSEC) Vault	54	II	IDS/Access Control
Media Equipment	5	III	IDS/Access Control
Automated Teller Machine (ATM)	5	IV	IDS

Part 4: Access Control Measures

[Mr. Jansen] Part 4 defines and establishes restrictions on access and movement into critical areas. The categories can include personnel, materials, and vehicles. These are some notes I took while reading the NDC example.

First, the NDC example outlines personnel access. It states who has authority to impose control measures and mentions roles of the Commander or Facility Director as well as Agency and Tenant Unit Directors. It also states criteria for different levels of access. For example, unit personnel will have different access than visitors.

Next, the NDC example outlines material control access. It lists controls for various incoming shipments, including commercial, arms, ammunition and explosives (AA&E) chemicals, and hazardous materials. It lists gates of entry and processes for inspection. We also see controls for outgoing materials, including requirements for removal of government property, such as written authorization from the Commander or those delegated for approval.

The NDC example also outlines vehicle control and includes policy on search of government-owned vehicles and privately owned vehicles (POVs). It outlines parking regulations, including the process for issuing and responding to traffic law violations.

It lists controls for government-owned vehicles, POVs, and emergency vehicle entrances into restricted and administrative areas.

[Narrator Tip] As you read the NDC model, think of any equivalent controls you have at your installation and begin to outline them in your own PSP.

Part 5: Physical Security

[Mr. Jansen] Part 5 indicates the manner in which we implement physical security on our installation.

This Physical Security Plan Template from CDSE, is helpful for writing this section. It contains a comprehensive outline of physical security measures and how they will be implemented.

Main topics to consider include:

- protective barriers
- protective lighting systems
- emergency lighting systems
- intrusion detection systems or IDS
- communications
- security forces
- contingency plans
- use of air surveillance
- coordinating instructions

[Narrator Tip] Reference the CDSE Job Aid and the NDC model to help identify all aspects of physical security on your installation and how they are implemented.

Part 6: Annexes

[Mr. Jansen] Part 6 contains annex documents. For operational reasons, these annexes may be separated from the PSP. If they are separated, note their location on the PSP.

You may write or include standard operating procedures, or SOP, listing the purpose, procedures, duties, and responsibilities of security personnel.
You may refer to the annexes in the event of an emergency, such as a bomb threat, natural disaster, or civil disturbance.

The CDSE Job Aid includes an extensive list of annexes and descriptions.

A. References
B. Installation Threat Statement
C. Terrorist Counteraction Plan
D. Bomb Threat Plan
E. Installation Closure Plan
F. Natural Disaster Plan

G. Civil Disturbance Plan
H. Work Stoppage Plan
I. Resource Plan
J. Communication Plan
K. Intrusion Detection Systems (IDS)
L. High Risk Personnel (HRP) Security
M. Motor Pool Security
N. Contingency Plans
O. Post Orders
P. Designated Restricted Areas
Q. Installation Mission Essential or Vulnerable Areas (MEVAs)
R. Maps of the Installation or Facility
S. Continuity of Operations Plan (COOP)
T. Glossary

It is important to note that not every installation or facility will include every annex we see in the Job Aid or in the NDC model.

As we see in the Fort Bravo model, it includes annexes for physical security needs of specific buildings (for example, Gate 1 and Building 1) as well as relevant waivers and approvals.

[Narrator Tip] Remember, the PSP is a living document that is edited or updated as needed. It's the responsibility of the Physical Security Manager to maintain the annexes. When you become aware of any changes, be sure to revisit the PSP and update it accordingly.

Knowledge Check 3

In your role as a Physical Security Manager, how do you identify annexes to include in a PSP?

- Include annexes relevant to the needs of your installation or facility
- Include all memorandums and SOPs you receive from directors and managers
- Choose a list of annexes from a model and develop policies based on the model
- All the above

Conclusion

[Narrator:] During this Short, you identified the importance of each part of the PSP in protecting DOD assets.

You learned from Mr. Jansen that a Physical Security Plan can have six parts:

- Purpose of the Plan
- Responsibilities
- Policies
- Access Control Measures
- Physical Security
- Annexes

Most importantly, a Physical Security Plan must be practical, flexible, and responsive.

Using the resources outlined in this Short, you are ready to contribute to your installation or facility's Physical Security Plan.

Congratulations! You have completed the Parts of a Physical Security Plan Short.

Answer Key

Knowledge Check 1

A Physical Security Plan outlines how a facility or installation will _____ DOD assets.

- hold
- assign
- **protect**
- interpret

Feedback: The Physical Security Plan is the blueprint for protection of DOD assets.

Knowledge Check 2

Part 1 of the PSP outlines the purpose of the document. Based on the Fort Bravo model, what is most important to communicate in this section?

- Needs for emergency responses
- The impact of threats and attacks
- Hazards within a facility or installation
- **The role of defense countermeasures**

Feedback: Part 1 of the PSP tells the purpose of the PSP, which is to communicate the role of defense countermeasures needed to respond to various threats and attacks.

Knowledge Check 3

In your role as a Physical Security Manager, how do you identify annexes to include in a PSP?

- **Include annexes relevant to the needs of your installation or facility**
- Include all memorandums and SOPs you receive from directors and managers
- Choose a list of annexes from a model and develop policies based on the model
- All the above

Feedback: It is important to note that not every installation or facility will include all the annexes you see in models. Include annexes relevant to the needs of your installation or facility.