Image of the outside of a chemical facility during sunset. Chemical Sector Cyber Tabletop Exercise

Situation Manual

[Insert Date]

**\*[Insert Caveat]\***

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 8:00 a.m. | 8:30 a.m. | Registration |
| 8:30 a.m. | 8:45 a.m. | Welcome and Participant Briefing |
| 8:45 a.m. | 8:55 a.m. | Objectives |
| 8:55 a.m. | 10:05 a.m. | Module One: Threat |
| 10:05 a.m. | 10:20 a.m. | Break |
| 10:20 a.m. | 11:30 a.m. | Module Two: Incident and Aftermath |
| 11:30 a.m. | 11:55 a.m. | Hot Wash |
| 11:55 a.m. | 12:00 p.m. | Closing Comments |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Chemical Sector Cyber Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX, planned for [insert exercise duration], and will focus on [insert scope].  This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP). |
| **Mission Area(s)** | Prevention, Protection, Mitigation, and Response [insert other Mission Areas] |
| **Capabilities** | Planning; Intelligence and Information Sharing; Risk Management for Protection Programs and Activities; Cybersecurity; and Public Information and Warning |
| **Objectives** | 1. Review intelligence and information sharing and dissemination processes in relation to a credible threat to domestic critical infrastructure owners / operators. 2. Assess information sharing capabilities with the public; sector partners; and federal, state, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures. 3. Discuss private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident and the coordination activities under the National Incident Management System (NIMS) with local, state, and federal agencies. 4. Discuss gaps and challenges in private sector stakeholders’ emergency preparedness plans and response procedures to a cyber-related incident. 5. [Insert additional exercise objectives, as necessary]. |
| **Threat or Hazard** | Cyber-Attack [insert additional threat vector, as necessary]. |
| **Scenario** | The Supervisory Control and Data Acquisition (SCADA) and / or business system(s) at a chemical facility is compromised by computer malware. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable] |
| **Participating Organizations** | [Please see Appendix A.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise Point of Contact (POC) (e.g., exercise director or exercise sponsor).] |

This page is intentionally left blank.

# General Information

## Exercise Objectives and Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

For additional information regarding core capabilities, please visit: <https://www.fema.gov/emergency-managers/national-preparedness/mission-core-capabilities>.

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Review intelligence and information sharing and dissemination processes in relation to a credible threat to domestic critical infrastructure owners / operators. | * Planning * Intelligence and Information Sharing * Public Information and Warning |
| Assess information sharing capabilities with the public; sector partners; and federal, state, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures. | * Planning * Intelligence and Information Sharing * Public Information and Warning |
| Discuss private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident and the coordination activities under NIMS with local, state, and federal agencies. | * Planning * Risk Management for Protection Programs and Activities |
| Discuss gaps and challenges in private sector stakeholders’ emergency preparedness plans and response procedures to a cyber-related incident. | * Planning * Intelligence and Information Sharing * Risk Management for Protection Programs and Activities |
| [Insert objective] | * [Insert capability aligned to each objective] |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

* **Players:** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
* **Observers:** 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.
* **Facilitator:** The facilitator provides situation updates and moderates discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Evaluators:** Evaluators are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

## Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following two modules:

* Module One: Threat
* Module Two: Incident and Incident Aftermath

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your jurisdiction’s/ organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

# Module One: Threat

## Scenario

## [Insert Location]

### [Insert Month, Day, Year]: [Time]

The [insert name of state or regional] Fusion Center has received updated intelligence analysis bulletins that express concern about the growing sophistication of and cooperation among groups involved in environmental, cyber, and economic terrorism.

The U.S. Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issues an alert stating that a software programmer has developed computer malware, which exploits a specific vulnerability, and can replicate itself over networks with vulnerable systems.

