Chapter 2

Asset Identification and Security Inventory

In this chapter . . .

- Definitions
- Asset Classification
- Identifying Critical Assets
- Target Selection
- Consequence Analysis
- Countermeasure Inventory
- Security Assessments

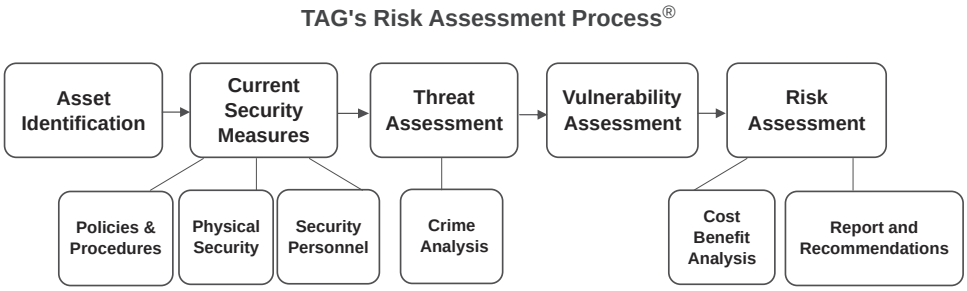

Figure 2-1.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

All security programs, regardless of their complexity or industry application, are designed to protect assets, and generally speaking, assets are anything of value. This chapter introduces the concepts of asset identification, determination of criticality, and consequence analysis. Also discussed is how assets are

selected by adversaries, those that seek to damage, destroy, or steal assets. Properly determining what is in need of protection is a necessary first step in the risk management process, for without asset identification, security measures are often haphazardly selected and deployed. This chapter also introduces more complex concepts that will be discussed in the remainder of the book. Thus, the first part of this chapter contains a list of terms and their definitions used throughout the book to ensure a commonality in understanding.

DEFINITIONS

Adversary—An individual or group that is motivated and capable of stealing, damaging, or destroying critical assets. Adversaries are threats. They can include insiders, outsiders, or a combination of insiders and outsiders.

Asset—People, property, and information. People may include employees and customers along with other invited persons such as contractors or guests. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.

Capability—The ability of an adversary to obtain, damage, or destroy an asset.

Consequence—The extent of loss that can be anticipated from a successful adversarial attack against an asset. The impact of loss may be human, economic, political, environmental, or operational; however, consequences should be stated in financial terms if possible.

Continuity of Operations (COOP)—A concept that seeks to ensure that an organization's essential functions and mission-critical operations can be performed.

Cost-Benefit Analysis—An assessment conducted during the countermeasure selection phase of the costs and benefits of each security measure option. Costs typically include the money and time resources required to implement the measure and any ongoing time and money needed to maintain the measure. Benefits are security program improvements derived from planned security measures.

Countermeasures—Security measures that include policies and procedures, physical security equipment and protection systems, and security personnel. The primary purpose of a countermeasure is to mitigate risk through a prevention process that eliminates or neutralizes threats and reduces vulnerabilities. The term *countermeasures* is used interchangeably with security measures.

Crime Analysis—The logical examination of crimes that have penetrated preventive measures, including the frequency of specific crimes, each incident's temporal details (time and day), and the risk posed to a property's inhabitants,

as well as the application of revised security standards and preventive measures that, if adhered to and monitored, can be the panacea for a given crime dilemma.

Criticality—The operational impact to the organization's mission due to the loss, damage, or destruction to an asset.

Defeat—A security strategy designed to neutralize adversaries before an asset is lost, damaged, or destroyed. For defeat to occur, the security program must be operating at an optimum level.

Delay—A security strategy designed to slow the progression of adversaries into or out of the facility. Barriers are an example of a delay measure.

Detection—A security strategy designed to assess the threat and to alert security personnel of an adversary's presence. Cameras and sensors are examples of detection measures.

Deterrence—A security strategy designed to discourage adversaries by increasing the risks to the adversary, promoting a sense of security, and instilling doubt on behalf of an adversary. Uniformed security personnel and lighting are examples of deterrence measures.

Emergency—Any event or combination of events that have the potential to negatively impact the organization's mission or components of that mission for a period of time and that require immediate response and action to continue normal mission operations.

