**Job Aid: Physical Security Plan Template**

# Map Reference Copy No. Issuing Agency

**Place of Issue** **Date of Issue**

**Physical Security Plan**

1. Purpose (also known as the Commanders Intent or Executive Summary). State the plan’s purpose.
2. Responsibilities. List the people who are responsible for physical security and what their specific responsibilities are related to the physical security of the installation or facility.
3. Policies.
	1. Area Security. Define the areas, building, and other structures considered critical and establish priorities for their protection.
	2. **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 I** (maximum-level security) | **BLDG #** | **PROTECTION** |
|  |  |  |
|  |  |  |

**CATEGORY II (Advance 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 II** (advanced-level security) | **BLDG #** | **PROTECTION** |
|  |  |  |
|  |  |  |

**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, intrusion detection system (IDS), closed-circuit television (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 III** (intermediate- level security) | **BLDG #** | **PROTECTION** |
|  |  |  |
|  |  |  |

**CATEGORY IV – X (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 Force Protection Conditions (FPCONs).

|  |  |  |
| --- | --- | --- |
| **CATEGORY IV** (basic-level security) | **BLDG #** | **PROTECTION** |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **CATEGORY V** (basic-level security) | **BLDG #** | **PROTECTION** |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **CATEGORY VI** (basic-level security) | **BLDG #** | **PROTECTION** |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **CATEGORY VI** (basic-level security) | **BLDG #** | **PROTECTION** |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **CATEGORY VII** (basic-level security) | **BLDG #** | **PROTECTION** |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **CATEGORY VIII** (basic-level security) | **BLDG #** | **PROTECTION** |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **CATEGORY IX** (basic-level security) | **BLDG #** | **PROTECTION** |
|  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **CATEGORY X** (basic-level security) | **BLDG #** | **PROTECTION** |
|  |  |  |
|  |  |  |

1. Access Control Measures. Define and establish restrictions on access and movement into critical areas. Categorize restrictions as to personnel, materials, and vehicles.
	1. Personnel access
		1. Establish controls pertinent to each area or structure
			1. Authority for access
			2. Criteria for access
				1. Unit personnel
				2. Visitors
				3. Maintenance personnel
				4. Contractor personnel
				5. National guard
				6. Emergency response teams (police, fire, ambulance, and so forth)
		2. Identification and control
			1. Description of the system to be used in each area. If a badge system is used, a complete description covering all aspects should be used in disseminating requirements for identification and control of personnel conducting business on the installation.
			2. Application of the system:
				1. Unit personnel
				2. Visitors to restricted areas
				3. Visitors to administrative areas
				4. Vendors, tradesman, and so forth
				5. Contractor personnel
				6. Maintenance or support personnel
				7. Fail-safe procedures during power outages
	2. Material control
		1. Incoming
			1. Requirements for admission of material and supplies
			2. Search and inspection of material for possible sabotage hazards
			3. Special controls on delivery of supplies or personal shipments in restricted areas
		2. Outgoing
			1. Documentation required.
			2. Controls
			3. Classified shipment not involving nuclear/chemical material.
		3. Nuclear/chemical material
			1. Controls on movement of warheads/chemicals on the installation.
			2. Controls on shipments or movement of training warheads/chemicals.
			3. Controls on pickup or delivery of warheads/chemicals outside the installation
	3. Vehicle control
		1. Policy on search of military and privately-owned vehicles (POVs). (See component Access Control regulation for search procedures.)
		2. Parking regulations
		3. Controls for entrance into restricted and administrative areas
			1. Military vehicles
			2. Privately Owned Vehicles (POVs)
			3. Emergency vehicles
			4. Vehicle registration
2. Physical security measures. Indicate the manner in which the following physical security measures will be implemented on the installation.
	1. Protective barriers
		1. Definition
		2. Fences
		3. Clear zones
		4. Signs
			1. Types
			2. Posting
		5. Gates
			1. Location in perimeter
			2. Hours of operation
			3. Security requirements
			4. Lock security
			5. Barrier plan for each gate
	2. Protective lighting system
		1. Use and control
		2. Inspection
		3. Action taken in case of commercial power failure
		4. Action taken in case of failure of alternate power source
	3. Emergency lighting system
		1. Stationary
		2. Portable
	4. IDSs
		1. Security classification
		2. Inspection
		3. Use and monitoring
		4. Actions to be taken in case of alarm conditions
		5. Maintenance
		6. Alarm logs or registers
		7. Tamper-proof provisions
		8. Monitor panel locations
	5. Communications
		1. Locations
		2. Use
		3. Tests
		4. Authentication procedures
	6. Security forces. General instructions that would apply to all security force personnel (fixed and mobile). Detailed instructions such as special orders and standard operating procedures (SOPs) information should be attached as annexes. Security force facets include:
		1. Composition and organization of the force.
		2. Tour of duty.
		3. Essential posts and routes.
		4. Weapons and equipment.
		5. Training.
		6. Use of MWD teams.
		7. Method of challenging with signs and countersigns.
		8. Alert forces:
			1. Composition
			2. Mission
			3. Weapons and equipment
			4. Location
			5. Deployment concept
	7. Contingency plans. Required actions in response to various emergency situations. Detailed plans for situations (counterterrorism, bomb threats, hostage negotiations, disaster, fire, and so forth) should be attached as annexes.
		1. Individual actions.
		2. Alert force actions.
		3. Security force actions.
	8. Use of air surveillance.
	9. Coordinating instructions. Matters that require coordination with other military and civil agencies such as:
		1. Adjacent installations or units
		2. State and local agencies
			1. Local county/city police
			2. Sheriff's Office
			3. State Police (Troops A, B, etc.)
		3. Federal Agencies
			1. Federal Bureau of Investigation
			2. U.S. Marshal
			3. U.S. Forestry Service
			4. Drug Enforcement Administration
			5. Immigration and Naturalization Service
		4. Similar host country agencies