This malware appears to be very similar to Stuxnet, initially spreading indiscriminately; however, it is determined that this new malware includes a highly specialized payload that is designed to only target [insert your facility’s SCADA software program, i.e., Siemens] SCADA systems that are configured to control and monitor [insert your facility’s specific industrial processes].

The programmer deployed this malware on the open Internet without any particular target in mind, only the goal of maximum infection.

The media is reporting a cybersecurity scare of potential global proportions.

Several employees of [insert your facility name] use a company-owned laptop outside of the physical workspace. In particular, one employee frequently connects to a wireless network hotspot at a local coffee shop to check his / her social media accounts and personal email before work.

## Discussion Questions

1. Given the threat, what is the process by which your organization would receive intelligence and protective measure information?
   1. With which departments and / or agencies or other organizations would your organization communicate regarding the potential threat?
   2. Does your organization maintain a relationship with its CISA Protective Security Advisor (PSA) or CISA Cybersecurity Advisor (CSA)? If so, is there a rapid means of contacting them?
   3. Does your organization use the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) Chemical Sector portal?
   4. Is your organization subscribed to the DHS *Cyber Spotlight* newsletter?
2. What internal information sharing and dissemination processes does your organization currently have in place?
   1. Who are the key stakeholders or groups (e.g., sectors, agencies, associations) with whom your organization must communicate to protect its critical infrastructure assets?
   2. Does your stakeholder group currently have information sharing processes? Are they documented?
   3. In addition to notifications to industry and federal government stakeholders, when would your organization initiate notification procedures to local and state authorities?
   4. How does your organization prioritize internal and external notifications?
3. What information platforms, if any, does your organization currently use?
   1. Does your organization currently own an information sharing platform? If so, does it have collaboration capabilities or is it used more as an intelligence / information collection repository?
   2. Are the platforms used for cyber incidents and the platforms used for other types of emergencies different? Are there common elements?
   3. What other capabilities (e.g., document library, calendar, alerts, special tools) would allow your organization to share information and help protect its critical infrastructure assets?
   4. Are there any technological conditions that, if not met, would be “show-stoppers”?
   5. What restrictions regarding access to and dissemination of information affect the ability to share information within your organization and with its public and private stakeholders (e.g., protected critical infrastructure information [PCII], sensitive but unclassified [SBU], business confidential)?
4. How does your organization process the information it receives (e.g., formal reporting, rumors, social media) for further dissemination within the organization and to personnel?
5. What resources are used to disseminate information?
   1. What notification capabilities (e.g., alerts, emails, telecommunications, text messages, special tools) does your organization use to share information and to communicate the process for implementing protective measures?
   2. Are there technological barriers, legal considerations, or institutional sensitivities that might affect or limit information sharing?
6. Given current and established information sharing procedures, what types of official information are the most useful (immediate information versus analyzed information) to your organization?
   1. Does your organization perform independent analysis on information provided? If so, what does that analysis process look like?
7. If there is identified “suspicious behavior” observed at a chemical facility, how does the facility report this information locally and within the Chemical Sector?
   1. Are trends suspicious activities tracked across the Chemical Sector nationwide?
   2. Is your organization aware of the “If You See Something, Say Something™” campaign or the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)
8. Given evidence of a credible cyber threat to the Chemical Sector, does your organization review its cyber security protocols?
9. What protective security measures or recommendations, if any, will your organization employ following this cyber threat?
   1. Does your organization coordinate protective measure implementation with any other organization within the Chemical Sector, or with government entities, such as law enforcement agencies or the PSA / CSA?
   2. How are the protective measures put in place by the Chemical Sector communicated back to the government?
   3. How useful are the recommended protective measures provided in information bulletins and advisories distributed by DHS (e.g., a Joint Intelligence Bulletin [JIB])?

