****

**CISA Tabletop Exercise Package Chemical Sector**

[Enter Organization Name]

<Exercise Date>

Updated November 2023

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc151122158)

[Exercise Overview 5](#_Toc151122164)

[General Information 6](#_Toc151122165)

[Module 1 8](#_Toc151122166)

[Module 2 11](#_Toc151122167)

[Appendix A: Additional Discussion Questions 13](#_Toc151122168)

[Appendix B: Acronyms 17](#_Toc151122169)

[Appendix C: Case Studies 18](#_Toc151122170)

[Appendix D: Malicious Activity 19](#_Toc151122171)

[Appendix E: IT and OT Risk Mitigation…………………………………………………………………………………..20](#_Appendix_E:_IT)

[Appendix F: Contacts and Resources 22](#_Toc151122172)

# Handling Instructions

**Delete instructions that are not applicable.**

TLP:CLEAR

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):CLEAR*”: Recipients can spread this to the world; there is no limit on disclosure. This designation is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):GREEN*”: Limited disclosure, recipients can spread this within their community. This designation is used when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note: When “community” is not defined, assume the cybersecurity/cyber defense community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):AMBER”:* Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER+STRICT

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *“Traffic Light Protocol (TLP):AMBER+STRICT*: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that “*TLP:AMBER+STRICT”* restricts sharing to the organization only. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TLP:AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER+STRICT and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):RED*”: For the eyes and ears of individual recipients only, no further disclosure. This designation is used when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

# 

# Exercise Overview

|  |  |  |
| --- | --- | --- |
| Exercise Name | Exercise Name | |
| Exercise Date, Time, and Location | Exercise Date  Time (e.g., 9:00 a.m. – 12:00 p.m.)  Exercise Location | |
| Exercise Activities | Time | Activity |
| 20 Minutes | Threat Briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module 2 |
| 20 Minutes | Hotwash |
| Purpose | Examine the cyber resilience of <Chemical Sector Organization> in response to a significant cyber incident. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Examine the response capabilities of <Chemical Sector Organization> during a significant cyber incident. 2. Assess information sharing, notification, and coordination processes during a cyber-physical convergence incident. 3. Explore plans to recover critical systems. 4. Identify areas of improvement in cyber incident response plans and overall organizational resilience during and following a significant cyber incident. | |
| Threat or Hazard | Unmanned aircraft system (UAS), insider threat, Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA) system breach | |
| Scenario | A threat actor targets a system administrator through a UAS as an entry point into networks/systems. Attackers compromise information technology (IT) and operational technology (OT) networks. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact (POC) | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program (NCEP)**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) | | |

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”[[1]](#footnote-2)

## Using this Situation Manual

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. There are footnotes with corresponding resources throughout the modules to guide your preparedness efforts. The appendices provide the following information to tailor the exercise discussion:

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Reference section for acronyms used within this situation manual.
* Appendix C: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix D: An explanation of the malicious activity presented in this scenario.
* Appendix E: An overview of risk mitigation techniques for IT and OT systems.
* Appendix F: Additional cybersecurity preparedness and response resources.

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Players may include IT/information security, OT, physical security, and emergency management staff.

**Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise. Observers may include senior-level staff, such as organization management/leadership.

**Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

**Note-takers** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

## Exercise Structure

This exercise is intended to be a multimedia, facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module introduces several events, including a UAS threat alert and sighting, and an unknown Universal Serial Bus (USB) drive.
  + **Module 2:** This module includes an incorrectly installed update, unscheduled vendor visit, and disruptions to information technology (IT) and operational technology (OT) systems, resulting in loss of control of ICS/SCADA systems.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.
* Decisions are not precedent-setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
* There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

## Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions. The hotwash is held at the end of the exercise discussion. The hotwash is designed to provide an opportunity to discuss strengths and areas for improvement immediately following the conduct of an exercise.[[2]](#footnote-3)

# Module 1

### Day 1

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Federal Aviation Administration (FAA) release a joint report addressing increased unmanned aircraft system (UAS) activity near chemical sector facilities across the U.S. The report provides details on specific incidents, including a chemical plant that found a grounded drone with a memory card containing footage of the facility, and a drone operator caught taking photos of a pipeline.

