SECURITY PLANNING WORKBOOK RESOURCE GUIDE

Developed by the

ILLINOIS STATE POLICE
Office Of Protective Security

THE SECURITY PLAN

What is a Security Plan? A security plan is similar to other management planning documents, but with a focus on the security and safekeeping of organizational assets. It is similar and complimentary to safety documents such the Continuity of Operations / Continuity of Government (COOP/COG) documents, but it addresses different dimensions. Think of the Security Plan as the guardrail at the top of a large gorge, and a COOP is the ambulance that responds at the bottom after the adverse incident, such as your bus driving over the cliff face. One stresses prevention and preservation, while the other focuses on mitigation and recovery.

PLANNING PROCESS

Every organization of state government should develop and implement a comprehensive, enterprise model security plan to protect its staff, property, visitors, clients and overall assets. The process of security planning is introspective, and is similar to other management planning methods such as the SWOT analysis framework.

This instrument can be used to guide your organization's security planning efforts; security expertise is not required in this phase, but a comprehensive understanding of the organization's operations and assets is a must. It is designed to compile key information that can be used as the ISP consults on building or refining a comprehensive security plan for you.

It is recommended that one individual be designated as a project manager to lead the planning effort. This individual should be at an executive level, and have the authority to direct staff at all levels in the organization during the information gathering process. Additional team members can be added, as appropriate, based on their knowledge of organizational functions, subject matter expertise, and other team-related needs. Other valuable skill sets might include policy development, strategic planning, finance and accounting, and training skillsets.

Within the Security Planning Team, the Team Leader should establish clears roles, responsibilities, and expectations for those directly involved. Additionally, the executive team should establish an expectation of cooperation from all personnel in the organization as it relates to the planning team's information gathering functions.

The objective of the team is to gather critical data that will be used to create the final security plan. The majority of these data points will consist of identified assets that are critical to organizational functions. This includes individual facilities, operationally critical functions, and personnel. In fact, anything that is critical to the fulfilment of organizations mission can be considered a relevant asset.

A common acronym used to describe potential assets is P.I.E.F.A.O., which stands for:

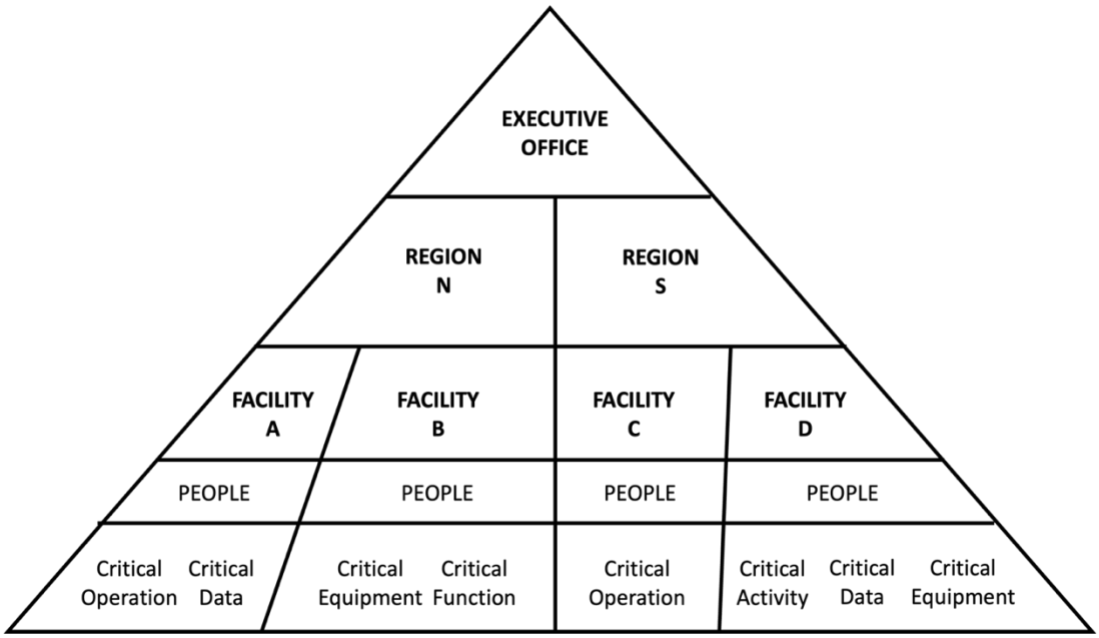
PEOPLE
INFORMATION
EQUIPMENT
FACILITIES
ACTIVITIES
OPERATIONS

While some assets are "stand-alone," many are inter-related. In fact, these "interdependencies" can in themselves constitute an asset (and in some cases a vulnerability).