NOTE: The coordination/interaction allows for an exchange of intelligence information on security measures being used, contingency plans, and any other information to enhance local security. On an installation, the host activity shall assume responsibility for coordinating physical security efforts of all tenants, regardless of the components represented, as outlined in the support agreements and the host-activity security plan. Applicable provisions shall be included in, or be an appendix to, the support agreement. A formal agreement will contain definite assignment of physical security responsibility for the items stored. The agreement should address:

* Maximum quantities to be stored
* Physical safeguards to be used
* Frequency of and responsibility for physical inventories or reconciliations
* Reporting of losses for investigation
* Lock and key control
* The unit that has overall responsibility

NOTE: Procedures for authorization and identification of individuals to receipt for and physically take custody of XXXX (installation/unit/facility name) property. The purpose of such coordination is protection in depth. Authority, jurisdiction, and responsibility must be set forth in a manner that ensures protection and avoids duplication of effort.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX A, REFERENCES**

This annex provides a list of DOD or Component-specific directives, regulations, instructions, manuals, etc. that apply to the physical security of the installation or facility.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX B, INSTALLATION THREAT STATEMENT**

This annex provides current intelligence pertaining to terrorist, criminal, civil disturbance, and other threats to the security of personnel and property at the installation or facility.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX C, TERRORIST COUNTERACTION PLAN**

This annex provides the immediate response by the local community and installation collectively, in the event of a terrorist attack. This is normally a joint document, which allocates critical resources, and outlines each agency duties and responsibilities. Additionally, routine exercises are performed together for readiness and evaluation.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX D, BOMB THREAT PLAN**

This annex provides a bomb threat plan, including as a minimum, guidance for:

* Control of the operation
* Evacuation
* Search
* Finding the bomb or suspected bomb
* Disposal
* Detonation and damage control
* Control of publicity
* After-action report

CHECKLIST WHEN YOU RECEIVE A BOMB THREAT

Time and Date Reported How Reported Exact Words of Caller Questions to Ask:

1. When is the bomb going to explode? \_
2. Where is the bomb right now?
3. What kind of bomb is it?
4. What does it look like?
5. Why did you place the bomb?
6. From where are you calling?
7. Description of caller’s voice:

Male: \_\_\_ Female: \_\_\_ Young: Middle-Age: Old:\_\_\_\_ Accent:

Tone of voice

Background noise

Is voice familiar ? If so, who did it sound like? Other characteristics

Time caller hung up Remarks

Immediately notify your supervisor, then the police desk sergeant. Keep this list with you.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX E, INSTALLATION CLOSURE PLAN**

This annex addresses an installation closure plan, which identifies contingency road closings and restriction of movement within specific areas of the installation. The inclusion of this annex must be coordinated with local and state law enforcement activities.