In addition to hostile surveillance, smuggling, disruption, and weaponization, the report stresses adversaries may illegally use UAS as a mobile platform to interrupt or modify digital services or gain unauthorized access to data systems. The report encourages increased vigilance for UAS activity and directs chemical sector infrastructure owners and operators to report suspicious activity to their local FBI Field Office.

## Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired. Additional questions can be found in Appendix A.

1. What are the greatest cybersecurity threats to your organization?
2. What cybersecurity threat information does your organization receive?
   1. What threat information is most useful?
   2. How is information disseminated to the relevant parties within your organization?
   3. What actions would your organization take in response to the report like the one presented in the scenario?
3. Discuss your organization’s cyber resilience planning.[[3]](#footnote-4)
4. What risk assessments have you conducted to identify specific cyber threats, vulnerabilities, and critical assets?[[4]](#footnote-5)
5. Describe your asset management plan and how you prioritize critical assets.
6. What improvements have you implemented to enhance cyber resilience following recent risk assessments?
   1. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[5]](#footnote-6)

### Day 2

Your IT department authorizes the installation of an “automated software update” on one of your critical systems.

1. Describe your organization’s network configuration and your approach to network segmentation of IT and OT systems.
   * + - 1. Describe your organization’s patch management and vulnerability management plans.

### Day 3 – 5:00 a.m.

Your organization’s security team receives a report from an employee who observed a drone appear to drop something near your facility’s central building before losing sight of it. Soon after, the IT department notices a new Media Access Control (MAC) address associated with a known UAS manufacturer attached to their network and narrows its location to inside the perimeter.

1. What UAS detection capabilities and techniques does your organization employ at your facility?
   1. How would your organization respond if an unrecognized UAS lands within your facility perimeter?
   2. How would physical security and IT security coordinate response?

### Day 3 – 6:00 a.m.

Upon arriving at one of your facilities, an employee picks up a USB drive with the company logo on a walkway within the facility perimeter.[[6]](#footnote-7) The employee connects the device to their company computer and opens a file with embedded links.[[7]](#footnote-8) They click one of the links and receive a “404 – Not Found” error message. After receiving the error message, they unplug the drive and throw it away.[[8]](#footnote-9)

1. What policies and procedures does your organization have to maintain the security of facilities, networks, and systems?
   1. What policies do you have regarding company-issued devices and removable media?
   2. Where are these policies and procedures documented?
   3. How is physical access managed?
   4. How is IT and OT access managed?
2. Describe your organization’s cybersecurity training program for employees.[[9]](#footnote-10)
   1. How often are employees required to complete this training?
   2. Describe the cross-training or the coordination between the IT and OT departments.
   3. What additional training is required for users with system administrator-level privileges?
   4. Does this training address removable media?
3. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?
   1. What IT and OT systems or processes are the most critical to your organization?
   2. Describe your organization’s asset management plan and how you prioritize critical assets.
   3. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
   4. How are insider threats integrated into your risk management efforts?
4. What tools (e.g., threat hunting, security audits) do you leverage as part of a proactive cybersecurity strategy? [[10]](#footnote-11)

### Day 6

Technicians responsible for monitoring the sensors on the chemical storage tanks notice anomalous readings. Upon inspection of the storage tanks and sensors, no specific cause of the anomalous readings is identified. The technicians replace the sensors and the readouts on the ICS/SCADA monitors return to normal.

1. How does your organization baseline network activity?[[11]](#footnote-12)
   1. How do you distinguish between normal and abnormal traffic?
   2. What are your next steps when abnormal activity is detected/reported?
   3. What Indicator of Compromise (IOC) feeds does your organization use?
2. How do employees report and log anomalous IT/OT activity?
   1. How does your IT/OT department respond to reports of widespread problems?
3. How do IT/OT and physical security teams coordinate their investigation into potential incidents impacting both physical and cyber security?

# Module 2

### Day 22

Staff discover a misconfigured firewall allows access to both IT and OT systems. Staff trace the issue to an incorrectly installed update.