***Cyber Specific Activities***

1. Does your organization have policies or procedures to address cyber vulnerabilities or cyber threats?
2. What are the procedures and requirements for hardening / securing mobile devices (e.g., laptops, smartphones, and tablets)?
3. Is the security of these mobile devices ever tested (vulnerability scans, penetration tests, assessments)?
4. How often is the security tested on these mobile devices?
5. Is software installed on mobile devices that can be used to control or access your organization’s control system? What are the security procedures? Are there any security controls in place (such as encryption of the communication channel)?
6. Is operational information (system configuration files, network diagrams, training manuals, or archive data) stored on these devices? How is this information protected from unauthorized access?
7. If SCADA or ICS systems are compromised, do you have back up manual procedures for these systems?
8. If SCADA or ICS systems are compromised, what cascading impacts may occur both internally to your facility and externally to other stakeholder / community members?
9. How are the security policies relating to your mobile devices enforced?
10. When onsite, are mobile devices connected to the internal operations local-area network (LAN)?
11. What would be the impact of a lost or stolen device? How many devices are lost or stolen per year? What is the procedure for reporting a lost or stolen device?
12. Are there laptops that function as servers when offsite (e.g., file transfer protocol [FTP], web, file shares)?
13. Has there ever been a security-related incident involving mobile devices?
14. Does your company have a formal / informal policy or procedure pertaining to information technology (IT) account management?
    1. Do these policies or procedures include protocols / steps for establishing, activating, modifying, disabling, and removing accounts?
    2. Do these policies or procedures include protocols / steps for notifying IT account managers / administrators when users are terminated?
15. Does your company employ a formal sanctions process for personnel failing to comply with established information security policies and procedures? If so, has this been communicated to the employees, and how often?
16. Security awareness and training:
    1. Does your company provide basic cybersecurity awareness training to all your information system users (including managers and senior executives)? How often is this training provided?
    2. Is cybersecurity awareness training provided to new employees prior to them being able to access the information system?
    3. Does your company provide adequate security-related training to IT managers, system and network administrators, and other IT personnel having access to system-level software? How often do they receive the training?
17. Does your company terminate information system access upon termination of an individual’s employment?
18. Does your company retrieve all information system-related property (e.g., authentication key, system administration’s handbook / manual, keys, identification cards) during the employment termination process?
19. Does your company participate in the Enhanced Cybersecurity Services (ECS) program through DHS? Would participation in such a program be useful in this situation? If so, how would it be used?
20. Is your company a member of the Critical Infrastructure Cyber Community (C3) Voluntary Program through DHS?
21. Has your company implemented the *Framework for Improving Critical Infrastructure Cybersecurity* issued by the National Institute of Standards and Technology (NIST)? How does the framework help your company manage cybersecurity risks?

# Module Two: Incident and Incident Aftermath

## Scenario

## [Insert Facility Name and Location]

### [Insert Month, Day, Year]: [Time]

On the morning of the outbreak, an employee of [insert your facility name] connects his / her laptop to a wireless network hotspot at a local coffee shop. The employee frequently connects to this hotspot to check his / her personal email and social media accounts prior to work.

The malware (from an infected host connected to the wireless network) scans the local coffee shop subnet for vulnerable systems, propagating itself onto the employee’s laptop in a matter of seconds.

Later that morning, the employee briefly connects the laptop to the LAN at [insert your facility name] to download data for work-related purposes.

Within minutes, several systems are infected on [insert your facility name’s] network. The laptop is disconnected and unused for the remainder of the day, but the malware is already attempting to spread to other local subnets. Eventually, the primary control network is scanned, and vulnerable systems are exploited.

At some point, infected systems begin to propagate the malware outside of [insert your facility name] by scanning thousands of random IP addresses across the Internet, increasing overall network traffic severalfold. As a result of these activities, network system performance degrades significantly in the control system environment.

The mid-shift operator notices some apparent system slowness in reporting system health, device status, etc. The operator logs onto the system and begins performing manual checks. During this process, the operator notices that the screen flickers several times, but there is no other evidence of a problem. He continues to perform manual checks of the devices and equipment, confirming that everything seems to be running normally.