NOTE: Typically, the physical security plan (PSP) is coordinated with federal agencies which support the installation. However, signed agreements normally are in the form of Memorandums of Agreement or Understanding.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX F, NATURAL DISASTER PLAN**

This annex is comprised of a natural-disaster plan that has been coordinated with natural disaster plans of local jurisdictions. At a minimum, the natural disaster plan should provide guidance for:

* + Control of the operation
	+ Evacuation
	+ Communications
	+ Control of publicity
	+ An after-action report

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX G, CIVIL DISTURBANCE PLAN**

This annex consists of the civil disturbance plan and is formulated by the commander based on local threats. (For example, commanders of chemical facilities should anticipate the need to develop crowd control procedures to handle anti-chemical demonstrations.)

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX H, WORK-STOPPAGE PLAN**

This annex identifies a work-stoppage plan. This is a requirement for conducting a physical security survey to determine the impact of a decrease in the installation’s work force. A work- stoppage plan includes additional physical security considerations regarding the activity involved (such as modified or alternate staffing considerations) and the area directly surrounding critical infrastructures and critical assets. This annex should include provisions for increased access and entry controls measures if the situation warrants.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX I, RESOURCE PLAN**

This annex addresses a resource plan to meet the minimum essential physical security needs (equipment, money, and personnel, etc.) for the installation or activity.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX J, COMMUNICATION PLAN**

This annex identifies all the specific communication systems or networks used at the installation and the infrastructure to support command and control. Typically, system configurations and geographical location of significant equipment is identified in detail. The communications plan should address all communication requirements such as encryption, line monitoring, shared networks, wireless, cellular, mobile radio, loss of communication, call signs, brevity codes, and routine maintenance actions.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX K, INTRUSION DETECTION SYSTEMS (IDS)**

This annex outlines procedures and policies for the effective and economical operation of government owned Intrusion Detection System (IDS) on the installation. This annex normally includes test and certification plans, maintenance, alarm rates (false/nuisance), emergency contacts, types of sensors, accessing and arming structures.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX L, HIGH RISK PERSONNEL (HRP) SECURITY**

This annex outlines procedures for providing minimal level security for HRP residing and working on the installation or facility and for visiting dignitaries. HRP are those who are more likely to be terrorist or criminal targets because of their grade, assignment, symbolic value, vulnerabilities, location, or specific threat.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX M, MOTOR POOL SECURITY**

This annex outlines how motor pools will be protected including rules for Privately Owned Vehicle (POV) storage, fuel tankers, and contractor vehicles.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX N, CONTINGENCY PLANS**

This annex identifies a contingency plan to be used in situations where the commander determines an increase in physical security measures and procedures are necessary. In most instances, it will be necessary to increase security for arms, ammunition, and explosives (AA&E) and other sensitive property, assets, and facilities during periods of natural disasters, natural emergencies, or increased threat from terrorists or criminal elements. Other contingencies that may require an increase in physical security measures and procedures include hostage negotiations, protective services, and special reaction teams. These provisions should be designed for early detection of an attempted intrusion, theft, or interruption of normal security conditions.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX O, POST ORDERS**

This annex outlines the post orders that establish roles and responsibilities at individual posts at an installation or activity.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX P, DESIGNATED RESTRICTED AREAS**

This annex includes a listing of all designated restricted/controlled areas on the installation or facility.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX Q, INSTALLATION MISSION ESSENTIAL OR VULNERABLE AREAS (MEVAs)**

This annex includes a list of all mission essential vulnerable areas (MEVAs) on the installation or facility.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX R, MAPS OF THE INSTALLATION OR FACILITY**

This annex includes the maps and map keys for the installation or facility.

# Map Reference Copy No. Issuing Headquarters

**Place of Issue Date of Issue**

**ANNEX S, CONTINUITY OF OPERATIONS PLAN (COOP)**

A COOP is a United States federal government initiative, required by U.S. Presidential Policy Directive 40 (PPD-40), to ensure that agencies can continue performance of essential functions under a broad range of circumstances.

It is a collection of resources, actions, procedures, and information that is developed, tested, and held in readiness for use in the event of a major disruption of operations.

The overall purpose of continuity of operations planning is to ensure the continuity of operations are performed efficiently with minimal disruption, especially during an emergency.

The current changing threat environment and recent emergencies, including acts of nature, accidents, technological emergencies, and military or terrorist attack-related incidents, have increased the need for viable continuity of operations capabilities and plans that enable agencies to continue their essential functions across a spectrum of emergencies.

# GLOSSARY

This annex spells out any acronyms used in your physical security plan.