### Day 23

An individual arrives at your facility and states they are a new employee from your ICS/SCADA device service vendor. The individual is allowed access to the facility. They connect their device to the facility’s network and multiple ICS/SCADA devices before leaving.

## Discussion Questions

1. What level of access do your third-party vendors have to your organization’s network?[[12]](#footnote-13)
   1. How often are third-party access rights and data logs reviewed?
   2. What mechanisms or processes are in place to prevent malicious activity?

### Day 24 – Morning

An alarm is triggered, notifying employees in the control room that sensors are malfunctioning. Staff hurry to the liquid chemical storage tanks and take manual readings. The readings reveal numerous abnormalities. While trying to make the adjustments at the control panels, staff realize every panel in the control room is unresponsive.

### Day 24 – Mid-morning

Additional staff are called to report to work as the facility attempts to go to manual operations. Upon arrival, staff cannot use their key cards to enter the facility, and closed-circuit television (CCTV) cameras are not working.

1. What are your procedures for addressing unresponsive ICS/SCADA control panels and nonoperational sensors?
   1. Where are these processes documented?
2. What redundant systems exist for when primary systems are compromised?
3. What alternative systems or manual processes do you implement to continue operations if a critical system is unavailable for a significant period?
4. Who can authorize use of alternate systems or procedures?
5. How long can you perform manual or alternate processes on your critical systems?
6. What resources do you have for additional staffing requirements?

### Day 24 – Afternoon

While conducting visual examinations of the chemical storage tanks, an employee notices one tank has a considerably lower volume than it had an hour ago. A system alarm alerts facility operators of several control valves opening and closing at random times. Attempts to close the valves via the ICS/SCADA controls do not work.

1. Using your organization’s cyber incident response plan (CIRP), describe the actions your organization would take to minimize impact on current operations.
   1. How does your plan define escalation criteria, notifications, activations, and/or courses of action?
   2. What guidance does the plan include on assessing the severity of the incident?
   3. How does incident severity level dictate response?[[13]](#footnote-14)
   4. How are critical systems and processes incorporated within your plan?
2. How does your CIRP/IT response plan incorporate OT incident response?
   1. Is your CIRP aligned with any OT incident response plans?
3. What information are you sharing internally (e.g., employees, leadership)?
4. What information are you sharing externally (e.g., customers, vendors)?
   1. What sector partners do you collaborate with before, during, and after a cybersecurity incident?
   2. What actions can your organization take to mitigate reputational impacts because of these incidents?
5. What legal and regulatory notifications are required based on the scenario?
   1. When would notifications be made and who is responsible for making the notifications?
6. Based on the discussion, what changes will you implement to increase the resilience of your organization against future attacks?

# 

# Appendix A: Additional Discussion Questions

The following section includes supplemental organizational resilience discussion questions designed to guide exercise play. Questions are aligned with the NIST functional areas and organizational roles and responsibilities. Exercise planners are encouraged to select additional, applicable discussion questions for the chosen scenario to bolster participant conversation. *This instructional paragraph, as well as undesired discussion questions, should be deleted.*

## Cyber Resilience

1. Discuss how cyber preparedness is integrated with your current all-hazards preparedness efforts.
2. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
   1. What were the most recent results and action items that followed?
3. Discuss your risk management strategy.
4. How is it developed/maintained?
5. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
6. Does your organization maintain a risk register that is consistently reviewed and discussed at an executive level?
7. Describe your organization’s review process for your cyber incident response plan (CIRP).
8. How is your CIRP integrated with other incident or emergency response/management plans?
9. How often is the CIRP reviewed?
10. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
11. How are updates to the plan communicated to department or agency employees?
12. Discuss your supply chain concerns related to your IT/OT infrastructure.
13. What cybersecurity language is included within third-party vendor contracts?
14. How do you evaluate the cybersecurity posture of your vendors?
15. How often are contracts reviewed?
16. How do your service level agreements address cyber incident notification?
17. What is your method for tracking and identifying firmware vulnerabilities in your network?
18. What processes do you have to ensure that your external dependencies (e.g., contractors, power, water, etc.) are integrated into your security and continuity planning programs?
19. How is the integrity of your critical data protected and validated?
20. What external entities have access to your data?
21. How would those entities report a compromise of their systems to your office?
22. What essential functions are impacted by the incidents described in the scenario?
23. If primary communications are compromised, how do you provide information to internal and external entities?
24. What policies and procedures does your organization use to decide when and how to restore backed-up data?
    1. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. What are your organization’s policies or procedures for IT account management?
2. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?
3. Describe your organization’s bring your own device (BYOD) policy.
4. Describe your organization’s employee off-boarding process.
5. Is this process coordinated with IT and Human Resources (HR)?
6. What additional actions are taken if the employee’s termination is contentious?
7. How does your organization retrieve all information system-related property during the employment termination process (e.g., authentication key, system administrator’s handbook/manual, keys, identification cards, etc.)?

