CHEMLOCK

Secure Your Chemicals

November 2021

CHEM LOCK

Know your chemicals.
Lock in your security posture.

Cybersecurity and Infrastructure Security Agency

Table of Contents

Acronym List iv

Executive Summary 1

Security Goals 1

Developing a Facility Security Plan 2

1 Risk Management 4

Risk Defined 4

Risk Management 5

2 Security Concepts 8

Necessity for Security 8

Security-in-Depth 8

Implementing Security-in-Depth 10

Security Goals 10

3 Detection 12

Intrusion Detection System (IDS) 12

Camera System 13

Employees or On-Site Security Personnel 14

Security Lighting 15

Inventory Controls 15

4 Delay 18

Perimeter and Asset Barriers 18

Physical Locking Mechanism 19

Access Control 20

Inspections and Screenings 20

Shipping and Receiving Procedures and a Know-Your-Customer Program 21

5 Response 23

Emergency Response Procedures and Crisis Management Plans 23

Outreach Programs 24

Security Plans for Elevated Threats 24

6 Cyber 27

Cybersecurity Policies and Procedures 27
Access Control and Password Management 28
Cybersecurity Training 29
Cybersecurity Controls, Monitoring, Response, and Reporting 29
Disaster Recovery and Business Continuity 30
7 Policies, Plans, and Procedures 32
Maintenance, Inspection, and Testing of Security Equipment 32
Security Awareness and Training Program 33
Background Check on Personnel 33
Insider Threat Program 34
Visitor Escort Policy 36
Processes for Incident Reporting and Investigations 37
Officials, Organization, and Records 37
8 Facility Security Plan 40
Chemical Facility Security Plan Template 41
Revisions 42
Contact Information 43
Facility Contact Information 43
Other Contact Information 43
Critical Asset Identification 44
Directions 44
Critical Assets 44
Notes 44
Detection 45
Directions 45
Notes 45
Detection Security Measures 46
Additional Security Measures 49
Delay 50
Directions 50
Notes 50
Delay Security Measures 51
Additional Security Measures 54

Response 55
Directions 55
Notes 56
Response Security Measures 56
Additional Security Measures 58
Cyber 59
Directions 59
Notes 59
Cyber Assets...60
Cybersecurity Measures..60
Additional Security Measures 63
Policies, Plans, and Procedures 64
Directions 64
Notes 64
Policies, Plans, and Procedures to Implement Security Measures....................................65
Additional Security Measures 68

Acronym List

ACS	Access Control System
CFATS	Chemical Facility Anti-Terrorism Standards
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of operations
DCS	Distributed Control System
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FSO	Facility Security Officer
GPS	Glocal Positioning System
ICS	Industrial Control System
IDS	Intrusion detection system
IP	Internet protocol
IPS	Intrusion Prevention System
IR	Infrared
IT	Information technology
LEPC	Local Emergency Planning Committee
NTAS	National Terrorism Advisory System
OT	Operational technology
PII	Personal identifiable information
PCS	Process Control Systems
PTZ	Pan-tilt-zoom
RMP	Risk Management Plan
SATP	Security awareness and training program
SCADA	Supervisory Control and Data Acquisition
UAS	Unmanned aircraft system
VBIED	Vehicle-borne improvised explosive device
WMD	Weapons of Mass Destruction

Executive Summary

Protecting Your Investment, Safeguarding Your Community

More than 96% of all manufactured goods depend on chemicals in some way, and these chemicals that are used, manufactured, stored, and transported across global supply chains are the bedrock of industries that touch nearly every aspect of American life—from microchips to food processing. Many of these chemicals that businesses interact with every day are dangerous chemicals that could be used in a terrorist attack.

CHEM LOCK

Know your chemicals.
Lock in your security posture.

Whether a small business or an international company, everyone who interacts with these chemicals has a role to play in understanding the risk and taking collective action to prevent chemicals being weaponized by terrorists. The Cybersecurity and Infrastructure Security Agency's (CISA) ChemLock program is a completely voluntary program that provides facilities that possess dangerous chemicals free services and tools to help them better understand the risks they face and improve their chemical security posture in a way that works for their business model. To learn more, visit the ChemLock webpage.

Whether upstream or downstream, small or large, the security measures recommended throughout this document are designed to present a flexible, holistic approach that can be tailored to the unique circumstances and security challenges of any facility, regardless of the type of dangerous chemicals on-site.

Security Goals

There are many different threats or hazards that may threaten your facility, and the probability that a specific one will impact your business is hard to determine. Thus, it is important to consider many different threats and hazards and the likelihood they will occur.

> **Since each facility that possesses dangerous chemicals faces different security challenges, facilities will benefit most from a flexible, holistic approach that can address their unique security challenges.**

To help facilities apply a comprehensive approach to security that can address different threats and hazards, "Part 1: Security Goals" presents five security goals for facilities to think through as they formulate a facility security plan:

1. Can you **DETECT** an attack or suspicious activity?
2. Can you **DELAY** the adversary?

3. Are you able to **RESPOND** in a timely manner?
4. Are you protecting your **CYBER** assets?
5. Do you have the appropriate **POLICIES, PLANS, and PROCEDURES** to implement your plan?

By considering a variety of potential avenues of attack and approaching security from this integrated approach, facilities can choose cost-effective, efficient security measures that work best to protect the dangerous chemicals at their facility from the threats and hazards most likely to occur at their facility.

In addition, because each facility will have a different perspective on the security measures that will work best for them, the security posture of every facility will differ. Thus, developing a facility security plan using a goal-oriented approach instead of a prescriptive approach also means that each facility's suite of security measures presents a new and unique challenge for an adversary to overcome.

Developing a Facility Security Plan

Understanding security principles is valuable, but without a facility security plan that implements specific security measures to meet those security principles, facilities may be unnecessarily exposing themselves to risk. Using the security goals and principles from "Part 1: Security Goals," and "Part 2: Facility Security Plan" provides a draft facility security plan that any facility can use to develop their own facility security plan.

CISA encourages facilities with dangerous chemicals to use this facility security plan template to develop a holistic, customized, site-specific security plan that mitigates risk and ensures chemical security at your facility.

The development of a facility security plan serves as a management tool to guide a facility's security and response efforts, and could be used as an addendum to a Crisis Management Plan or mandated Environmental Protection Agency (EPA) Risk Management Plan (RMP) (if applicable) or other local security mandates.

> **While the security principles contained in this document are focused on an intentional attack by an adversary, they can also be used to develop a risk-based, all-hazards plan.**

Part 1: Security Goals

1 Risk Management

Risk Defined

Risk management is making informed decisions after a thorough review of anticipated threats, vulnerabilities, and associated consequences.

Specific definitions of risk vary from one field or organization to another and from one context to another. CISA defines risk as the potential for an unwanted outcome resulting from an incident, event, or occurrence as determined by its likelihood and the associated consequences. CISA encourages critical infrastructure partners to assess risk for various scenarios and as a product of threat, vulnerability, and consequence. While the risk management approached below is focused on the risk of an intentional hazard by an adversary—such as theft of a chemical, cyberattack, employee sabotage, or theft of intellectual property—they can also be used to develop a risk-based, all-hazards plan.

Critical Asset Identification: When developing a security strategy, the first step is to identify and understand what you need to protect—your critical assets. In the chemical security realm, this means those assets that are dangerous in nature, including the inherent dangers of various chemicals, their storage and process locations, and the security or safety systems and elements that protect them.

Threat: Threats can be anything—whether in nature or caused by man—that has the potential to harm life, information, operations, the environment, and/or property. From a chemical security perspective, the primary threat of concern is an intentional, malicious act by an adversary.

When calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack being attempted by an adversary. In the case of terrorist or other malicious attacks, the likelihood of the threat is based on the intent and capability of the adversary (i.e., Does someone want to attack your facility? Does someone have the resources, tools, and skills to attack your facility?). For other hazards, threat is generally estimated as the likelihood that a hazard will occur (i.e., How often will a tornado or severe storm impact your facility?).

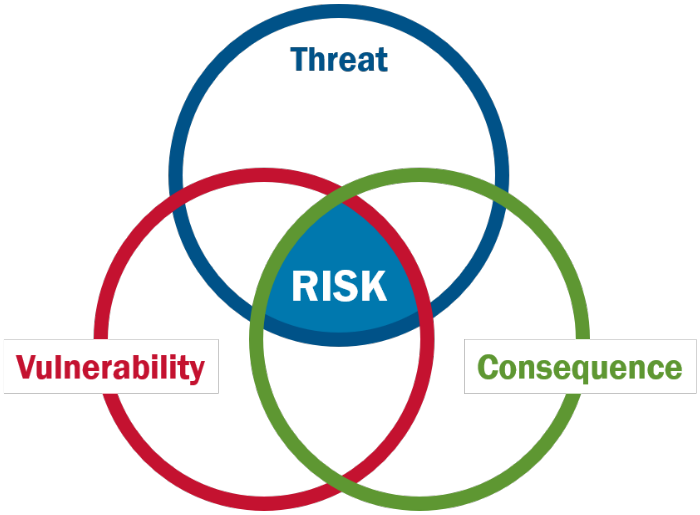

Figure 1. Risk is assessed for each critical asset as a function of threat, vulnerability, and consequence.

Vulnerability: Vulnerabilities include physical features or operational attributes that render an entity open to exploitation or susceptible to a given threat or hazard. In calculating the risk of an intentional hazard, a common measure of vulnerability is the likelihood that an attempted attack is successful.

Consequence: Consequence is the effect of an event, incident, or occurrence and reflects the level, duration, and nature of the loss resulting from the incident. Analysis of consequences may include the following categories:

- **Public health and safety:** Effect on human life and physical well-being (e.g., fatalities, injuries/illness)
- **Economic:** Direct and indirect economic losses (e.g., cost to rebuild asset, cost to respond to and recover from adverse events, downstream costs resulting from disruption of product or service, long-term costs due to environmental damage)
- **Psychological:** Effect on morale and confidence (encompasses those changes in perceptions emerging after an adverse event that affect the sense of safety and well-being and can manifest in aberrant behavior)
- **Mission:** Effect on the ability of the chemical sector to maintain order and deliver goods and services

For facilities that possess dangerous chemicals, this applies to the specific consequences of the chemical. For example, propane gas is considered a release-flammable chemical with the potential to contribute to an explosion and poses a different hazard than chlorine gas, which is a release-toxic hazard chemical with the potential to create a toxic vapor. For more information on the ChemLock Chemical Hazard List, please visit the ChemLock Resources webpage.