A technician at the internet service provider (ISP) for [insert your facility name] is aware of outbreaks of this particular malware and begins to check traffic logs for possible signs of contamination. ISP sends out an email alert to customers that appear to be infected before complaints are generated by other network providers. [Insert your facility name] received one of those emails but it does not get routed to the appropriate cybersecurity personnel until mid-afternoon.

A worker, who is verifying that all valves are in the “off” position, notices Valve #1 is “open”. According to company protocols, he reports the incident.

Half (50%) of the failsafe systems are triggered and begin to shutdown various processes. These shutdowns are accompanied by several effluent and / or gas releases that mandate reporting to the Environmental Protection Agency (EPA), state environmental officials, and local first responders. A hazardous materials emergency is declared, and the local media outlets begin to call asking for a statement.

Once the attack is realized, control system administrators need to contain and recover the environment at [insert your facility name]. they determine that the outbreak is isolated to the control networks. During the process, control data is lost, aspects of the SCADA operation are forced to manual overrides, and there is general loss of functionality in key services across the entire facility.

## Discussion Questions

***General Discussion Questions***

1. What are your organization’s information sharing responsibilities during the response to the incident?
2. What formal information sharing processes would your organization use at this point?
3. What resources are used to disseminate information?
   1. What notification capabilities (e.g. alerts, emails, telecommunications, text messages, special tools) does your organization use to share information and communicate protective measures implementation?
   2. Are there technological barriers, legal considerations, or institutional sensitivities that might affect or limit information sharing, such as religious customs that prohibit use of electronic communication during specific times?
      1. If so, how will threat-based alerts and notifications be distributed to community members who might not receive the latest alert through electronic communication methods?
4. What protective security measures will be employed at your organization following these cyber-attacks?
5. What measures would local law enforcement take at this time to protect your organization (e.g., improved cyber security, employee training, increased vigilance)?

***Cyber-Specific Activities***

1. What types of cybersecurity policies, plans, and / or protocols does your company have in place to detect, respond to, and recover from a cyberattack?
2. Who would your organization contact internally or externally about the incident?
3. What internal and external messages should be developed? How are they distributed?
4. What are the business implications of the scenario? How are they determined?
5. Would your organization contact customers? If so, how is your firm’s public relations department involved? What role would you have in shaping the messages for customers and media inquiries?
6. At what point is law enforcement contacted?
7. What protocols exist in your firm to address such an event?
   1. Are there detection, prioritization, and response capabilities?
   2. Do employees know what constitutes suspicious cybersecurity activities or incidents?
   3. Do they know what actions to take when one arises?
8. Would this incident trigger contact with regulators?
   1. When would your organization make contact?
9. If SCADA or ICS systems are compromised, do you have back up manual procedures for these systems?
10. If SCADA or ICS systems are compromised, what cascading impacts may occur both internally to your facility and externally to other stakeholders / community members?
11. Given the scenario, does your Emergency Action Plan (EAP) include measures for protecting the security of chemicals at your facility?
12. Who is responsible for ensuring the chemical security measures are met?
13. Given the scenario, does your notification to responders include information about the chemicals at your facility?
    1. Do you maintain a relationship with first responders as to what chemicals are at your facility?
    2. Do you know if they are able to adequately respond if an attack at your facility impacts those chemicals?
    3. Who else within the first responder community should be notified if the attack impacts those chemicals?
14. Are IT and business continuity planning (BCP) functions coordinated with physical security? Will they collaborate with public relations, human resources, and legal departments?

This page is intentionally left blank.

# Appendix A: Exercise Participants

| **Participating Private Sector Organizations** |
| --- |
| [Insert private sector participants] |
|  |
|  |
|  |

| **Participating Local Organizations** |
| --- |
| [Insert local participants] |
|  |
|  |
|  |

| **Participating State Organizations** |
| --- |
| [Insert state participants] |
|  |
|  |
|  |

| **Participating Federal Organizations** |
| --- |
| [Insert federal participants] |
|  |
|  |
|  |

| **Other Participating Organizations** |
| --- |
| [Insert other participants] |
|  |
|  |
|  |

This page is intentionally left blank.