## Incident Identification

1. Who would be notified of suspicious UAS activity at your facility and how would your response be coordinated?
   1. What information are you sharing with outside agencies and who coordinates that process?
   2. Who coordinates and authorizes information for release to outside agencies?
   3. What incident response plan(s) does your facility have for UAS encounters?
   4. What regulations and procedures must be followed?
2. How are cyber incidents reported within your organization?
3. What would trigger the reporting requirements established by regulation, state law, and/or organization policy?
4. What training do employees receive regarding reporting requirements and your cyber incident response plan?
5. What cybersecurity incident escalation criteria is defined in your cyber incident response plan?
6. Who is responsible and what actions would they take based on the scenario?
7. Who needs to be notified internally and externally according to the plan?
8. When would leadership be notified?
9. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
10. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
11. How often is your organization’s data reviewed?
12. How would you determine whether unauthorized manipulation of data occurred?

## Incident Response

1. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
2. At what point in the scenario would you contact law enforcement?
   1. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
3. Are IT/OT system owners’ contact information documented in your response plans to ensure the correct personnel can be reached during a cyber event?
4. What are the processes for contacting critical personnel outside of core hours?
5. How do you proceed if critical personnel are unreachable or unavailable?
6. How would an incident at vendor(s) affect your organization if they have access to your information?
7. What are the notification requirements to your organization for incidents?

## Recovery

1. When does your organization determine a cyber incident is over?
2. Who makes this decision?
3. What post-incident activities would your organization conduct?
4. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
5. What is the risk associated with reactivating critical business processes and systems?
6. Describe the process to completely rebuild these systems.
7. What factors do you consider when making these decisions?

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
2. What additional training and/or exercise requirements do you require for your incident response staff?
3. How often does your organization exercise its CIRP?
4. Who is involved in the exercises?
5. What external agencies are involved in the exercise?
6. How do your organization’s training and exercise efforts address both physical and cyber risks?
7. How often do senior staff/leadership participate in a cybersecurity exercise?

## Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?
2. How do these goals align with organizational objectives?
3. Describe your organization’s cybersecurity culture.
4. What cybersecurity training is required for senior leadership?
5. At what point would you activate your organization’s Security Operations Center/Emergency Operations Center?
6. What is your role during a cyber incident?
7. What information do you need to support your decision-making process?
8. What are the gaps in your cybersecurity workforce?
9. How does your organization recruit, develop, and retain cybersecurity staff?

## Public Information

1. Describe your organizational processes to respond to media reports and inquiries.
   1. How would you preserve and reinforce the public’s confidence and trust in your organization during a significant incident?
   2. Who is responsible/authorized to speak to the media?
2. What training do employees receive on reporting contact with the media?