Risk can be calculated using this formula:

Risk = f(Threat, Vulnerability, Consequence)

In other words, risk is a function (or “f”) of threats exploiting vulnerabilities to obtain, damage, or destroy assets.

Risk Management

Risk management is a continuous process of evaluating assets, threats, and vulnerabilities and then adjusting as necessary. Mitigating any of these three components of risk lowers the specific risks that on-site chemicals present.

In an ideal world, all security measures could be implemented without concern for costs or other resources. However, resources and personnel are limited. Risk management processes help facilities to prioritize security efforts—because if you try to protect everything, you could either expend all your money and resources or you protect nothing as resources are spread too thin across identified risks.

Figure 3 can help facilities prioritize security efforts based on the consequence and likelihood of a threat occurring.

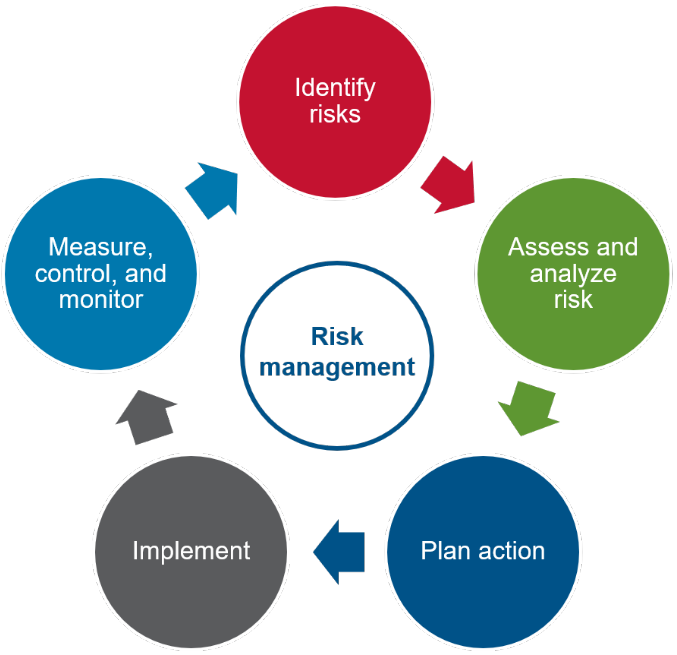

Figure 2. Risk Management Cycle

		Consequence				
		Insignicant 1	Minor 2	Significant 3	Major 4	Severe 5
Likelihood	Almost Certain 5	Medium 5	High 10	Very High 15	Extreme 20	Extreme 25
	Likely 4	Medium 4	Medium 8	High 12	Very High 16	Extreme 20
	Moderate 3	Low 3	Medium 6	Medium 9	High 12	Very High 15
	Unlikely 2	Very Low 2	Low 4	Medium 6	Medium 8	High 10
	Rare 1	Very Low 1	Very Low 2	Low 3	Medium 4	Medium 5

Table 1. Risk Evaluation Table

Risk combines critical asset identification, threat, vulnerability, and consequence.

- Critical asset identification identifies the importance of given resources (e.g., dangerous chemicals).
- Threat equals the probability of attack. Threats may exist, but if there are no vulnerabilities, then there is little/no risk.
- Vulnerability equals the probability of success given an attack. You can have a vulnerability, but if you have no threat, then you have little/no risk.
- Consequence equals the impact of an attack.

2 Security Concepts

Necessity for Security

Security—a separate discipline from law enforcement or police services—refers to physical and cyber features and procedures that protect critical assets, personnel, physical structures and materials, and data, at a minimum. Protection of these assets prevents harm or abuse, while failure to properly secure these assets exposes them to injury, damage, theft, or other misuse, as well as negatively impacting the facility's reputation should such activities occur.

Security-in-Depth

Security-in-depth (also referred to as layered security) is an industry accepted concept in asset protection used to slow or dissuade potential criminals from unauthorized facility access. Most frequently, this is accomplished by placing the most critical (or dangerous) assets within the innermost interior of the site while applying multiple active and passive physical security measures to deter, detect, and delay an adversary.

> **Security-in-depth can increase protection because a facility has multiple layers of complementary security measures.**

Using multiple layers between the outer and inner layers—including the use of physical barriers, fencing, signs, lighting, and advanced technologies, such as access control systems, intrusion detection systems, and camera systems—dramatically increases the likelihood of delaying and detecting unauthorized access, and ensures a facility's critical assets can be suitably protected against a variety of potential threats.

Security-in-depth integrates security procedures—such as a personnel screening at an entry point—with technologies—such as an electronic access card reader—that complement each other. Furthermore, layered security measures can be used in different application levels because not all assets are valued equally and thus require different levels of protection.

When evaluating which security layers should be implemented, facilities should consider security measures that counter identified security threats. For example, assets at risk for theft may want additional layers of detection or access control, while assets at risk for release may consider additional delay barriers to protect against both human-borne and vehicle-borne attacks. In addition, consideration of security layers should include emerging threats—such as the physical and cyber threat posed by drones that can easily fly over physical barriers to carry out an attack or surveil a facility to identify assets or security protocols.

Figure 4 provides an illustration of security-in-depth.

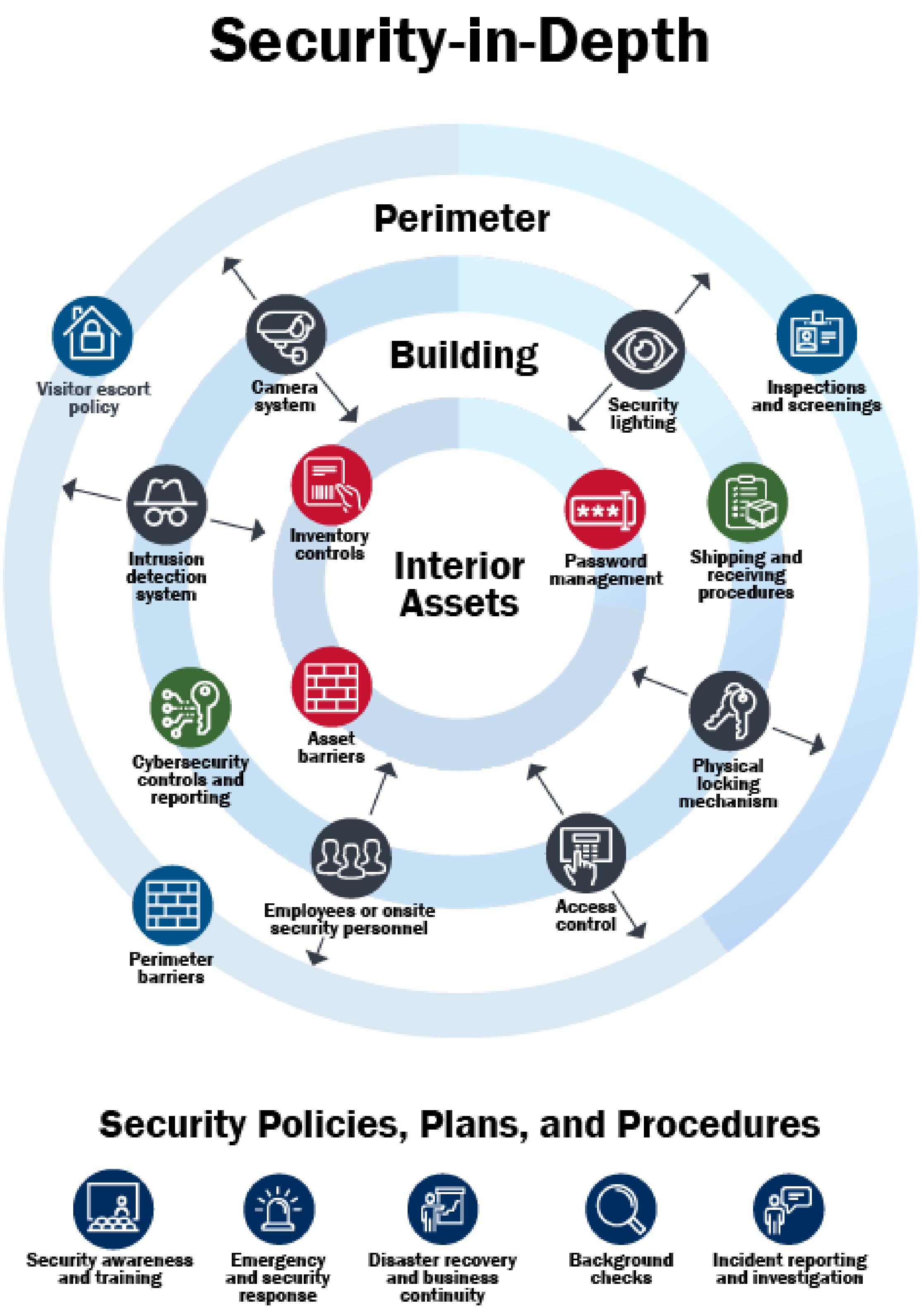
Security-in-Depth
Perimeter
Building
Interior Assets
Visitor escort policy
Camera system
Security lighting
Inspections and screenings
Intrusion detection system
Inventory controls
Password management
Shipping and receiving procedures
Cybersecurity controls and reporting
Asset barriers
Physical locking mechanism
Employees or onsite security personnel
Access control
Perimeter barriers
Security Policies, Plans, and Procedures
Security awareness and training
Emergency and security response
Disaster recovery and business continuity
Background checks
Incident reporting and investigation

Figure 3. Security-in-depth is often illustrated as a series of concentric circles or rings of security, with the inner-most layer protecting the most critical components or assets and the outer-most layer providing the initial barrier and lines of detection.

Implementing Security-in-Depth

To achieve security-in-depth that protects people, assets, and the company's reputation, managers must determine how best to protect the facility in keeping with the operational facility constraints or business needs.

A facility may opt to protect just an asset (asset-based approach), the entire site (facility-wide security approach), or a combination of the two approaches. Both strategies are used to protect assets from various threat scenarios, such as asset theft or a toxic hazard release.