Exposure—An instance of being exposed to losses from a threat. A weakness or vulnerability can cause an organization to be exposed to possible damages.

Facility—A structure or group of structures in one physical location.

Hybrid Assessment—A type of assessment that includes both qualitative and quantitative data and components. Typically, hybrid assessments numerically measure that which can be measured, such as response times, and assess qualitatively that which cannot.

Infrastructure—The underlying foundation of assets needed for an organization to perform its essential functions and mission-critical operations.

Mitigation—The act of causing a consequence to have less adverse impact on the organization's mission.

Project Management—The planning and execution of all aspects of a security project and application of skills, knowledge, and methods to achieve the project's objectives, goals, and requirements on time, within budgetary limitations, and with a high level of quality.

Qualitative Assessment—A type of assessment that is driven primarily by the assessment subject's characteristics. Qualitative risk assessments are dependent upon the assessor's skills. Scenario-based risk assessments are typically qualitative in nature. The National Terror Alert System is an example of a qualitative threat assessment.

Quantitative Assessment—A type of assessment that is metric based and that assigns numeric values to the risk level. For example, quantitative assessments incorporate security response times and barrier delay times.

Risk—A function of threats and vulnerabilities. Risk is the possibility of asset loss, damage, or destruction as a result of a threat exploiting a specific vulnerability.

Risk Assessment—The process of identifying and prioritizing risks. A quantitative, qualitative, or hybrid assessment that seeks to determine the likelihood that an adversary will successfully exploit a vulnerability and the resulting impact (degree of consequence) to an asset. A risk assessment is the foundation for prioritizing risks in order to effectively implement countermeasures.

Risk Management—A process that seeks to manage threats, vulnerabilities, and risks within an organization. Risk management involves assessing risk, evaluating and selecting security measures to reduce identified risks, and implementing and monitoring the selected measures to ensure that the measures are effective in reducing risk to an acceptable level.

Security Decision Maker—Anyone who has an active role within an organization for asset protection. This term, or its acronym, SDM, is used throughout this text since some organizations do not have a formal position of security manager or security director. Risk managers also fall within the security decision maker definition.

Security Survey—A fact-finding process whereby the assessment team gathers data that reflects the who, what, how, where, when, and why of an organization's existing operation and facility. The purpose of a security survey is to identify and measure the vulnerabilities to the facility or to specific assets by determining what opportunities exist to exploit current security policies and procedures, physical security equipment, and security personnel.

Threat—Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. Threats are classified as either human or natural. Threat can also be defined as an adversary's intent, motivation, and capability to attack assets.

Threat Assessment—An evaluation of human actions or natural events that can adversely affect business operations and specific assets. Historical information is a primary source for threat assessments, including past criminal and terrorist events. Crime analysis is a quantitative example of a threat assessment, while terrorism threat analysis is normally qualitative.

Vulnerability—Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. Vulnerabilities include structural, procedural, electronic, human, and other elements that provide opportunities to attack assets.

Vulnerability Assessment—An analysis of security weaknesses and opportunities for adversarial exploitation. A security survey is the fundamental tool for collecting information used in the vulnerability assessment. A vulnerability assessment is sometimes referred to as a security vulnerability assessment, or SVA for short.

Asset Classification

What is an asset? Assets are anything of value to an organization, and they range from the basic to the mission critical. It is the mission-critical aspect that is of primary importance for protection by the security program. Generally, assets consist of people, property, and information. Critical assets are those that are needed for the organization to execute its primary missions and functions.

People

People assets may include employees and customers along with other invited persons such as contractors or guests. At a typical chemical facility, on one hand, the employees and contractors are the people in need of protection from various threats, including chemical leaks and explosions to natural disasters. On the other hand, at a hotel, the employees and guests are considered assets, for without the employees the hotel will not operate and without guests, the hotel does not serve its intended purpose.

Property

An organization's property assets consist of both tangible and intangible items that can be assigned a value. Tangible assets are usually simple to identify, whereas intangible assets are more difficult to identify and assign a value. Intangible assets include the organization's reputation and proprietary information. While all property assets have value, not all are critical to the organization's mission.