## Legal

1. What is the role of the legal department during a cyber incident?
2. What issues need to be addressed based on the scenario?
3. What legal documents does your organization have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| BYOD | Bring Your Own Device |
| CCTV | Closed-Circuit Television |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| CTEP | CISA Tabletop Exercise Package |
| FAA | Federal Aviation Administration |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| ICS | Industrial Control System |
| IT | Information Technology |
| MAC | Media Access Control |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| OT | Operational Technology |
| POC | Point of Contact |
| SCADA | Supervisory Control and Data Acquisition |
| TLP | Traffic Light Protocol |
| UAS | Unmanned Aircraft System |
| USB | Universal Serial Bus |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

## Pipeline Ransomware Attack Led to Operational Shutdown

In May of 2021, the largest supplier of gasoline, diesel, home heating oil, and jet fuel in the United States experienced a cybersecurity attack that led it to shut down operations for five days. The shutdown created widespread impacts across the East Coast, leading to a regional emergency declaration in 17 states and the District of Columbia.[[14]](#footnote-15) The shutdown caused a fuel shortage, resulting in panic-buying and long lines at gas stations.

The pipeline company did not experience a direct cyber incident on their industrial control systems. An incident on its information technology systems, including the billing system[[15]](#footnote-16), and the loss of 100 gigabytes of data led to the decision to shut down operations during investigation and ensure operational systems were not impacted.[[16]](#footnote-17) An investigation revealed the ransomware group DarkSide accessed the pipeline IT network via a compromised VPN password from an inactive account. The password was reused on another website and likely stolen at that location.[[17]](#footnote-18) The company was notified of the data exfiltration when they received the ransom note. The pipeline company initially paid the $4.4 million ransom for a decryption key, and the FBI recovered approximately half of the ransom.[[18]](#footnote-19)

## Ransomware Attack Against Chemical Manufacturers

Two major U.S.-based chemical companies that make resin, silicone, and other materials, were the victims of a ransomware attack that disrupted operations and caused a “global IT outage” on March 12, 2019. Company computers could not connect to the network, displayed a blue screen error, and had their files encrypted.[[19]](#footnote-20)

Because the companies kept their manufacturing systems on separate networks, the attack primarily impacted corporate functions.[[20]](#footnote-21) One of the companies was forced to order hundreds of new computers and create new email accounts for numerous employees after the attack.

# Appendix D: Malicious Activity

## Unmanned Aircraft Systems

Unmanned Aircraft Systems (UAS) are aircrafts that operate without the possibility of direct human intervention from within or on the aircraft and can range from aircraft-size UAS to hand-size mini drones. While not all UAS use is illegal or malicious, UAS may be leveraged by threat actors to carry out malicious attacks as they are modifiable and can create anonymity through a degree of separation between the UAS and the operator. Drones are highly flexible in their usage and can approach undetected to sensitive areas and conduct surveillance to visually map physical security measures, intercept and access sensitive data, block communications, mimic Wi-Fi networks, and perform keylogging operations to steal sensitive passwords. For information on best practices to protect users from the threat of illegal use of UAS, see the resource list below.

### Additional Resources

* ChemLock: Drone Activity (<https://www.cisa.gov/resources-tools/resources/chemlock-drone-activity>)
* Protect Critical Infrastructure and Public Gatherings (<https://www.cisa.gov/topics/physical-security/be-air-aware/protect-critical-infrastructure-and-public-gatherings>)
* Homeland Security Information Network-Critical Infrastructure (HSIN-CI) Cybersecurity and C-UAS Portal (<https://www.cisa.gov/hsin-ci-uas-cybersecurity-and-c-uas-portal>)
* Interagency Security Committee Best Practices for Protecting Against the UAS Threat (<https://www.cisa.gov/resources-tools/resources/isc-best-practices-protecting-against-uas-threat>)
* Emerging Risks: The Cyber-Physical Drone Threat (<https://www.cisa.gov/sites/default/files/2022-12/summit-2022-emerging-risk-drones-508.pdf>)
* Chemical Sector UAS CTEP Situation Manual (<https://www.cisa.gov/sites/default/files/2023-01/chemical-sector-uas-threat-ctep-situation-manual-iseb-508-112022.docx>)

# Appendix E: IT and OT Risk Mitigation

## Boundary Protection

One of the most fundamental characteristics of a secure ICS network is the design and deployment of boundary protection. Boundary protection is the electronic division between ICS and enterprise networks. If boundary protection is not developed thoroughly, access to ICS networks can be manipulated via enterprise networks and other internet connected devices. Inadequate boundary protection can also make it difficult to detect unauthorized activity on ICS systems. To mitigate threats against network boundaries, limit the number of external network connections to the system; implement a managed interface for each external telecommunication service; deny network communications traffic by default and allow network communications traffic by exception; detect and deny outgoing communications traffic posing a threat to external systems; and enforce adherence to protocol formats. For more information on boundary protection refer to the resource below.