Security Goals

To assist in applying a holistic approach to security that can address different threats and hazards, the rest of "Part 1: Security Goals" presents five security goals for facilities to think through as they evaluate what security measures make the most sense for each particular facility and formulate a facility security plan:

1. Can you **DETECT** an attack or suspicious activity?
2. Can you **DELAY** the adversary?
3. Are you able to **RESPOND** in a timely manner?
4. Are you protecting your **CYBER** assets?
5. Do you have the appropriate **POLICIES, PLANS, and PROCEDURES** to implement your plan?

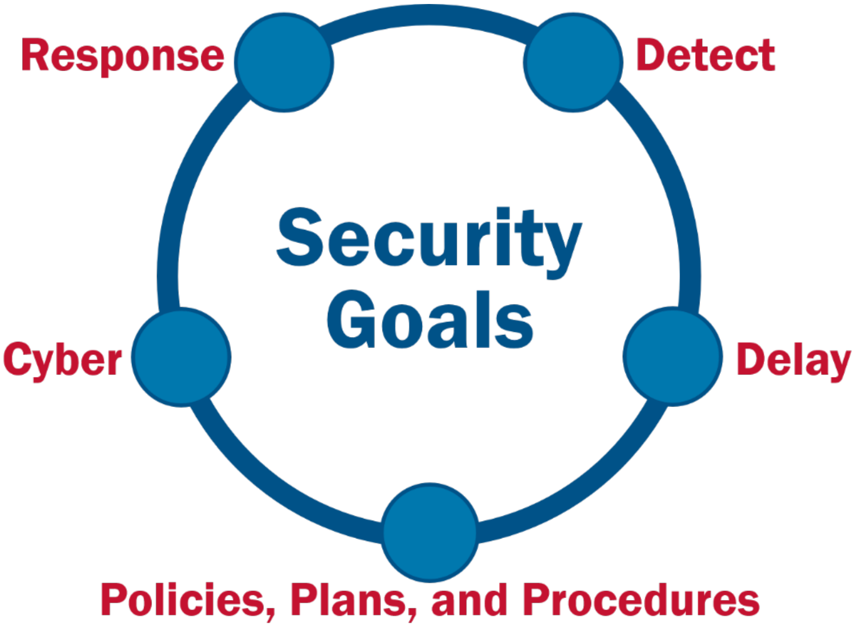

Figure 4. These five security goals are critical to a holistic approach to chemical security.

Layered security provides the best option to protect your facility from a variety of threats.

3 Detection

Can you detect a potential attack or suspicious activity?

Detection refers to the ability to identify potential attacks or precursors to an attack and to communicate that information as appropriate. Detection measures typically include surveillance and other types of monitoring to ensure the protection and security of dangerous chemicals or assets. For a protective system to prevail, detection needs to occur prior to an attack (i.e., in the attack-planning stages) or early enough in the attack where there is sufficient delay between the point of detection and the successful conclusion of the attack for the arrival of response forces to thwart the attempt. Therefore, detection, deterrence, and layers of delay are inherently linked. The levels of detection that a facility chooses to implement should be based on the levels of delay implemented and vice versa. A facility that has multiple layers of robust delay measures could decide to implement a lower level of detection and still have a successful protection system in place.

> **Detection is the capability to identify potential attacks or indicators of an attack—such as the theft, release, or sabotage of your chemicals—and to communicate that information, as appropriate.**

Facility activity can be monitored through a combination of human oversight and a variety of technical sensors interfaced with electronic entry-control devices, remote surveillance imaging, and alarm-reporting displays. When an event of interest to security is identified, it is either assessed directly by sending persons to that location or remotely assessed by personnel evaluating sensor inputs and surveillance images. Whichever method or combination of methods a facility utilizes, it is important to ensure the efficacy of those security measures through ongoing assessment.

Intrusion Detection System (IDS)

An IDS provides early warning of unauthorized penetration. IDSs typically consist of various hardware and software elements operated by trained personnel with security responsibilities. The system triggers an alarm or other notice of an attempted breach, which can be used for activating corresponding cameras or for dispatching personnel to investigate the alarm. Examples of IDS systems include infrared (IR) sensors, microwave sensors, fiber optic sensors, buried cable, magnetic switches, balanced magnetic switches, volumetric motion sensors, glass break sensors, and passive IR motion sensors.

Key Considerations:

- Cover all entry points, such as doors and windows. The line of intrusion sensors around the areas to be protected should be continuous.
- Use multiple lines of detection to achieve security-in-depth at critical assets.
- Use complementary sensors covering the same area but using different means of detection (such as a video camera used in conjunction with an alarm) to decrease the probability of defeat.
- Enhance system effectiveness with alarm combination and priority schemes.
- For exterior sensors, take into account weather and terrain to ensure effective deployment of sensors. Nuisance alarm rates due to environmental causes should be considered for technical applications.
- Always ensure activation of IDS when other detection methods are not available.
- Ensure alarm notifies a responsible and trained individual(s) or a third-party monitoring service to initiate a response.
- Create a documented process for response to alarms.
- Consider systems that can detect a UAS flying near or over a facility.
- Consider back-up power.

Types of IDS include:

- **Fence-mounted sensors**
- **Wall-mounted sensors**
- **Window-mounted sensors**
- **Volumetric sensors**
- **Beam sensors**
- **Gate/door sensors**

Camera System

Camera surveillance systems are a proven and trusted security method for monitoring your facility’s critical assets. The equipment is often relatively inexpensive compared to other means of surveillance, provides detailed images of scenes for positive assessment of what is happening, and operates for years with minimal maintenance.

Key Considerations:

- Include the integration of cameras, recorders, switches, keyboards, and monitors.
- Ensure camera system is monitored by a dedicated and trained individual.
- Choose an appropriate lamp that has accurate color reproduction.

- Consider the material that will be illuminated and its ability to reflect and transmit light.
- Identify whether reflected lighting will assist or interfere with camera operation.
- Identify what wireless and remote devices can be accessed and used both on- and off-site and are they properly secured with strong passwords.
- Ensure ability to remotely access camera systems, including disarming and deleting.
- Ensure ability to detect motion, including alerting abilities.
- Consider backup power.

There are many types of camera systems:

- Day/night cameras
- Infrared/night vision cameras
- Network/internet protocol (IP) cameras
- Wireless cameras
- Dome cameras
- Pan-tilt-zoom (PTZ) cameras

FYI **Cameras can also provide a safer alternative for assessing damage during or after a natural disaster, especially if there is a release or other dangerous circumstances that must be considered before re-entering the area where the asset is located.**

Employees or On-Site Security Personnel

Personnel are often used to enhance perimeter and asset security and provide a means of deterrence, detection, delay, and response. Such forces can be proprietary or contracted and can be armed or unarmed. Protective forces can be used in a variety of ways, including standing post at perimeter entry points and/or critical assets, monitoring entry points and/or critical assets using remote surveillance, or conducting roving patrols on a documented schedule (often rotating) that specifically includes identified targets, processes, or other critical assets. Protective forces may be qualified to interdict adversaries themselves or they may simply deter and detect suspicious activities and call local law enforcement to provide an interdiction. Employees may be trained in security awareness and may act as your facility's line of detection for your critical assets.

Key Considerations:

- If using personnel, ensure training is provided that includes recognizing attempts in breaching the facility and/or asset, suspicious person or vehicles, degradation to security measures, and reporting potential security incidents. Ongoing and refresher training is key when detection capabilities rely on personnel.
- If employing protective forces, consider their use in combination with one or more security measures as personnel alone generally do not provide sufficient perimeter security.
- Depending on the circumstances, consider joint security details among co-located facilities or facilities sharing common infrastructure, if appropriate.
- Consider utilizing records of patrols/monitoring to ensure that all areas are specifically targeted and observed (i.e., security tour patrol wand).
- Consider varying patrol times and locations in order to avoid predictability.

Security Lighting

Security lighting can help to both deter attempts at accessing a facility's perimeter or assets and assist in the monitoring and detection of any such attempts. Inadequate lighting can make it more difficult to monitor a perimeter and detect attempts to breach the perimeter. Maintaining a well-lit facility perimeter also can help deter adversaries from attempting to breach the perimeter. Many different types of security lighting are available for implementation at facilities.

Key Considerations:

- When selecting appropriate lighting, identify your facility's power sources, grounding, and interoperability with and support to other monitoring and detection systems, such as camera systems.
- Consider how local weather and environmental conditions can also significantly affect sensor and lighting performance. Security lighting that may be considered acceptable during ideal weather conditions may be insufficient during periods of inclement weather.
- Consider backup power.

Inventory Controls

Inventory controls used to track a facility's chemicals can provide not only a level of security for the chemicals, but also offer a financial benefit to the company by limiting theft of raw materials or finished products, interruptions in production due to lack of material, or loss of sales caused by limited stock. A good inventory control system will consider raw materials, in-process or semi-finished materials, and finished goods ready for sale or transport.

Key Considerations:

- List all the chemicals, mixtures, and products at the facility and provide regular tracking of the quantity and the physical location of each chemical.
- Monitor use by authorized personnel.
- Consider container-based tracking of multiple lots, vendors, and sizes.
- Track disposal and maintain a record of disposed containers.
- Limit access to areas where potentially dangerous chemicals are stored to authorized personnel.
- Maintain quality records of sales, deliveries, and transfers.

Detection measures include:

- Intrusion detection system
- Camera system
- Employees or on-site security personnel
- Security lighting
- Inventory controls

4 Delay

Can you delay the adversary?

Delay security measures include physically limiting access to your facility and/or assets to reduce the likelihood of an adversary successfully breaching the perimeter and/or assets or using the area immediately outside of the facility's perimeter to launch an attack. Delay security measures also include security measures that deter an attempt to breach the perimeter and/or assets. An optimal security solution typically involves the use of multiple protective measures that provide layers of security. A facility may want to consider employing facility perimeter and asset-specific measures. Delay measures include:

> **Delay includes the capability to slow down an adversary's progress sufficiently to allow adequate protective forces to respond.**

- Perimeter and asset barriers
- Physical locking mechanisms
- Access control
- Inspections
- Screenings
- Know-your-customer program

Perimeter and Asset Barriers

Perimeter and asset barriers reduce the likelihood of unauthorized access for malicious purposes, such as theft, sabotage, or intentional release of chemicals. By securing and monitoring the perimeter of the facility, facility personnel can more easily and effectively control who enters and leaves the facility, both on foot and in vehicles. Perimeter and asset barriers provide both physical obstacles and psychological deterrents to unauthorized entry, delaying or preventing forced entry. They can be used in a variety of ways to restrict the area perimeter and increase overall facility security, including controlling vehicular and pedestrian access, providing channeling to facility entry control points, delaying forced entry, and protecting critical assets.