Information

Among other things and dependent upon the type of organization, information assets may include databases, software code, and company financial records. Proprietary information, such as vital records, formulas, and methods, are also assets. Vital company records normally do not exceed 2 percent of an organization's records and may include incorporation certificates, stock records, corporate meeting minutes, and some financial records.

Critical Assets

Identifying the organization's critical assets is the first step in risk management. Critical assets within industrialized nations include electrical power, gas and oil production, telecommunications, banking and finance, water supply systems, transportation, government operations, and emergency services. Business-critical assets are those that are needed to perform the primary mission of the business. Assets are deemed critical based on two primary factors:

the value as defined by the organization and the short-term and long-term consequence to the business operations due to its loss, damage, or destruction. The critical assets of a business are those that are necessary for continued business operations and in need of protection. For governments, critical assets are those that sustain the economy, security, political landscape, and social services. Assets do not have equal value to the business operation. Whatever the critical assets of any organization, a value must be assessed for each and each asset must be prioritized based on the consequence of its loss due to human actions. For example, in the oil industry, pipelines are considered a critical asset as any damage or loss of a pipeline reduces the availability for refineries to continue production. For small professional service firms, computer files containing company information and client data may be the only critical asset.

Protecting assets is the principal goal of any security program. These assets have both tangible and intangible value whose value can often be quantitatively assessed using the following elements:

1. Criticality of the asset to business operations
2. Replacement value
3. Relative value of the asset

Criticality is a function of the operational impact to the organization's mission due to the loss, damage, or destruction of an asset. The more impact asset has on the business operation, the more critical it is. The criteria for assessing the level of criticality should be specific. Does an asset affect companywide operations, or would the loss, damage, or destruction impact only a portion of the operations? In the oil example, it was determined that pipelines are critical assets; however, pipelines vary in their value for oil and gas production. Some pipelines are more significant because of their throughput, whereas others are less valuable.

Assets are categorized by their level of criticality. This may be a quantitative assessment based on their actual value, or the impact on business operations from their loss, damage, or destruction. Numerically assigned criticality levels can be more difficult to ascertain but can be meaningful to the overall risk assessment. Alternatively, qualitative assessments can also be used by rank ordering the assets on relative scales such as high, medium, or low. Descriptive values such as catastrophic, critical, marginal, or negligible may also be used in understanding the relative value to business operations. A matrix of critical assets may be beneficial in understanding the relative nature of asset loss, damage, and destruction.

For effective business continuity planning, security decision makers should not only consider the immediate impact of asset loss, but also the time and cost to replace the asset. Time to replacement can significantly impact the criticality level due to operational downtime, which in turn leads to loss of revenue. The longer the time necessary to replace a critical asset, the higher the conse-

quence. For some critical assets, it is imperative to have a fully operational backup in place. Take, for example, a professional services firm whose primary deliverables to clients are reports and other data files. The reports and data files are generated on a computer word processing application. Should the firm's computer be destroyed, reports cannot be generated and a substantial loss of revenue can result. Most small firms such as the one described could either have a backup personal computer, or their client files should be stored on a storage device, such as a compact disc or flash drive, and a location where they can use another computer. The loss of one asset may affect other assets as well and should be considered in identifying the overall asset criticality analysis. For example, in preparing for natural disasters, hospitals use electrical generators to provide a backup source of power in the event of a loss of electricity to provide continued support to patients.

Identifying Critical Assets

Asset information can come from various sources; however, critical asset information is best obtained for those who manage the day-to-day operations of the organization. This may be the asset owners themselves or operations managers. Comprehensive interviews of these people should be conducted to obtain the information regarding each asset. Often, a consultant is brought in to conduct a risk assessment. Interviewing key personnel is the first step that the consultant will take, guiding the interviewee through a series of questions that will allow the consultant to fully understand the process and procedures of the organization. For example, a consultant hired by a manufacturing company would start the project with a series of interviews with site personnel, review security manuals and other documentation, and seek out other sources of information to assist in ranking assets based on their mission criticality. Depending on the organization's mission, asset information may be available via the Internet and other public sources. Property management companies, for example, often list their entire portfolios on their website. From a marketing perspective this makes sense; it can be used by adversaries by helping them select a target.