*Additional Resources*

* NIST SP 800-53, Rev. 5.1.1.: “System and Communications Protection (SC) – Boundary Protection”(<https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SC-07>)
* Layering Network Security Through Segmentation (<https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf>)

## Principle of Least Functionality

The principle of least functionality states that information systems should be configured to provide only essential capabilities and restrict or prohibit the use of non-essential functions, such as ports, protocols, and/or services that are not a key part of the industrial control system.[[21]](#footnote-22) Systems which are not structured using this principle have increased vectors for malicious parties to access. To implement the principle of least functionality, configure information systems to provide only essential capabilities; limit component functionality to a single function per device; disable any functions, port, protocol, and services that are deemed unnecessary; and identify and remove unauthorized/unsecure function, ports, protocol, services, and applications.

*Additional Resources*

* NIST SP 800-171, Rev. 3.0.0: “03.04: Configuration Management” (<https://csrc.nist.gov/pubs/sp/800/171/r3/final>)
* NIST Guide for Security Focused Configuration Management of Information Systems (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf>)

## Physical Access Control

Physical access to assets should be managed and protected. Unauthorized physical access to field equipment provides a malicious actor the opportunity to modify, delete, or copy critical device programs and firmware. Malicious actors can also gain access to ICS networks and steal or vandalize cyber assets. Additionally, unprotected physical access locations present threat actors with an opportunity to add rouge devices to capture and retransmit network traffic. To mitigate threats against physical access control locations, develop, document, and disseminate a physical and environmental protection policy; maintain a list of individuals with authorized access to the facility where ICS systems reside; enforce physical access authorization; control physical access; monitor physical access; maintain visitor access logs; and protect equipment for the ICS system from damage and destruction.

*Additional Resources*

* NIST Cybersecurity Framework, v2.0 (via NIST CSRC CPRT), PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk. (<https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AA-06>)
* Interagency Security Committee (ISC) Best practices for Facility Access Control (<https://www.cisa.gov/resources-tools/resources/isc-best-practices-facility-access-control>)
* Recommended Cybersecurity Practices for Industrial Control Systems (<https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf>)

# Appendix F: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact <https://www.secretservice.gov/contact/field-offices>, <https://www.secretservice.gov/investigation/cyber>)
* Federal Bureau of Investigation (FBI)
* Field Offices (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complain Center (IC3) (contact: [http://www.ic3.gov](http://www.ic3.gov/))
* National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov); 855-292-3937)

Chemical Sector Resources

* CISA Chemical Sector Resources (<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/chemical-sector>)
* Chemical Sector Risk Management Agency Fact Sheet (<https://www.cisa.gov/sites/default/files/publications/Chemical%2520SRMA%2520Fact%2520Sheet_508.pdf>)
* Chemical Sector Cybersecurity Framework Implementation Guidance (<https://www.cisa.gov/resources-tools/resources/chemical-sector-cybersecurity-framework-implementation-guidance>)
* Chemical Sector Playbook (<https://www.cisa.gov/resources-tools/resources/chemical-sector-playbook>)
* ICS/OT:
* CISA/Department of Energy Recommended Cybersecurity Practices for ICS: (<https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf>)

State Level Resources

* Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* National Governors Association (NGA) (<https://www.nga.org/>)
* NGA Center for Best Practices (<https://www.nga.org/bestpractices/divisions/hsps/>)
* DHS Fusion Centers (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)
* National Association of State Chief Information Officers (NASCIO) (<https://www.nascio.org/>)

Private Sector/Business Resources

* InfraGard (<https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf>)
* Internet Security Alliance (<https://isalliance.org/>)
* Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (<https://www.isao.org/information-sharing-groups/>)
* International Association of Certified ISAOs ([http://www.certifiedisao.org](http://www.certifiedisao.org/); contact: [operations@certifiedisao.org](mailto:operations@certifiedisao.org))
* National Council of ISACs ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