Key Considerations:

- The most commonly used manmade human barriers by industrial facilities are chain-link fencing. Chain-link fencing is readily available through a variety of sources and is easily and inexpensively maintained. This type of fence provides clear visibility for security patrols and is available in varieties that can be installed in almost any environment.

- Facilities can elevate the level of effectiveness of fencing simply by adding barbed wire, razor wire, or other available toppings to increase intrusion difficulty. Signage (i.e., keep out, no trespassing, etc.) can also act as a deterrent.
- Facilities should identify if vehicle barriers, such as bollards, berms, ditches, and jersey barriers, are also appropriate for your facility. These are especially important for chemicals with release concerns where a vehicle-borne improvised explosive device (VBIED) could pose a threat.
- Walls are one of the most common types of barriers. Various types of walls are used for interior and exterior security boundary separation. A wall can serve as a human barrier and/or a vehicle barrier.
- A layered approach to perimeter barriers and monitoring potentially increases the opportunity to reduce cost and uses existing facility natural features or more applicable technologies to meet the performance objectives.
- Facilities can achieve a higher level of security performance by deploying barriers behind the intrusion detection system so that an intruder would activate an alarm sensor before defeating the barrier(s), thereby providing additional time for assessment and response. Barriers located in front of alarm sensors serve to mark property boundaries.

Types of perimeter barrier include:

- Fences
- Walls
- Bollards
- Berms
- Ditches
- Jersey barriers

FYI **When considering which security barriers are best for your facility, consider which barriers would also protect the asset from natural threats, such as floods and fires.**

Physical Locking Mechanism

Physically limiting access to your chemicals can reduce the likelihood of authorized access. Securing an asset is frequently accomplished by using multiple layers of physical barriers and by using a combination of security measures.

Key Considerations:

- Utilize one or more types of locking mechanisms for entry points to the perimeter or critical asset(s): locksets, deadbolts, magnetic locks, padlocks, cam locks, mortise locks, and/or cylinder locks.
- Ensure access points are always locked when the access point is not in use or manned.

- Maintain a key lock, combination, and/or access credential control and accountability program that ensures keys, locks, combinations, and access credentials are:
    - Only issued to authorized individuals
    - Collected upon termination of employment or change in work status
    - Periodically inventoried
    - Changed when there is a loss or suspicion of compromise or upon termination of employment

Access Control

Through access control measures, a facility is better able to prevent unauthorized access to the facility or its restricted areas and is more likely to deter and detect unauthorized introduction or removal of substances and devices that may cause a dangerous chemical reaction, explosion, or hazardous release. Access control measures may include a personnel identification program, visitor policies, perimeter restrictions, and/or an electronic access control system.

Restricting access to only authorized individuals requires personnel identification as it can help both security officers and other employees quickly know whether an individual is authorized for access.

Key Considerations:

- Maintain a personnel identification program appropriate to your employees and operation by employing badges, uniforms, or other identification means.
- Grant access only to authorized individuals using the least privilege concept and use an identification program which enhances this, such as color-coded badges.
- Ensure access points are locked when not in use or manned.
- Maintain a key/access program to ensure access is only issued to authorized individuals.
- Use employee training to recognize and identify facility personnel granted access.
- Identify appropriate on-site parking policies such as limiting on-site parking to certain vehicle classes or creating a significant distance away from the critical assets.
- Establish control point measures to help control vehicular access to a facility or a restricted area. These entry points calm traffic as it approaches the facility or restricted area, provides an opportunity for vehicle identification to occur, and denies access to unauthorized vehicles.

Inspections and Screenings

Through identification, screening, and inspection, a facility is better able to prevent unauthorized access to the facility and more likely to deter and detect unauthorized introduction or removal of substances and devices that may cause a dangerous chemical reaction, explosion, or hazardous release. A variety of different types of measures may be used to perform screening, such as personnel identification, hand-carried items inspections, vehicle identification, and vehicle inspections.

Key Considerations:

- A primary component of successfully screening and controlling access is knowing who is allowed on-site. Identification measures can help both security officers and other employees quickly know whether an individual is authorized for facility access. This can be accomplished by conducting checks of government IDs of visitors or issuing company IDs to employees.
- Facilities should consider implementing a screening program to inspect items brought into the facility, whether brought in by employees, contractors, or visitors. This could include the use of visual inspections, X-ray inspections, metal detectors, ionic explosives detection equipment, and/or trained explosive detection canines.
- Vehicle identification measures can include using a facility-issued vehicle ID system (e.g., providing authorized vehicles with stickers or placards), using only known shippers and/or delivery companies, and requiring authorized bills of lading for access to the facility.

Shipping and Receiving Procedures and a Know-Your-Customer Program

Product stewardship describes a product-centered approach to protection of potentially dangerous chemicals so that manufacturers, retailers, and consumers share responsibility for reducing the potential for theft, contamination, or misuse of such chemicals. Stewardship includes having a set of shipping and receiving procedures to ensure proper handling and receipt of chemicals, as well as having a know-your-customer program or similar practice that ensures customers purchasing chemicals are properly vetted, to include verifying a customer’s identity, business location, financial status, and chemical end use.

Key Considerations:

- Use an active, documented know-your-customer program that includes a policy of refusing to sell chemicals to those who do not meet the pre-established customer qualification criteria. Examples of such criteria may include verification that shipping addresses are valid business locations and confirmation of financial status.
- Plan and approve all shipments and orders of chemicals in advance using known and previously approved carriers.
- Monitor en route shipments and confirm all shipments have arrived at their final destination.
- Ensure all sales and shipments of chemicals are documented, including the method of shipment, carrier information, the times and dates of shipments, and the destination.

Delay measures include:

- Perimeter and asset barriers
- Physical locking mechanism
- Access control
- Inspections and screening
- Shipping and receiving procedures

5 Response

Are you able to respond in a timely manner to a perceived or known threat?

As part of response preparations, your facility should include training personnel to effectively respond to a threat of or actual theft or release of chemicals. This may comprise plans to mitigate and respond to the consequences of a security incident and to report security incidents internally and externally in a timely manner. Comprehensive response plans should involve all facility personnel, designated facility emergency response personnel, local law enforcement, and other off-site first responders.

> **Response includes the capability to communicate, report, and manage the appropriate reaction(s) to potential attacks and/or adversary actions, and/or to reduce the effect of security related events.**

Response measures should address the identification of the hazards, the corresponding response plans for those hazards, the number and capabilities of the various responders, and the equipping and training of response personnel. Properly equipped personnel who understand the potential consequences of a security incident and the need for timely, effective actions, when coupled with well-rehearsed response plans, reduce the probability of an attack achieving the adversaries' desired goals.

Additionally, practiced response plans help ensure that on-site responders and local law enforcement, fire, medical, emergency management, mutual aid, and rescue agencies are familiar with the facility and chemicals stored on site and are not impeded from reaching the location of the security incident.

Emergency Response Procedures and Crisis Management Plans

One of the most important elements for a successful response to an incident is a well thought-out, documented crisis management plan upon which the relevant individuals have been trained. The types of activities that a facility may want to address in its overarching crisis management plan may include contingency plans, continuity of operations (COOP) plans, emergency response, post-incident security (e.g., post-terrorist attack, security incident, accident, hurricane, or other natural disaster), evacuation, notification control and contact requirements, re-entry, and security response.

Key Considerations:

- Consider maintaining documented agreements with off-site responder services, such as ambulance, environmental restoration, explosive device disposal, firefighting, hazardous material spill/recovery, law enforcement, marine, and medical.
- Designate an individual responsible for executing each portion of the plans and procedures.
- Consider the use of backup power, emergency communications equipment, and process safeguards.
- Test response plan capabilities and identify suspected vulnerabilities with drills and exercises.
- Train staff and leadership to identify and adjust to changes in threats and adversary capabilities to help ensure your facility's response plans are practiced.
- Consider community notification protocols should an incident occur.

Outreach Programs

In order to ensure that external resources are properly prepared, the facility should consider an active outreach program with local first responders such as local police department, fire department, emergency management, and Local Emergency Planning Committees (LEPCs).

Key Considerations:

- Share emergency plans with first responders and local law enforcement.
- Provide facility layout information to local first responders or invite local first responders to facility orientation tours.
- Share, as appropriate or required by law, information regarding dangerous chemicals on site with local first responders and law enforcement.
- Consider outreach programs to the local community that could be affected by an on-site incident.

> **The first time that local law enforcement or first responders actually access the facility should not be the day of an incident.**

Security Plans for Elevated Threats

The ability to escalate the levels of security measures for periods of elevated threat provide a facility with the capacity to increase security measures to better protect against known increased threats or generalized increased threat levels declared by the federal government. The Department of Homeland Security (DHS) utilizes the National Terrorism Advisory System (NTAS) to communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports, and other transportation hubs for the private sector.

Key Considerations:

- Maintain awareness of NTAS bulletins and notifications (dhs.gov/national-terrorism-advisory-system).
- Develop a documented process for increasing security measures commensurate to the designated threat level during periods of elevated threats tied to the NTAS.
- Coordinate with federal, state, and/or local law enforcement agencies to identify recommended actions and additional security measures.

Response measures include:

- Emergency response procedures and crisis management plans
- Outreach programs
- Security plans for elevated threats

6 Cyber

Are you protecting your cyber assets?

Cybersecurity threats can take a variety of forms, all of which may endanger the strength and resilience of critical infrastructure. Malicious actors may implement a variety of tactics to compromise an organization's information and control systems. Depending on the desired effect of the malicious actor, outcomes can include loss of privacy, data, money, and/or life; disruption of service; physical harm; and depreciation of consumer confidence.