# Appendix B: Reference List

## CISA Exercises Resources

* [Critical Infrastructure Exercises](https://www.cisa.gov/critical-infrastructure-exercises)
* [Cybersecurity Training & Exercises](https://www.cisa.gov/cybersecurity-training-exercises)
* [CISA Tabletop Exercise Package (Exercise-in-a-Box)](https://www.cisa.gov/publication/cisa-tabletop-exercise-package)

## Tools

***Active Shooter***

* [Active Shooter Preparedness](https://www.cisa.gov/active-shooter-preparedness)
* [Pathway to Violence Video](https://www.dhs.gov/pathway-violence-video)
* [Pathway to Violence Fact Sheet](https://www.cisa.gov/sites/default/files/publications/dhs-pathway-to-violence-09-15-16-508.pdf)
* [National Counterterrorism Center (NCTC) First Responder Toolbox](https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox)

***Insider Threat***

* [Insider Threat Fact Sheet](https://www.dhs.gov/publication/fact-sheet-insider-threat-mitigation-program)
* [Insider Threat Mitigation](https://www.dhs.gov/cisa/insider-threat-mitigation)
* [Insider Threat - Training & Awareness](https://www.dhs.gov/cisa/training-awareness)
* [Violence in the Federal Workplace: A Guide for Prevention and Response 2019](https://www.dhs.gov/publication/isc-violence-federal-workplace-guide)

## CISA Architecture

* [CISA’s Cybersecurity Division](https://www.dhs.gov/cisa/cybersecurity-division)
* [CISA’s Emergency Communications Division](https://www.dhs.gov/cisa/emergency-communications-division)
* [CISA’s Federal Protective Service](https://www.dhs.gov/topic/federal-protective-service)
* [CISA’s Infrastructure Security Division](https://www.dhs.gov/cisa/infrastructure-security-division)
* [Infrastructure Information Collection Division (IICD)](https://www.dhs.gov/cisa/iicd)
* [National Infrastructure Coordinating Center (NICC)](https://www.dhs.gov/cisa/national-infrastructure-coordinating-center)
* [Protective Security Coordination Division (PSCD)](https://www.dhs.gov/cisa/protective-security-coordination-division)
* [Sector Outreach and Programs Division (SOPD)](http://www.dhs.gov/sopd)
* [CISA’s National Risk Management Center](https://www.dhs.gov/cisa/national-risk-management)

## Fact Sheets

* [Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS) 1-7: Detection and Delay](https://www.dhs.gov/publication/cfats-detect-delay)
* [CFATS RBPS 8 – Cyber](https://www.dhs.gov/publication/cfats-rbps-8-cyber)
* [CFATS RBPS 12(iv) - Screening for Terrorist Ties](https://www.cisa.gov/sites/default/files/publications/fs-rbps-12iv-psp-508_1.pdf)
* [CFATS RBPS 15 and 16 – Reporting Significant Security Incidents](https://www.dhs.gov/publication/rbps-15-16-incidents-fs)
* [Government Emergency Telecommunications Service (GETS)](https://www.cisa.gov/sites/default/files/publications/GETS%20Factsheet_March%202017%20FINAL%20508C%20031617%20%28003%29.pdf)
* [Homeland Security Information Network - Critical Infrastructure (HSIN-CI)](http://www.dhs.gov/sites/default/files/publications/HSIN-Fact%20Sheet-Critical%20Infrastructure.pdf)
* [If You See Something, Say Something - Information and Public Display Materials](http://www.dhs.gov/see-something-say-something)
* [National Terrorism Advisory System (NTAS) Public Guide, April 2011](https://www.dhs.gov/xlibrary/assets/ntas/ntas-public-guide.pdf)
* [Nationwide Suspicious Activity Reporting Initiative (NSI)](https://nsi.ncirc.gov/documents/Nationwide_SAR_Initiative_Fact_Sheet_2014.pdf?AspxAutoDetectCookieSupport=1)
* [Protective Security Advisor (PSA) Program](https://www.cisa.gov/sites/default/files/publications/CISA%20Fact%20Sheet%20-%20PSA%20Program%20-%20508c_IAA%20Final.19MAR2020.pdf)
* [Technical Resource for Incident Prevention (TRIPWire)](https://www.cisa.gov/sites/default/files/publications/TRIPwire%20Fact%20Sheet.pdf)
* [Wireless Priority Service (WPS)](https://www.cisa.gov/sites/default/files/publications/Wireless%20Priority%20Service_March%202017_FINAL%20508C%20031617%20%28003%29.pdf)