ENTERPRISE APPROACH TO SECURITY

Assets may be multi-layered, and will generally reside within a "hierarchy." For example, your agency may have ten (10) physical office facilities throughout the state. Some may be stand-alone facilities, and some may by situated within a larger, multi-tenant office building. In addition to the physical offices, your agency may have information data that is sensitive, and may also have a number of functions that are mission critical. This complex, encompassing configuration is termed an *enterprise model*, and all state agencies will conform to this model.

The hierarchy will start with all of the lowest levels, and consolidate upward into higher levels, until it culminates into the executive suite. This is a scalable model that will work for most organizations, whether you have 1 or 30 locations. A simplified, graphic depiction is shown as an example below.



For planning purposes, a master list of all significant, relevant assets will be created by the team. What is defined as significant and relevant is determined by the stakeholder, in consultation with the security advisor. The information will then be organized in a logical, structured format that is arranged to provide a uniform *yet flexible* document. This is important because while there are a number of characteristics common to all agencies of state government, no two organizations are alike. The final document will constitute an agency wide plan that incorporates all applicable assets and will serve as the agency's final *Security Plan*.

ASSET CHARACTERIZATION

To further define assets for purposes of this exercise, the following information may be helpful. As stated above, an asset is anything that is critical to the organization. It could be that the mission of the organization cannot be fulfilled effectively or efficiently if the asset is lost, stolen or otherwise compromised. Additionally, interdependencies are important, such that if one asset is compromised it can affect others in a cascading manner.

Once the asset *criticality* is identified, additional analysis is applied. This includes an assessment of *replaceability*. Is the asset unique, difficult to acquire, or expensive to replace? Clearly, relative expense alone can be a factor to define an asset, as defined by state audit guidelines, statue statute, and agency policies, but replaceability is an additional layer for determination purposes. If the item falls below the threshold cost, but is difficult to replace, then its value increases as an asset.

RISK EQUATION

For the additional analysis, it helpful to understand the "*Risk Equation*." It can be thought of as a mathematical equation, and is graphically represented as:

$$\text{RISK} = \frac{(\text{THREATS} + \text{HAZARDS}) \times \text{VULNERABILITY} \times \text{CONSEQUENCE}}{\text{COUNTERMEASURES}}$$

Risk may also be expressed as a qualitative function, that is high, medium, or low in varying degrees by scale. Another perspective is to view Risk as a frequency-based probability. For purposes of this framework, Risk is generally defined as the relative potential for an "Undesirable Event" with an adverse outcome assessed as a function of threats, hazards, vulnerabilities, and consequences associated with an incident, event, or occurrence. Below are working definitions for the respective components:

Threat: Man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Threats are directed while hazards are not directed.

Hazard: Natural or man-made source or cause of harm or difficulty. A hazard differs from a threat in that a threat is intentionally directed at an entity, asset, system, network, or geographic area, while a hazard is not directed.

Vulnerability: Characteristic of design, physical features, location, security posture, operational attribute, human failure, policy and procedures, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation from a hazard or threat. Generally viewed as weaknesses that can be exploited by adversaries. A generic, non-exhaustive list of vulnerability examples is included in Appendix B.

Consequence: The impact of an adverse event, incident or occurrence, usually measured in direct and indirect terms of the effect on people, economics, mission and psychodynamics, and may include an assessment of frequency.

Countermeasures: Countermeasures are what most individuals visualize when they consider the concept of "security." Countermeasures are the integrated people, procedure, and equipment components of a "Physical Protection System" that are developed and implemented in response to the threats, hazards, and vulnerabilities identified in the security assessment phase that are designed to mitigate an adverse impact resulting from an undesirable event.

Also, it includes the employment of devices or techniques that impair the operational effectiveness of adversary activity, and may include anything that effectively negates an adversary's ability to exploit vulnerabilities. Examples include: policies, procedures (e.g. Emergency Action Plans or EAP) signage, cameras, alarm systems, lighting, guard service, magnetometers, etc.

Undesirable Event: An incident that has an adverse impact on the Asset, operation of the facility, or mission of the agency.

Your team will work to identify these dimensions as a function of your organization and relative to your assets, and the Office of Protective Security will collaborate with your agency to refine and finalize the product.

ADVERSE EVENTS

In order to understand the threat environment relative to your agency's Assets, it will be helpful to understand general and sector specific threats, as well as historical adverse events that could impact your agency.

General threats are identified as something that can impact *any* individual or organization. Examples include general street crime or *crimes of opportunity*. Examples include vehicle burglaries, muggings, simple theft, graffiti, etc. While generally less predictable, these events can be easier to mitigate through basic crime prevention methods.

A “Sector” is defined as a general group of related functions in the critical infrastructure inventory as identified by the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA). For example, all state government functions can be included in the Government Services sector. However, some agencies will also fall into other sectors, such as healthcare and Public Health, Emergency Services, Information Technology, and others.

As a function of the planning process, your project team should research the historic incidents of adverse events related to your agency’s assets, and prepare a summary for assessment purposes. This could be anything from thefts, assaults, unauthorized entry, communicated threats, etc. This can be organized by individual facility, agency-wide, etc. For example, if you have a call center operation and a threatening call is received, it may not affect any one facility, but might be directed at a work function or the agency as a whole. We would recommend a look back period of 20 years minimum.