Protecting against cybersecurity incidents is essential to the management of the overall risk for a facility. The goal of a chemical facility's cybersecurity risk framework should include the ability to identify, protect, detect, respond, and recover from a cyberattack, while also minimizing the consequences of physical impacts. This can be accomplished by preventing unauthorized access to critical cyber systems, such as information, business, and control systems. Specifically, information technology (IT) and operational technology (OT) systems that a facility might consider critical may include those that:

> **Cybersecurity is the capability to protect critical information, business, and control systems against damage, unauthorized on-site or remote access, modification, or exploitation.**

- ▶ Monitor and/or control physical processes that contain a chemical.
- ▶ Manage physical processes that contain a chemical which could be used to cause disruption or even destruction to the process and surrounding environment.
- ▶ Contain business or personal information that, if exploited, could result in the theft, diversion, or sabotage of a chemical.

These systems and the network they operate on are often integrated throughout the operations of chemical facilities.

Cybersecurity Policies and Procedures

Security policies, plans, and procedures that specifically address operational constraints, sensitivity issues, and processing environment issues can be addressed in general IT documentation or specified in their own dedicated documentation. Given the unique security considerations surrounding control systems, facilities may want to develop policies, plans, and procedures specific to control systems.

Key Considerations:

- Change management is a formal process for directing and controlling alterations to the information processing environment. The objectives of change management are to reduce the risks posed by changes to the information processing environment and improve the stability and reliability of the processing environment. Cyber change management policies should cover account policy mandates, security concerns, business impact, authorization, risk reductions, and oversight.
- All policies and procedures should be provided to all employees and contractors, as appropriate, who have access to the critical cyber system.

Access Control and Password Management

Understanding and managing data access—both in-person access and transferring data electronically (i.e., across the internet, a wireless connection, or portable cyber equipment, such as flash drives)—is an essential component of cybersecurity. By verifying external connections with network tools designed for this purpose, managers can be certain of who or what is accessing their systems and networks.

Key Considerations:

- Identify any critical cyber control systems or business systems to ensure adequate cybersecurity protections and physical security systems are in place to protect your chemicals.
- Ensure all external connections to/from critical systems are documented and have a business need. Organizations should have a policy that no new connections can be established without management authorization and documentation.
- Maintain access control lists and ensure that accounts with access to critical/sensitive information or processes are deactivated immediately when personnel leave and when users no longer require access.
- Implement password management protocols to enforce strong password requirements, ensure all default passwords have been changed, and implement physical controls for cyber systems where changing default passwords is not technically feasible. Consider two-factor authentication or biometric authentication if feasible and/or cost effective.
- Use physical security measures to secure the buildings, rooms, access panels, or other elements.
- Implement role-based physical access controls to restrict access to critical systems and information storage media.
- Ensure that all wireless devices or wireless access points use the latest encryption technologies and use strong authentication requirements to prevent unauthorized or remote access.

Cybersecurity Training

The human component is often the most vulnerable aspect of a system. As a result, a good cybersecurity culture and training program generally involves making system users aware of the need for security and instructing them on their roles in keeping the cyber system secure. This includes bringing together users of information technology (IT) and operational technology (OT) systems. A documented cybersecurity training program, which establishes the types and frequency of training, is one effective way to accomplish this.

Key Considerations:

- Basic training that all employees should receive includes general company policy reviews, roles and responsibilities, password procedures, acceptable practices, and how to report suspected inappropriate or suspicious activity.
- Training is most effective when delivered repetitively and frequently and when training courses are updated to reflect the changing threat and vulnerability environment. An effective training program may provide for different training regimens appropriate for employees with different roles. For example, system administrators typically need more training than standard users because of their access to highly sensitive material.

Cybersecurity Controls, Monitoring, Response, and Reporting

Facilities should monitor networks for unauthorized or malicious access to maintain situational awareness and mitigate risk. Recognizing and logging events and incidents is critical to overall system and network security.

Key Considerations:

- Use an IDS—which is designed to capture network or host traffic, analyze it for known attack patterns, and take specified action when it recognizes an intrusion or attempted intrusion—to monitor networks. An IDS can be software or hardware and can be network-based or host-based.

> **Because cyber systems and the network they operate on are often integrated throughout the operations of chemical facilities, defending against adverse cyber events is essential to the management of the overall risk for a facility.**

- Use an Intrusion Prevention System (IPS) that monitors a network for malicious activities, such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and then report it. An IPS can be software or hardware and can be network-based or host-based.
- Implement anti-malware software on a facility's systems.

- Update software (after appropriate testing) on a regular basis.
- Install software patches so that attackers cannot take advantage of known problems or vulnerabilities.
- Report significant cyber incidents to senior management and CISA Central at central@cisa.gov. CISA Central provides a critical infrastructure 24/7 watch and warning function, and gives all stakeholders a means to connect with and receive information from all CISA services.

Disaster Recovery and Business Continuity

An organization with plans in place for COOP, IT contingency, and disaster recovery has a mature cybersecurity program for its critical cyber assets, as all of these plans incorporate cybersecurity considerations during contingency operations and recovery/reconstitution activities. As recovery operations (i.e., those operations addressed in the COOP, IT contingency, and disaster recovery plans) are often performed under pressure, systems often are vulnerable to security concerns when they are underway. Thus, it is important to consider cybersecurity during such operations.

Key Considerations:

- Ensure that cybersecurity best practices are followed when setting up an alternate system or network.
- Set up alternate systems to allow rebuilding and reconfiguring of the primary systems and networks.
- Ensure that remote access to systems includes safeguards such as virtual private network (VPN) access.
- Ensure audits that review compliance with the facility's cybersecurity policies, plans, and procedure are being conducted regularly. Report audit results to senior management for action if needed.
- Implement processes and procedures for backup and secure storage of information.
- Implement procedures for operating the control system environment in manual mode.
- Maintain a complete and up-to-date logical network diagram.
- Test backup media.
- Test all plans repeatedly and take actions based on the results of the tests.

CISA's Cyber Essentials is a guide to help public and private sector organizations understand where and how to start implementing cybersecurity practices. Learn more on the Cyber Essentials webpage.

Cyber measures include:

- Cybersecurity policies and procedures
- Access control and password management
- Cybersecurity training
- Cybersecurity controls, monitoring, response, and reporting
- Disaster recovery and business continuity

7 Policies, Plans, and Procedures

Do you have the appropriate policies, plans, and procedures to implement your plan and security measures?

A facility's security plan cannot be effective without the integration of cyber and physical security measures with procedural security measures. These procedural measures are required to execute all aspects of the security plan. This covers plans in place for maintenance of security equipment, training of personnel, employee background checks, incident reporting and investigation, security organization and officials, and recordkeeping.

> **Policies, plans, and procedures ensure the capability to manage your facility security plan, including the development and implementation of policies, procedures, and other processes that support security plan implementation and oversight.**

Maintenance, Inspection, and Testing of Security Equipment

Regular maintenance, inspection, tests, repairs, and improvements to the security, safety, and communications systems increases the reliability of such systems and will improve response time.

Key Considerations:

- ► Comply with the manufacturers' instructions and specifications for frequency of testing, repair, and replacement schedules to increase the likelihood that the physical security equipment will function as it is expected to and decrease the likelihood that it will malfunction.
- ► Institute a regular, written plan for the maintenance, testing, calibration, and inspection of equipment as equipment that is functioning well is often overlooked.
- ► Employ appropriate temporary security measures when performing maintenance and in response to nonroutine equipment outages, failures, and malfunctions.
- ► Document nonroutine incidents and promptly report them to the designated facility personnel.

- Identify an individual responsible for ensuring the inspection, testing, and maintenance of security systems.

Security Awareness and Training Program

A security awareness and training program (SATP) is a predefined and documented set of scheduled activities that include training, exercises, drills, tests, and joint initiatives that focus on relevant security related issues for the facility and enhance the overall security awareness of all facility employees. By performing proper security training, exercises, and drills, a facility enables its personnel to be better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders.

> **Well-trained personnel who practice how to react and who understand the facility's layout and hazards will be more effective at detecting attackers, delaying intruders, initiating response activities, and reducing the consequences of an attack.**

Key Considerations:

- Include all levels of facility personnel in the program, including executives, management, operations, and technical employees.
- Include policy, guidance, and standards; training courses and materials; exercises of varying types and scope; a schedule; and evaluation and remedial action programs.
- Blend hands-on activities, seminars, orientations, workshops, online or interactive programs, briefings, and lectures that enhance the overall security awareness of all facility employees.
- Incorporate drills and exercises to provide training with new equipment, develop new policies or procedures, or practice and maintain current skills.

Background Check on Personnel

A successful background check program can significantly improve a facility's capability to deter, detect, and defend against insider threats or covert attacks. Employee background checks address the need for a facility to ensure that individuals allowed on site have suitable backgrounds for their level of access. Examining personnel backgrounds is the process of acquiring information on an individual through third-party services, government organizations, and private individuals to make a "suitability determination" for the future actions based upon past actions. Background investigations can also verify the accuracy of an applicant's employment history, educational history, and credentials, as well as confirm the lack of criminal history and sanctions.

Key Considerations:

- Consider what level of checks are appropriate to your facility. The contents, type, and depth of background investigations vary widely, but most basic checks consist of at least criminal record search, employment verification, education verification, driving record, and credit check.
- Verify and validate the legal authorization to work by utilizing the I-9 process or E-Verify prior to granting access to restricted area(s) and critical asset(s).
- Maintain a process for adjudicating the results of these background checks and determining access restrictions in a reasonable manner.
- Identify and maintain lists of employees who have access to chemicals. Consider whether contractors or visitors would be a part of this determination.

Insider Threat Program

One of the biggest threats that a company faces is an insider causing harm to the organization. Current or former employees that have access and knowledge to internal company policies and procedures may either intentionally or unintentionally use their access to harm their organization. It is important for companies to consider this threat while developing all areas of their security plan and what could happen if these areas were compromised. Could chemical inventory be changed or delivered elsewhere? Can someone gain access during non-operational hours? Can alarm systems be compromised?

Some insider threat examples are:

- Cyber threat
- Theft of intellectual property
- Sabotage of systems or equipment
- Espionage
- Fraud
- Workplace violence
- Non-malicious, accidental incidents

CISA's Tabletop Exercise Packages (CTEPs) can assist facility owners and operators develop an exercise that meets the specific needs of the facility. To learn more, visit the ChemLock webpage.