## Doctrine and Training

* [CISA Security of Soft Targets and Crowded Places Resource Guide](https://www.dhs.gov/publication/securing-soft-targets-and-crowded-places)
* [Federal Emergency Management Agency (FEMA) – Emergency Management Institute](https://training.fema.gov/emi.aspx)
* [FEMA Independent Study Program](https://training.fema.gov/is/)
* [Security and Awareness Courses](https://training.fema.gov/is/cisr.aspx)
* [Homeland Security Exercise and Evaluation Program (HSEEP), January 2020](https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf)
* [Infrastructure Visualization Platform (IVP) (formerly Computer Based Assessment Tool (CBAT)](https://www.dhs.gov/infrastructure-visualization-platform)
* [Nationwide Suspicious Activity Reporting Training Courses](https://nsi.ncirc.gov/training_online.aspx)
* [National Infrastructure Protection Plan (NIPP) Overview](https://www.dhs.gov/cisa/national-infrastructure-protection-plan)
* [National Preparedness Goal (NPG), Second Edition, September 2015](https://www.fema.gov/media-library/assets/documents/25959)
* [National Response Framework (NRF), Fourth Edition,](https://www.fema.gov/media-library-data/1582825590194-2f000855d442fc3c9f18547d1468990d/NRF_FINALApproved_508_2011028v1040.pdf) October 2019
* [Private Sector Clearance Program (PSCP) for Critical Infrastructure](https://www.dhs.gov/publication/dhs-nppd-pia-020a-private-sector-clearance-program-critical-infrastructure)
* [Framework for Improving Critical Infrastructure Cybersecurity](https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11)

# Appendix C: Relevant Plans

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

# Appendix D: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **BCP** | Business Continuity Plan |
| **C3** | Critical Infrastructure Cyber Community |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **CSA** | Cybersecurity Advisor |
| **DHS** | U.S. Department of Homeland Security |
| **EAP** | Emergency Action Plan |
| **ECS** | Enhanced Cybersecurity Services |
| **EPA** | Environmental Protection Agency |
| **EPT** | Exercise Planning Team |
| **FTP** | File Transfer Protocol |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **ICS-CERT** | Industrial Control Systems – Cyber Emergency Response Team |
| **IP** | Improvement Plan |
| **ISP** | Internet Service Provider |
| **IT** | Information Technology |
| **JIB** | Joint Intelligence Bulletin |
| **LAN** | Local-Area Network |
| **NIMS** | National Incident Management System |
| **NIST** | National Institute for Standards and Technology |
| **NSI** | Nationwide SAR Initiative |
| **PCII** | Protected Critical Infrastructure Information |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SAR** | Suspicious Activity Reporting |

|  |  |
| --- | --- |
| **Acronym** | **Term** |
| **SBU** | Sensitive but Unclassified |
| **SCADA** | Supervisory Control and Data Acquisition |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **TTX** | Tabletop Exercise |