Preparedness Resources

* Cyber Security Evaluation Tool (CSET) (<https://www.cisa.gov/downloading-and-installing-cset>)
* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>)
* NIST Cybersecurity Framework Tools ([<https://www.nist.gov/cyberframework>](https://www.nist.gov/cyberframework))

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Standards and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. FEMA, “Homeland Security Exercise and Evaluation Program,” January 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-3)
3. NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST’s CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM-04> [↑](#footnote-ref-4)
4. NIST CSF 2.0 via CPRT, “ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.AM-05> [↑](#footnote-ref-5)
5. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model> [↑](#footnote-ref-6)
6. CISA – News & Events, “Using Caution with USB Drives,” <https://www.cisa.gov/news-events/news/using-caution-usb-drives> [↑](#footnote-ref-7)
7. NIST CSF 2.0 via CPRT, “DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=DE.CM-03> [↑](#footnote-ref-8)
8. NIST CSF 2.0 via CPRT, “PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS-01> [↑](#footnote-ref-9)
9. NIST CSF 2.0 via CPRT, “PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AT-01> [↑](#footnote-ref-10)
10. CISA, “Cyber Resource Hub,” <https://www.cisa.gov/cyber-resource-hub> [↑](#footnote-ref-11)
11. NIST CSF 2.0 via CPRT, “PR.PS-01: Configuration management practices are established and applied,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.PS-01> [↑](#footnote-ref-12)
12. NIST CSF 2.0 via CPRT, “PR.AA: Identity Management, Authentication, and Access Control,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AA> [↑](#footnote-ref-13)
13. NIST CSF 2.0 via CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM-04> [↑](#footnote-ref-14)
14. Kevin Collier, Pete Williams, “Feds recover millions from pipeline ransom hackers, hint at U.S. internet tactic,” *NBC News,* June 7, 2021, <https://www.nbcnews.com/tech/security/u-s-recovers-millions-pipeline-ransom-because-hackers-mistake-n1269889>. [↑](#footnote-ref-15)
15. Natasha Bertrand et al., “Colonial Pipeline did not pay ransom to hackers, sources now say,” *CNN,* May 13, 2021, <https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html>. [↑](#footnote-ref-16)
16. Sean Michael Kerner, “Colonial Pipeline hack explained: Everything you need to know,” *TechTarget,* April 26, 2022, <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>. [↑](#footnote-ref-17)
17. Alexander Culafi, “Mandiant: Compromised Colonial Pipeline password was reused,” *TechTarget,* June 9, 2021, <https://www.techtarget.com/searchsecurity/news/252502216/Mandiant-Compromised-Colonial-Pipeline-password-was-reused?Offer=abMeterCharCount_var2>. [↑](#footnote-ref-18)
18. Collier, 2021. [↑](#footnote-ref-19)
19. Lorenzo Franceschi-Bicchierai, “Ransomware Forces Two Chemical Companies to Order ‘Hundreds of New Computers,’” *Vice*, March 22, 2019, <https://www.vice.com/en/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers>. [↑](#footnote-ref-20)
20. Edward Kovacs, “Major U.S. Chemical Firms Hit by Cyberattack,” *Securityweek*, March 25, 2019, <https://www.securityweek.com/major-us-chemical-firms-hit-cyberattack/>. [↑](#footnote-ref-21)
21. Georgetown University Information Security Office, “Least Functionality Guidelines,” “[https://security.georgetown.edu/config-mgt-policy/least-functionality-guidelines/#:~:text=The%20principle%20of%20least%20functionality%20provides%20that%20information,integral%20to%20the%20operation%20of%20that%20information%20system.st Functionality Guidelines | University Information Security Office | Georgetown University](https://security.georgetown.edu/config-mgt-policy/least-functionality-guidelines/#:~:text=The%20principle%20of%20least%20functionality%20provides%20that%20information,integral%20to%20the%20operation%20of%20that%20information%20system.)”. [↑](#footnote-ref-22)