Key considerations:

- Develop and conduct insider threat training on a regular basis and include recognition of security incidents, reporting of security incidents, classified information training (if applicable), IT policies, personnel ethics policies, and reporting and response procedures. Training should also include lessons learned from previous security incidents.
  - Insider threat training should be facility-specific and address specific information that if stolen or destroyed would destroy or ruin the organization. Identify what makes this vulnerable and what is necessary to access the information. Consider use of tabletop exercises, functional exercise, and full-scale exercises.
- Ensure reporting procedures should:

  - Identify reporting guidelines, including anonymous reporting and multiple communication channels for reporting.
  - Ensure reporting protects the privacy of all concerned.
  - Provide quick feedback to those who report (as applicable).
  - Document near-misses, lessons learned, and signs of suspicion (i.e., abrupt change in behavior, substance abuse, repeated rule violations, odd working hours, etc.).

- Develop an insider threat working group with personnel from across the organization (to include human resources) and work with the group to develop governance and policy documents that describe acceptable behavior and consequence for violation. The group should ensure legal and ethical oversight is maintained, establish relationship with investigative authorities, and define response process for potential insider threats with adherence to privacy policy.
- To minimize the risk of theft, implement controls for shipping and selling chemicals, including:
  - Confirmation of shipments, verification of transactions, “know-your-customer” program, and advanced approval of shipments.
  - Procedures for handling the arrival of an unknown or unapproved customer.
  - Inventory management (enhanced methods include Glocal Positioning System [GPS] tracking, surveillance monitoring, etc.).
  - Exercises for effective sales and shipments (i.e., discuss what would happen if an unauthorized customer attemptted to pick up dangerous chemicals).
  - Restriction of contact and purchase information to a need-to-know basis.

More information on insider threat resources is available on CISA’s Insider Threat Mitigation webpage.

- Organizations should consider internal cybersecurity systems and policies:
  - Ensure that IT security training includes security requirements and violations.
  - Identify if employees can log in from the internet, if they have email accounts, and if remote access is tracked and monitored.
  - Identify via system monitoring if employees are logging on remotely; accessing information they do not need for their job; copying, printing, or emailing excessive amounts of information; or engaging in anomalous activity that goes beyond their work role.

  - Identify where your information is stored—including personal identifiable information (PII), purchasing, inventory, etc.—and who has access to view and/or change and manipulate information.
  - Monitor user activity on the system consistent with applicable privacy laws.
  - Consider restricting some capabilities to certain trusted individuals.
  - Implement dual authentication with recurring checks for access.
- Consider the following questions as they specifically relate to the organization.
  - Who has access to the asset(s)? Are individuals allowed solitary access? Is there a possibility for “piggy-backing” to gain access?
  - If an access control system is used, does management review access reports?
  - If an employee is entering or exiting organization facilities at odd hours, does he or she have a legitimate work reason?
  - Are attempts to access restricted areas, systems, or information logged and reviewed? If there have been multiple failed attempts, would this be known?
  - How often is inventory conducted? Who reviews inventory? When would a loss or theft be noticed? What internal controls are in place? Is there inventory verification conducted?
  - What type of screening occurs at the facility and critical asset(s)? Are people and/or vehicles searched after leaving access to theft areas?
  - Who has access to surveillance equipment? Who can control cameras/IDS/access control system (ACS)? Can systems be manipulated and, if so, would anyone know?
  - Who is notified when systems fail? Are there internal controls for temporary or compensatory measures? If a rogue staff member disabled the IDS, what would happen?
  - How are keys, locks, and access controls monitored and controlled? How often is inventory conducted? Are keys, locks, and access controls changed upon employee termination? Are pins and access codes unique? If not unique to each employee, are they hard to decipher (i.e., not 1234, etc.)?

Visitor Escort Policy

By implementing identification and control mechanisms for visitors, a facility can help mitigate the risk posed by visitors.

Key Considerations:

- Define who is considered a visitor at a facility: this could be contractors, delivery personnel, customers, etc.
- Consider the use of visitor registration forms, cards, or badges.

- Implement policies to escort all visitors gaining access to critical assets that do not have appropriate background checks.
- Ensure personnel escorting visitors have appropriate background checks and have been trained on escort procedures.

Processes for Incident Reporting and Investigations

Facilities should have an incident reporting and investigation program so that all significant security incidents are promptly and adequately reported to the appropriate facility personnel, local law enforcement entities, and CISA, as applicable, and that investigations are thorough in order to reveal vulnerabilities and identify corrective actions.

Key Considerations:

- Develop written procedures that define what is a reportable incident, how and two whom personnel should report, and when reporting elevates to external sources, such as local law enforcement, CISA, and the Federal Bureau of Investigation (FBI).
- Develop procedures for the investigation of a security incident, to include roles and responsibilities of internal and external resources. Consider how to identify vulnerabilities, document lessons learned, identify and implement corrective actions, and update training programs and policies based on these lessons learned.
- Include CISA Central at Central@cisa.gov as part of this reporting protocol.

Officials, Organization, and Records

To establish and reinforce a security culture, maintaining a security organization so employees understand their roles and responsibilities as it relates to security is an imperative. In addition, the establishment of a records management program ensures the company is following established policies and programs and allows for a comprehensive audit program.

Key Considerations:

- Identify individual(s) responsible for security.
- Consider what other facility roles may be involved in security, such as the cybersecurity officer and facility plant manager, and identify roles and responsibilities for all employees to further establish a culture of security.
- Create, maintain, and store the appropriate records related to the management of your facility's security to ensure all policies, plans, and procedures are being properly implemented.
- Audit your security plan on a reoccurring basis (e.g., annually) and conduct ongoing reviews of personnel roles within security plans.

Policies, plans, and procedures include:

- Maintenance, inspection, and testing
- Security awareness and training program
- Background check on personnel
- Insider threat
- Visitor escort policy
- Processes for incident reporting and investigation
- Officials, organization, and records

Part 2: Facility Security Plan

8 Facility Security Plan

A template for this facility security plan that does not contain CISA markings and can be edited and customized to meet company specifications is available on the ChemLock Resources webpage.

Understanding security principles is valuable, but without a facility security plan that implements specific security measures to meet those security principles, facilities may be unnecessarily exposing themselves to risk. CISA encourages facilities with dangerous chemicals to use this facility security plan template to develop a holistic, customized, site-specific security plan that mitigates risk and enhances chemical security at your facility.

In combination with "Part 1: Security Goals," this security plan helps facilities evaluate how dangerous chemicals are currently secured, identify gaps in security, and, ultimately, put plans in place to meet the various security goals.

This facility security plan aligns with the security goals described in Part 1:

- Critical asset identification (i.e., location, packaging, and other pertinent logistical information for on-site chemicals)
- Risk Management
- Detection security measures
- Delay security measures
- Response security measures
- Cybersecurity measures
- Policies, plans, and procedures to implement specific security measures

This plan should be developed with input from the facility's on-site security, safety, and logistical professionals to encompass all components of a security plan. Once a plan has been devised, facilities are encouraged to train all personnel on the plan and to establish an annual audit of the plan to ensure ongoing effectiveness, keeping in mind that security measures may need to change. It is also important to ensure contact information is identified and updated in the plan for local law enforcement and fire departments, as well as regulatory agencies, should emergencies arise.

Since there are a multitude of facility types that use potentially dangerous chemicals, aspects of this template security plan may not be applicable to all facilities.

If you have any questions or feedback pertaining to the security goals, aspects of this facility security plan, or other chemical security related topics, please email ChemLock@cisa.dhs.gov.

CHEMICAL FACILITY SECURITY PLAN TEMPLATE

[Name of Chemical Facility]

[Updated Month Year]

Revisions

Revision Version	Date Finalized	Effective Date	Authorized By
Ex. v1.0	January 21, 2021	February 1, 2021	Facility Security Officer John Doe

Contact Information

Facility Contact Information

Facility Name:	
Address:	
Facility’s Primary Contact – Name:	
Facility’s Primary Contact Phone/Email:	
Facility Security Officer:	
Facility Security Officer Phone/Email:	
Cybersecurity Officer:	
Cybersecurity Officer Phone/Email:	
Hours of Operation:	
Special Hours or Closures (Describe):	

Other Contact Information

Local Law Enforcement:	
Local Fire Department or First Responders:	
County Emergency Management Agency Official:	
City/Town/Locality Emergency Management Agency Official:	
County Public Health Official:	
City/Town/Locality Public Health Official:	
Local Emergency Planning Committee (LEPC) Chair:	
LEPC Vice-Chair:	
Cybersecurity and Infrastructure Security Agency (CISA) Chemical Security Personnel:	
Federal Bureau of Investigation (FBI) Weapons of Mass Destruction (WMD) Coordinator:	

Critical Asset Identification

Identifying the dangerous chemicals at your facility is the first step in determining what you need to protect and how you will protect them from threats.

Directions

- For each chemical, describe the location at your site and how it is used.
- Consider the inclusion of maps or plot plans in your security plan to help your facility personnel and emergency responders quickly identify the locations of dangerous chemicals.

Critical Assets

Chemical	Critical Asset Name	Location	Use (i.e., Ship, Sell, Manufacture, Store, Receive)
Ex. Chlorine	Chlorine Storage Cage	Warehouse Building 1	Receive

Notes

Detection

Detection includes the capability to identify potential attacks or indicators of an attack—such as the theft, release, or sabotage of your chemicals—and to communicate that information, as appropriate.

Directions

- ▶ Assess how your facility currently detects unauthorized access or suspicious activities.
- ▶ When you have identified the current security measures, compare them to the security principles laid out in Part 1, Section 3, Detection.
- ▶ Use this portion of the security plan to ensure each security measure is properly implemented and confirm whether it covers the chemical asset area.
- ▶ Identify any gaps in detection capabilities and any additional security measures that may be necessary to close those gaps.
- ▶ Develop a plan to implement any additional security measures.
- ▶ Consider your facility's operational hours when conducting this assessment and assigning security measures.