The Office of Protective Security will work with your Project team to assess those sector specific issues and along with historic data, assist your agency in creating a “threat model” that can be incorporated into your Risk Equation for planning purposes.

CONCLUSION

The Office of Protective Security looks forward to working with your agency to develop your Security Plan and improve your security posture. A general framework of the planning process is included in “Appendix A” which shows the information and data that will need to be gathered in order to go forward with the development of your Security Plan.

APPENDIX A

PLANNING STRUCTURAL FORMAT: Information Gathering

- ☐ Agency Information – Name, Function, "State Government Hierarchy" (executive branch, etc.)
- ☐ Agency Leadership
  - Short narrative of Organization ***Leadership*** Positions
  - Table of Organization (T.O.) (graphic representation)
  - Security Team Narrative and T.O. (authorities and responsibilities)
- ☐ Planning Team Composition
- ☐ Agency Mission (Functions: General to Specific)
- ☐ Mission Critical Operations (any Asset that is critical to the organization's functionality)
  - Mission Critical Functions
  - Other Critical Functions
  - Critical Interdependencies
  - Mission Critical Staff / Personnel Assets
  - Counter-Measures (see note above)
- ☐ Critical Assets (non-Operational)
  - Equipment (Inventory)
  - Counter-Measures
- ☐ General Workforce Security
  - Personnel Hiring Policies (Screening, Vetting, Verification, etc.)
  - Internal security-related investigations
- ☐ Facilities (Inventory of Facilities owned or leased)
  - Characterization and Functions of each
  - Existing Security Features
- ☐ Security Related Contracts – Includes guard services, alarm and camera services, parking lot towing services, etc.

- Training and Drills
  - Security-Related Training Conducted
    - Training to Policies and EAP
    - DOIT Cyber Security
    - Civilian Response to Active Threat
  - Security-Related Drills Conducted
    - Active Threat Drills

Appendix B

TABLE OF HAZARDS, THREATS, VULNERABILITIES AND COUNTER-MEASURES

Risk = [(Hazard + Threat) * Vulnerability * Consequence) / Countermeasures]

HAZARDS

Accident
Fire
Flood
Earthquake
External Impact
Extreme Cold/Heat
Hazmat (Internal, External, etc.)
Hurricane\Monsoon
Nuclear
Snow / Blizzard
Tornado / Wind / Hail

THREATS

Arson
Assault
Biological
Burglary
Civil Disturbance
Chemical
Coordinated Attack
Cyber Attack
Espionage
Explosive (IED, VBIED, etc.)
External Impact
HIPPA / PHI violation
Identity Theft
Insider Threat (Sabotage, Theft, etc.)
Kidnapping
Mob Action
Nuclear
Radiological
Robbery
Sabotage
Significant Disorderly / Disruption
Standoff / Ballistics / Sniping
Hostile Surveillance / Electronic Intercept
Unauthorized Entry (Trespass)
Forced or Surreptitious
Vandalism
Workplace Violence

VULNERABILITIES

Critical Assets
Critical Functions
Data / PHI / Personally Identifiable Information
Doors
External Factors
Hostile Surveillance Points
Interdependencies / Utilities
Other Life Safety
Other Operations
Parking lots
Policy (lacking, inadequate, fail to follow, etc.)
Shipping / Receiving / Mailroom / Warehouse
Supply Chain / Logistics
Waiting Areas
Windows

COUNTER-MEASURES

Access Control / Access Control Systems
Background Checks / Vetting
Barriers / Fencing
Buffer zones
Cameras and Recording
Counter Surveillance
CPTED
Doors, Locks, and Key Control
Environmental Shaping
Intrusion Detection System (IDS)
Layered Security
Lighting
Mail & Package control
Natural Terrain and layout
Policy and Procedure
Proximities / Buffer Zones
Safes, Vaults and Other Storage
Screening (Magnetometer, X-ray, Package)
Security force / Presence / Response
Signage
Training / Awareness / Reinforcement
Windows

VULNERABILITY SUB-CLASSIFICATIONS

Vulnerability by Function

Administration
Audio/visual
Badging / Credentials
Data-Warehouse
Daycare
Dispatch
Distribution
Engineering
First-Aid
Food Service / Lunchroom
Food Storage
Hearing rooms
High Value Storage
Housing
Housekeeping
HVAC
Kitchen
Laundry
Locker rooms
Mail / Messenger / Delivery
Main Entrance
Medical
MIS
Parking Lot / Garage
Phone room
Playground / Recreation
Receiving / Shipping
Reception
Records (Paper files, Other)
Refuse / Trash
Retail POS
School
Security
Service Entrance
Surrounding Environment
Telecom
Training Room / Center
Warehouse