Target Selection

From the adversarial perspective, assets are called targets. Targets may not be of the same value to the adversary as they are to the owner. As such, asset value must be based not only on its mission-critical level, but also on its value to the adversary. Target value must be calculated based on the best available information. For example, from a national security perspective, certainly the Pentagon and U.S. Capitol building are of higher value to the U.S. government than the World Trade Center was. A foreign government would certainly place a high value on the Pentagon when waging a war against the United States.

However, for terrorist groups such as al-Qaeda, the World Trade Center presented a far more attractive target because of its social, economic, and political value. Depending on the industry for which a risk assessment is being performed, certain factors should be considered in evaluating target values:

- Casualty and injury rates
- Asset potential for loss, damage, or destruction
- Damage to the political landscape
- Disruption to operations
- Disruption to the economy
- Media attention
- Impact on the organization's reputation
- Impact to employees' morale
- Fear

Depending on the nature of a company's business, asset value may not be obvious to security decision makers. Threat assessments can help discern which assets are susceptible to loss, damage, or destruction. In the grocery business, for example, criminals target small, high-value items such as infant formula and over-the-counter medicines. For U.S. national security purposes, particularly for the prevention of terrorism, political and economic assets are more likely to be targeted. With recent and realistic threat information, security professionals can make decisions based on asset attractiveness and provide for higher security levels.

Consequence Analysis

History indicates that the likelihood of crime and terrorism, as well as other threats, is inversely related to its magnitude. That is, the probability of attack decreases as consequence increases since it is easier to conduct small-scale attacks than large-scale ones. The recent history of al-Qaeda reflects this type of consequence analysis in that this organization executed a number of relatively low level attacks prior to and since the September 11 attacks, a large scale, high consequence attack.

> ***We have to get it right every day and the terrorists only have to get it right once. So we have to be ahead of the game.***
>
> ***—TSA Spokeswoman Lauren Stover***

Consequence analysis is an assessment of the effect on operations if an asset is lost, damaged, or destroyed. Operations may include business operations or national defense. Business continuity planning is based on consequence analysis. By estimating the likelihood and magnitude of asset loss, security decision

makers can prepare alternative methods to continue operations and restoration of primary operations capability. Organizations need to be prepared for a wide range of attacks based on statistical probabilities of occurrence. A consequence analysis allows the assessment team to prioritize assets in need of protection given their criticality to the organization. Consequence analysis is a fundamental step in the risk assessment process since the organization may not be able to afford the same level of protection for all vulnerable assets; thus, prioritizing assets allows the organization to protect those that are most critical.

Consequences can be categorized in a number of ways: economic; financial; environmental; health and safety; technological; operational; and time. For example, a process control center may be essential for the safe production of a particular product. Its loss, or inability to function properly, could result not only in a disruption of production (with its concomitant loss of revenue and additional costs associated with replacing the lost capability), but it might also result in the loss of life, property damage, or environmental damage, if the process being controlled involves hazardous materials. The loss of an asset might also reduce a company's competitive advantage, not only because of the financial costs associated with its loss, but also because of the loss of technological advantage or loss of unique knowledge or information that would be difficult to replace or reproduce. Individual firms, too, have to worry about loss of reputation. The American Petroleum Institute and the National Petrochemical and Refiners Association (API/NPRA) in their Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries also suggested considering the possibility of "excessive media exposure and resulting public hysteria that may affect people that may be far removed from the actual event location.

A criticality assessment is a process designed to systematically identify and evaluate important assets and infrastructure in terms of various factors, such as the mission and significance of a target. For example, nuclear power plants, key bridges, and major computer networks might be identified as "critical" in terms of their importance to national security, economic activity, and public safety. In addition, facilities might be critical at certain times but not at others. For example, large sports stadiums, shopping malls, or office towers when in use by large numbers of people may represent an important target but are less important when they are empty. Criticality assessments are important because they provide a basis for identifying which assets and structures are relatively more important to protect from an attack. The assessments provide information to prioritize assets and allocate resources to special protective actions. These assessments have considered such factors as the importance of a structure to accomplish a mission, the ability to reconstitute this capability, and the potential cost to repair or replace the asset. Thus far, what has been discussed is a quantitative assessment of assets using actual costs, replacement values, and operational downtime. Criticality can be measured qualitatively also using

relative terms to prioritize asset loss, damage, or destruction. A four-level scale is suggested ranging from low to critical.

Critical—Assets that, if lost, damaged, or destroyed, can result in mission failure

High—Serious unwanted impact that may impair normal operations in their entirety or complete loss of a portion of the operations for an extended time period

Medium—Moderate operational impact that may only affect a portion of the business processes and for a short period of time

Low—A manageable impact to business operations and no likelihood of mission failure

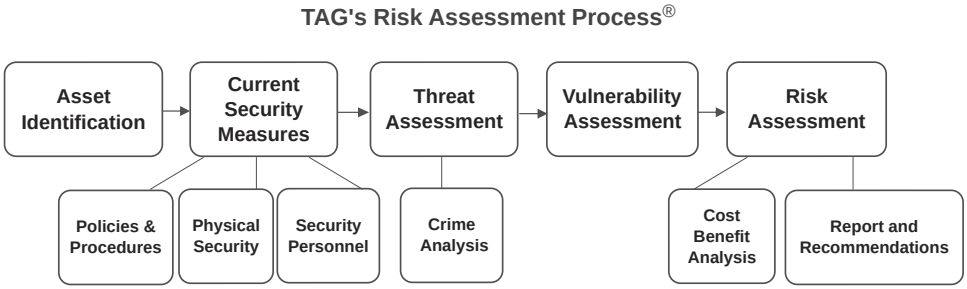

Figure 2-2.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

Countermeasure Inventory

Asset identification is just the first step in the risk assessment methodology. The second step involves inventorying existing security measures designed to protect the assets at the facility. Depending on the quality of previous assessments, existing countermeasures may or may not be effective in protecting the facility and its critical assets. While time brings change to both the assets and the countermeasures, previous risk assessments and subsequent security program designs should be working to protect assets.

Existing countermeasures may include security personnel, physical measures, and policies and procedures. Security personnel include people specifically designated or indirectly working toward the protection of assets. Uniformed security officers would be the most visible and recognizable example of security personnel. Others who may also be involved in the protection are not as easily identified, including undercover officers, security managers dressed in business attire, and common employees trained in how to handle security incidents. Physical security measures may range from low-

technology items such as barriers and curbing to high-tech measures such as closed circuit television (CCTV) cameras, biometrics, and fencing. Physical security measures may also include items not visible to the naked or untrained eye, such as pressure mats and alarm sensors. Policies and procedures are written documents and unwritten rules that relate directly to asset protection and guide the security program. Security manuals and security post orders are examples of policies and procedures.

One of the best sources of information regarding current security measures at a facility is the security officer who is trained in observation and awareness and spends much of his or her time simply observing. Other sources may include the security manager or the officer's direct supervisor. Security manuals, if updated, can also provide invaluable information regarding the security program.

Controlling the capability and motivation of adversaries is a difficult proposition for security decision makers. Motivation is created by the actual crime target and is considered the reason for security breaches. Since organizations usually require assets to operate, the removal of motivation is not always possible. Most organizations must instead turn their attention to blocking the opportunity of crime. As seen in Figure 2-3, reducing vulnerabilities for security breaches leads to a reduction in incidents. Thus, the security decision maker's strategic goal of countermeasure deployment is to reduce the opportunity for security breaches to occur by reducing vulnerabilities. Opportunities relate to targets in that removing or hardening an asset will lead to a reduction or an elimination of vulnerabilities. Asset protection programs integrate a combination of policies and procedures, physical countermeasures, and

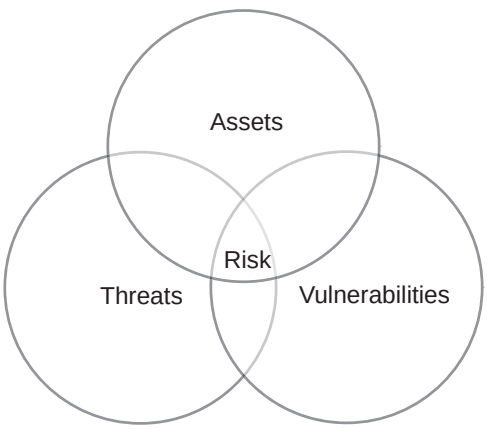

Figure 2-3.
Venn Diagram—assets, threats, and vulnerabilities.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

security personnel to protect assets against a design-basis threat. The characteristics of asset protection programs include deterrence, detection, delay, and defeat.

Typical security measures of a comprehensive security program include security policies and procedures, physical security measures, and security personnel. These security measures are inventoried during the risk assessment and are categorized into key areas as described in the following.

Security Policies and Procedures

- Security Management Plan
- Emergency Management Plan
- Workplace Violence Prevention
- Crisis intervention
- Vital Records Protection
- Key Control Policy
- Visitor Management
- Security Escort
- Physical Security System Testing
- Security Force Deployment
- Fire Prevention and Response
- Bomb Threat
- Access Control
- Employment Background Investigations

Physical Security Equipment

Alarm Systems

- Control Panels/Communicators and Keypads
- Door and Window Contacts
- Motion Sensors
- Glass break detectors
- Object Detectors
- Miscellaneous Detectors
- Duress Alarms

CCTV Systems

- Cameras
- Monitors

- Recording
- IP Video
- Intelligent Video

Access Control Systems

- Stand-alone Devices
- System Controllers
- Readers
- Locking Devices
- Egress Devices
- Door Hardware

Perimeter Security Systems

- Fencing
- Gates
- Bollards
- Locks
- Lighting
- Fire Systems

Specialized Protection Systems

- Metal and Explosive Detectors
- Ballistic-Resistant Materials

Security Personnel

- Proprietary Security Force
- Contractual Security Force
- Off-Duty Law Enforcement Officers
- Other personnel who serve in a protection capacity

Security Assessments

The remaining steps of a risk assessment involve various evaluations designed to analyze threats, vulnerabilities, and overall risks and a suggested course of remediation. Each step is a systematic approach to determining the actual risk posed to the assets, specifically those that are mission critical. As discussed in Chapter 1, there are three types of security assessments: vulnerability, threat, and risk assessments. The final step of the risk assessment is to

evaluate the costs and benefits of remedial measures, including redeployment of resources to protect higher risk areas or assets. This step often provides the greatest heartache to security decision makers because it often involves reducing security to one asset and redeploying those resources to protect more critical assets or at-risk assets. While the heartache is justified, the task is possible. It is possible. It is reasonable. It is defendable. In a nutshell, the risk assessment is designed to provide a continuous process of identifying critical assets and threats to those assets, and reducing any vulnerabilities by careful analysis and implementation of effective countermeasures to achieve an optimum level of protection.

Security assessments are very specific to the type of organization or facility being assessed. Similarly, the methodology used must also be specific to the organization or industry. An assessment methodology designed for chemical facilities will not be useful for a university campus. If an industry-specific methodology is used, it should clearly identify the type of facility for which it is designed and any limitations. Security assessment methodologies are also designed to address certain security arenas. Currently, the division is twofold: physical security and information technology security. Although the gap is closing through the process of convergence, the two fields still stand alone and require different methodologies.

Regardless of the type of organization or whether the assessment is related to physical security or to information technology security, the assessment should state what critical assets require protection, what type of information is needed for each asset, and how the asset's loss, damage, or destruction would impact the mission of the organization. The assessment should also include a threat assessment, vulnerability assessment, and risk assessment that allow security decision makers to prioritize asset protection protocols. Finally, the assessment should make specific recommendations as to how to block opportunities for adversaries to attack and how to protect specific assets.

Once the risk assessment has been completed, certain assets may have a high critical rating, but a lower security level may be required for the overall facility. A typical qualitative approach to facility security levels is as follows:

Security Level 1

Minimum Security

A system designed to impede some unauthorized external activity.

Security Level 2

Low-Level Security

A system designed to impede and detect some unauthorized external activity.

Security Level 3

Medium Security

A system designed to impede, detect, and assess most unauthorized external activity and some unauthorized internal activity.

Security Level 4

High Security

A system designed to impede, detect, and assess most unauthorized activity.

Security Level 5

Maximum Security

A system designed to impede, detect, assess, and neutralize all unauthorized activity.

This page intentionally left blank