Notes

Detection Security Measures

1. Intrusion detection system (IDS): Yes □ No □

   a. Areas and critical assets that the IDS covers (Use chemical asset names identified above and nomenclature for your facility):

   ____

   ____

   ____

   b. IDS monitoring by: ______________________________

   c. IDS response by: ______________________________

   d. System backup power supply: Yes □ No □

      i. ______ hours of backup power available

      ii. If no backup power, are there other compensatory measures?
      Yes □ No □
      If yes, describe: ______________________________

      ____

   e. Hours of active IDS monitoring: ______________________

   f. Types of sensors (Select all that apply):
   □ Fence-mounted sensors
   □ Wall-mounted sensors
   □ Window-mounted sensors
   □ Volumetric sensors
   □ Beam sensors
   □ Gate/door sensors
   □ Counter-UAS/object-detecting sensors
   □ Other (Describe): ______________________________

   ____

2. Camera system: Yes □ No □

   a. Areas and critical assets that the camera system covers (Use chemical asset names identified above and nomenclature for your facility):

   ____

   ____

   ____

   b. Camera system monitored by: ______________________

   c. Camera system response by: ______________________

   d. Camera system backup power supply: Yes □ No □

      i. ______ hours of backup power available

ii. If no backup power, are there other compensatory measures?
Yes □ No □
If yes, describe: ______________________________
____

e. Camera system includes video motion detection: Yes □ No □

f. Camera system is integrated with IDS: Yes □ No □
If yes, describe:______________________________
____

3. Employees and on-site security personnel

a. The facility has on-site security personnel: Yes □ No □

i. Hours security personnel are on-site: ______________________________

ii. Locations where security personnel are posted (Use chemical asset names identified above and nomenclature for your facility):
____
____
____

iii. Frequency of roving patrol: ______________________________

b. Employee presence

i. Hours employees are on-site: ______________________________

ii. Locations with employee presence (Use chemical asset names identified above and nomenclature for your facility):
____
____
____

iii. Employee training includes:

1. Security awareness training: Yes □ No □

2. Personnel detection training: Yes □ No □

4. Security lighting

a. There is sufficient lighting on asset areas for security equipment (i.e., camera systems, fencing, IDS, etc.): Yes □ No □

b. Lighting coverage areas:

i. Interior (Describe): ______________________________
____
____

ii. Exterior (Describe): ____
____
____

c. Security lighting backup power supply: Yes □ No □

i. ______ hours of backup power available

ii. If no backup power, are there other compensatory measures?
Yes □ No □
If yes, describe: ____
____

5. Chemical product inventory

a. Frequency of inventory: ____

b. Inventory conducted by: ____

c. Inventory management system, if applicable: ____________________________
____

d. Discrepancies in inventory are reported to: ______________________________

Additional Security Measures

If gaps in detection capabilities were identified for any of the chemical assets listed in this section of this security plan, consider what additional security measures might be needed to close the identified gap. In this portion, identify specific security measures that your facility will plan to implement in the future to ensure detection.

Tip: Include a timeline and point of contact responsible to ensure accountability and project completion.

Delay

Delay means physically limiting access to the facility and/or asset(s) to reduce the likelihood of an adversary successfully breaching the facility perimeter and/or asset(s) or using the area immediately outside of the facility's perimeter to launch an attack.

Complete perimeter security is rarely attained through the deployment of a single security barrier; rather, an optimal security solution typically involves the use of multiple protective measures that provide layers of security. Layering of security measures can be achieved by incorporating different types of security measures (e.g., integrating physical protective measures—such as barriers, lighting, and electronic security systems—with procedural security measures—such as procedures guiding how security personnel should respond to an incident). When developing a layered security approach, facilities should consider how to use existing facility and natural features or other technologies applicable to the facility's circumstances to meet the performance objectives at a reduced cost.

Directions

- ▶ Assess how your facility currently provides delay capabilities and prevents unauthorized access.
- ▶ When you have identified the current security measures, compare them to the security principles laid out in Part 1, Section 4, Delay.
- ▶ Use this portion of the security plan to ensure each security measure is properly implemented and confirm whether it covers the chemical asset area.
- ▶ Identify any gaps in delay capabilities and any additional security measures that may be necessary to close those gaps.
- ▶ Develop a plan to implement any additional security measures.
- ▶ Consider your facility's operational hours when conducting this assessment and assigning security measures.

Notes

____

____

____

____

____

____

____

____

____

____

Delay Security Measures

1. Perimeter and asset barriers

    a. Defined perimeter and asset characteristics

        i. Type of perimeter and asset barriers (Use chemical asset names identified above and nomenclature for your facility) (Select all that apply):

Perimeter/Asset Name	Fence	Wall	Bollards	Berms	Ditches	Jersey Barriers	Other (Describe)
Ex. West perimeter	X				X		

ii. No trespassing/restricted area/private property signage posted: Yes □ No □

iii. Perimeter barrier coverage: Full □ Partial □ None □

iv. Asset barrier coverage: Full □ Partial □ None □

b. Access Points (Include all gates, doors, and other access points):

Access Point Name	Description	Type	Security Measure Details
Ex. Gate in west perimeter fence	Hinged gate in chain link fence	Gate	Gate is locked with padlock and chains

2. Physical locking mechanism

    a. Assets secured by:

Asset Name	Physical Locking Mechanism
Ex. Chlorine Storage Cage	Cage is locked with keyed padlock

b. Key and credential inventory

i. Frequency of inventory: ____

ii. Inventory conducted by: ____

iii. Discrepancies in inventory are reported to: ________________________

iv. Upon compromise/suspected compromise, locks are:
□ Rekeyed
□ Replaced
□ No action
□ Other (Describe): ____
____

v. Upon termination/departure of employees, keys/credentials are collected: Yes □ No □

3. Access control

a. Personnel identification program: Yes □ No □

i. Personnel identification conducted via:
□ Badges
□ Uniform
□ Other (Describe): ____
____

ii. Credential administration conducted by: __________________________

iii. Badges are required at the facility: Yes □ No □

iv. Visitor access: Yes □ No □
If yes, describe: ____
____

b. Access control system: Yes □ No □

i. If yes, type of access control system:
□ Proximity or smart card reader
□ Token/fob reader
□ Biometric reader
□ Personal access code
□ Common access code
□ Other (Describe): ____
____

4. Inspection and screening

a. Screening at access points: Yes □ No □

i. Personnel screening: Yes □ No □

ii. Electronic access control: Yes □ No □

b. Frequency of vehicle inspection: ____

c. Vehicle restrictions and parking restrictions: Yes □ No □
If yes, describe: ____
____

5. Shipping and receiving procedures

a. Know-your-customer program: Yes □ No □

b. Product stewardship program: Yes □ No □

c. Documentation of:

i. Sales and purchases to or from manufacturers: Yes □ No □

ii. Sales and purchases to or from third parties: Yes □ No □

iii. Confirmation of shipment arrival: Yes □ No □

d. Type of customer vetting (Describe): ____
____

e. Titles of procedures for controlling activities related to purchase and sale:
____
____

Additional Security Measures

If gaps in delay capabilities were identified for any of the chemical assets listed in this section of the security plan, consider what additional security measures might be needed to close the identified gap. In this portion, identify specific security measures that your facility will plan to implement in the future to ensure delay.

Tip: Include a timeline and point of contact responsible to ensure accountability and project completion.

Response

Response within the security plan context primarily refers to the response of appropriately trained personnel—either facility personnel or external first responders—to a threat to or actual theft, release, or sabotage of dangerous chemicals. However, it also includes mitigating the consequences of an incident and the reporting of suspicious behavior or a security incident internally and externally in a timely manner.

Due to the broad scope of this security goal, an appropriate response plan should then involve not only designated facility emergency response personnel, but also all facility personnel (including security personnel), local law enforcement, and other off-site first responders.

Response measures should address the identification of hazards, the corresponding response plans for those hazards, the number and capabilities of the various responders, and the equipping and training of the response personnel. Properly equipped personnel who understand the potential consequences of a security incident and the need for timely, effective actions, coupled with well-rehearsed response plans, reduce the probability of an attack achieving the adversaries' desired goals.

Additionally, practiced response plans help ensure that on-site responders and local law enforcement, fire, medical, emergency management, mutual aid, and rescue agencies are familiar with the facility and the chemicals stored on site and are not impeded from reaching the location of the security incident.

Directions

- ▶ Assess how your facility currently responds to the theft, release, or sabotage of dangerous chemicals.
- ▶ When you have identified the current security measures and plans in place, compare them to the security principles laid out in Part 1, Section 5, Response.
- ▶ Use this portion of the security plan to ensure each security measure is properly implemented and confirm whether it covers the chemical asset area.
- ▶ Identify any gaps in response capabilities and any additional security measures that may be necessary to close those gaps.
- ▶ Develop a plan to implement any additional security measures.
- ▶ Consider your relationships with local law enforcement and emergency planning committees.

Notes

____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____

Response Security Measures

1. Emergency response procedures and crisis management plan

    a. Emergency/security response organization and program: Yes □ No □

        i. Designated individual responsible for response: ______________________

        ii. Emergency management team:

Name	Title	Role in Response

    b. Crisis management plan: Yes □ No □

        i. Title: ______________________________________

        ii. Issue or revision date: ______________________________

iii. Plan includes (Select all that apply):
□ Contingency/continuity of operations (COOP)
□ Emergency response/shutdown/re-entry/evacuation
□ Media response
□ Security response plan
□ Post-incident actions
□ Other (Describe): ______________________________
____

c. Documented response agreements with off-site response services: Yes □ No □
If yes, titles of agreements: ______________________________
____

d. Response drills and exercises: Yes □ No □
If yes, frequency of drills and exercises: ______________________________

2. Outreach Programs

a. Information sharing/meet-and-greet

i. Dates for local law enforcement contact: ______________________________

ii. Dates for local fire department contact: ______________________________

iii. Dates for Local Emergency Planning Committee (LEPC) participation:
____

iv. Dates for contact with other officials (Specify the official): ____________
____
____

b. Joint initiatives and exercises (Describe): ______________________________
____
____

3. Security plans for elevated threats

a. Title of policy for elevated threats: ______________________________

b. Awareness of National Terrorism Advisory System (NTAS) bulletins and alerts:
Yes □ No □

c. Security measures increased during elevated threats: Yes □ No □
If yes, describe: ______________________________
____
____

d. Imminent threat alert (Describe): ______________________________
____
____

Additional Security Measures

If gaps in response capabilities were identified for any of the chemical assets listed in this section of the security plan, consider what additional security measures might be needed to close the identified gap. In this portion, identify specific security measures that your facility will plan to implement in the future to ensure response.

Tip: Include a timeline and point of contact responsible to ensure accountability and project completion.

Cyber

Because cyber systems and the network they operate on are often integrated throughout the operations of chemical facilities, defending against adverse cyber events is essential to the management of the overall risk for a facility. Facilities deter cyber sabotage and minimize the consequences of physical events through the protection of cyber systems. This includes preventing unauthorized access to critical process controls—such as Supervisory Control and Data Acquisition (SCADA) systems, Access Control Systems (ACSs), Distributed Control Systems (DCSs), Process Control Systems (PCSs), Industrial Control Systems (ICSs)—critical business systems, and other sensitive computerized systems. Facilities should consider how best to include comprehensive cybersecurity policies, practices, and personnel to handle adverse cyber events and mitigate their effects.

Directions

- For each cyber asset, describe the location at your site and how it is used.
- Assess how your facility currently provides cybersecurity capabilities and supports the prevention of unauthorized access to cyber systems.
- When you have identified the current security measures, compare them to the security principles laid out in Part 1, Section 6, Cybersecurity.
- Use this portion of the security plan to ensure each security measure is properly implemented and confirm whether it applies to the chemical asset area or system.
- Identify any gaps in cybersecurity capabilities and any additional security measures that may be necessary to close those gaps.
- Develop a plan to implement any additional security measures.
- Consider your facility's existing cyber systems—to include operational technology (OT) and information technology (IT)—as well as those systems connected to physical security systems, such as IDS or ACS, when conducting this assessment and assigning security measures.

Notes

Cyber Assets

Cyber System Type	Cyber Asset Name	Location and Description
Ex. SCADA system	ABC SCADA system for XYZ process	ABC SCADA system is connected to and controls the centrifuge mixing chemicals on machine #1.
Ex. Ordering and Inventory Management	123 Ordering	Located onsite and controls the ordering of all chemicals at the site as well as the management of inventory.

Cybersecurity Measures

1. Cybersecurity policies and procedures

   a. Change management process: IT and OT cultural and technical procedures to safeguard systems (e.g., adding devices, air gaps, etc.): Yes □ No □

   b. Security procedures for employees, system/vendor maintenance, and visitors/contractors using IT and ICS systems: Yes □ No □

   c. Procedures to audit/validate/verify cyber controls: Yes □ No □

   d. Procedures/contract to ensure system security and maintenance from third-party cyber support: Yes □ No □ N/A □

   e. Policies and procedures maintained by: ______________________________

   ____

2. Access control and password management

   a. Network accounts and access

      i. List of requested accounts and approved access: Yes □ No □

      ii. Unique accounts: List of privileged accounts (e.g., domain administrator, local admin): Yes □ No □

      iii. Least privilege: Process for granting only required system/data access: Yes □ No □

iv. Access control lists: Process for managing access for changing roles of employees (e.g., changing positions): Yes □ No □

v. Access control rules of behavior: Procedures describing IT user responsibilities and expected behavior: Yes □ No □

b. Password management

i. Procedures for changing default passwords: Yes □ No □

ii. Procedures for password rules: Yes □ No □

c. Physical access to cyber systems and information storage

i. Physical security in place to safeguard equipment from unauthorized access: Yes □ No □
If yes, describe: ______________________________
____

d. External connections

i. Managing connectivity and ability to transfer data (e.g., external access, wireless connections, etc.): Yes □ No □
If yes, describe: ______________________________
____

e. System boundaries

i. Policy for all IT technical assets and limiting system access points:
Yes □ No □
If yes, title of policy: ______________________________

3. Cybersecurity employee training and process

a. Cybersecurity awareness training is required for:
□ All personnel
□ Security personnel only
□ Other (Describe): ______________________________
____

b. Schedule/record of required cybersecurity training: Yes □ No □
If yes, maintained by: ______________________________

c. List of required training, procedures, and policies for new employees:
Yes □ No □
If yes, maintained by: ______________________________

d. Procedures for conducting and documenting training: Yes □ No □
If yes, maintained by: ______________________________

4. Cybersecurity controls, monitoring, response, and reporting

a. Intrusion detection or intrusion prevention system: Yes □ No □
If yes, describe: ____
____

b. Regular anti-malware software and other software updates: Yes □ No □

c. Procedures to manage lifecycle of IT and ICS system components from acquisition to disposal: Yes □ No □

d. Cybersecurity incident reporting (Select all that apply):
□ CISA Central (Central@cisa.dhs.gov)
□ Facility Cybersecurity Officer
□ Other (Describe): ____
____

5. Disaster recovery and business continuity

a. Audits to review compliance with facility's cybersecurity policies: Yes □ No □
If yes, frequency of audits: _______________________________________

b. Processes and procedures for (Select all that apply):
□ Backup and security storage information
□ Operating the control system environment in manual mode
□ Backup media
□ Network diagram
□ Testing
□ Other (Describe): ____
____

c. Processes and procedures maintained by: __________________________

Additional Security Measures

If gaps in cybersecurity capabilities were identified for any of the chemical assets listed in this section of the security plan, consider what additional security measures might be needed to close the identified gap. In this portion, identify specific security measures that your facility will plan to implement in the future to ensure cybersecurity.

Tip: Include a timeline and point of contact responsible to ensure accountability and project completion.

Policies, Plans, and Procedures

This section covers recommendations for maintenance of security equipment, training of personnel, employee background checks, incident reporting and investigation, security organization and officials, and recordkeeping.

Directions

- Assess the policies, plans, and procedures currently in place at your facility to manage security measures.
- When you have identified the current policies, plans, and procedures, compare them to the security principles laid out in Part 1, Section 7, Policies, Plans, and Procedures.
- Use this portion of the security plan to ensure each policy, plan, or procedure is properly implemented.
- Identify gaps in current policies, plans, and procedures for which additional policies, plans, or procedures may be necessary to close those gaps.
- Develop a plan to develop and implement any additional policies, plans, and procedures.
- For each item listed below, identify the name of the corresponding policy, plan, and procedure, and any pertinent information regarding its implementation.
- Consider including the plan for each item directly within this plan.

Notes

Policies, Plans, and Procedures to Implement Security Measures

1. Maintenance, inspection, and testing of security equipment program

   a. Maintenance policy: Yes □ No □

      i. Title of policy: ______________________________

      ii. Policy includes (Select all that apply):
      □ Procedures to mitigate failure of security systems/equipment
      □ Policy for reporting and correcting deficiencies
      □ Policy for reporting nonroutine outages, failures, and malfunctions
      □ Other (Describe): ______________________________
      ____

   b. Testing and inspection policy: Yes □ No □

      i. Title of policy: ______________________________

      ii. Policy includes (Select all that apply):
      □ Restricted areas/fence line
      □ Access doors/gates
      □ Vehicle barriers
      □ Lighting
      □ Locking mechanisms
      □ IDS
      □ Cameras
      □ ACS
      □ Other (Describe): ______________________________
      ____

2. Security awareness and training program

   a. Site Security Officer training includes (Select all that apply):
   □ Security laws/regulations
   □ Threats
   □ Duties/responsibilities
   □ Drills and exercises
   □ Inspection/screening methods
   □ Other (Describe): ______________________________
   ____

   b. Security personnel training includes (Select all that apply):
   □ Security threat/patterns
   □ Communications
   □ Emergency procedures/continency plans
   □ Operation of security equipment/systems
   □ Testing/calibration/maintenance of security systems
   □ Inspection/screening methods

□ Other (Describe): ____

____

c. All employees training includes (Select all that apply):
□ Recognizing suspicious activity/security incident
□ Reporting suspicious activity/security incident
□ Emergency procedures
□ Security systems/equipment operation
□ Other (Describe): ____

____

d. Training methods (Select all that apply):
□ Face-to-face
□ Online
□ Handouts/bulletin boards
□ Hands-on activities
□ Other (Describe): ____

____

e. Frequency of tabletop exercises:
□ Weekly
□ Monthly
□ Quarterly
□ Semi-annually
□ Annually
□ Biannually
□ Other (Describe): ____

f. Frequency of functional exercises:
□ Weekly
□ Monthly
□ Quarterly
□ Semi-annually
□ Annually
□ Biannually
□ Other (Describe): ____

g. Frequency of full-scale exercises:
□ Weekly
□ Monthly
□ Quarterly
□ Semi-annually
□ Annually
□ Biannually
□ Other (Describe): ____

3. Employee background checks

a. List of employees with access to chemicals: Yes □ No □
If yes, maintained by: ____

b. Employees with access to chemicals require:

i. Verification of identity: Yes □ No □
If yes, acceptable documents include: ________________________
____

ii. Verification of legal authorization to work (i.e., I-9, eVerify): Yes □ No □

iii. Criminal background investigation: Yes □ No □

iv. Other (Describe): ____
____

c. Adjudication of background checks completed by: ____________________

i. Disqualifying issues (Describe): ______________________________
____

ii. Adjudication completed on a case-by-case basis: Yes □ No □

4. Insider threat

a. Insider threat policy: Yes □ No □
If yes, title of insider threat policy: ______________________________

b. Insider threat program training: Yes □ No □

c. Procedures for reporting insider threat: Yes □ No □
If yes, maintained by: ____

5. Visitor escort

a. Visitor escort policy: Yes □ No □
If yes, title of visitor escort policy: ______________________________

6. Incident reporting and investigations

a. Process for incident reporting and investigations: Yes □ No □
If yes, title of policy for incident reporting and investigations: ____________
____

b. List of reported incidents: Yes □ No □
If yes, maintained by: ____

c. CISA Central (Central@cisa.dhs.gov) is included in reporting protocol:
Yes □ No □

7. Officials, organization, and records

a. Policy or chart for security organization: Yes □ No □

b. Policy for Facility Security Officer: Yes □ No □

c. Policy for retaining security records: Yes □ No □

Additional Security Measures

If gaps in policies, plans, and procedures were identified for any of the chemical assets listed in this section of the security plan, consider what additional policies, plans, and procedures might be needed to close the identified gap. In this portion, identify specific policies, plans, and procedures that your facility will plan to develop and implement in the future.

Tip: Include a timeline and point of contact responsible to ensure accountability and project completion.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA