

**CISA Tabletop Exercise Package Defense Industrial Base Sector**

[Enter Organization Name]

<Exercise Date>

Updated June 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc164241368)

[General Information 5](#_Toc164241374)

[Exercise Overview 8](#_Toc164241375)

[Module 1 9](#_Toc164241376)

[Module 2 11](#_Toc164241377)

[Appendix A: Additional Discussion Questions 13](#_Toc164241378)

[Appendix B: Case Studies 16](#_Toc164241379)

[Appendix C: Malicious Activity 17](#_Toc164241380)

[Appendix D: Contacts and Resources 19](#_Toc164241381)

[Appendix E: Acronyms 20](#_Toc164241382)

# 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>.

# 

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s (NCEP) 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)

The CTEP materials (<https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>), including this Situation Manual, are designed to support the planning and execution of a tabletop exercise. A tabletop exercise is a discussion-based exercise in response to a scenario intended to generate a dialogue of various issues, identify strengths and areas for improvement, and/or achieve changes in perceptions about plans, policies, or procedures.[[2]](#footnote-3) NCEP also offers facilitated CTEPs. If you are interested in NCEP assistance with the planning and execution of a facilitated CTEP, please contact [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov).

## Using this Situation Manual

This Situation Manual provides a scenario and accompanying discussion questions designed to identify strengths and areas for improvement, including understanding of plans, policies, and procedures. Any organization interested in conducting this exercise should have an understanding of both IT and OT networks and the use of cloud services and service providers, as applicable.

This Situation Manual is intended to be adaptable and editable. Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. The footnotes throughout the modules contain corresponding resources to guide your preparedness efforts, including the CISA Cross-Sector Cybersecurity Performance Goals (CPG).[[3]](#footnote-4) 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: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix C: An explanation of the threats presented in this scenario.
* Appendix D: Additional cybersecurity preparedness and response resources.
* Appendix E: Reference section for acronyms used within this situation manual.

## 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 personnel, emergency management personnel, human resources personnel, legal personnel, and any other personnel with a role in incident response.

**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 leadership, IT/information security personnel, emergency management personnel, legal personnel, and any other personnel without a role in incident response.

**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 a spear phishing incident targeting your employees with elevated system access. Later, employees report widespread system latency that impacts their ability to work.
  + **Module 2:** This module continues the scenario with several computers restarting unprompted. When they come back online, employees notice sensitive files and other information was deleted. The Department of Defense (DoD) Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Assessment team is prepared to engage as the incident unfolds.
* 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.[[4]](#footnote-5)

# 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 | To explore, assess, and enhance plans, procedures, and overall enterprise resilience in response to a significant cyber incident. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Discuss organizational resilience and response to threats targeting the defense industrial base (DIB) sector. 2. Examine plans, policies, and procedures for responding to a cyber incident. 3. Assess internal and external communications processes. | |
| Threat or Hazard | Cyber incident | |
| Scenario | A cyber threat actor targets your employees with a phishing email, gaining elevated access to your network/systems and stealing sensitive data. | |
| 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  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov)  DIBCAC Business Operations  DCMA\_7012\_Assessment\_Inquiry@mail.mil  DoD DIB Cybersecurity Program  [OSD.DIBCSIA@mail.mil](mailto:OSD.DIBCSIA@mail.mil) | | |

# Module 1

### Day 1

In the past year, state-sponsored cyber actors targeted small DIB suppliers in an attempt to disrupt defense-related production and acquire commercial secrets/proprietary information. The incidents resulted in unauthorized access to data and production shutdowns.

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the United Kingdom National Cyber Security Centre (NCSC) issued a coordinated cybersecurity advisory detailing the tactics, techniques, and procedures (TTPs) of these incidents, including gaining access to networks via spear phishing emails.[[5]](#footnote-6) The advisory urges the use of multi-factor authentication, keeping devices up to date and exercising vigilance.[[6]](#footnote-7)

## Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your cyber 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. Does your organization participate in any of DoD’s cybersecurity services?[[7]](#footnote-8)
   2. What services or threat information is most useful?
   3. How is information disseminated to the relevant parties within your organization?
   4. What actions would your organization take in response to an advisory like the one presented in the scenario?
3. Discuss your organization’s cyber resilience planning.
   1. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[8]](#footnote-9)
4. Does your organization have a disaster recovery plan (DRP) and/or Cyber Incident Response Plan (CIRP)?
   1. How is your DRP/CIRP integrated with other incident or emergency response/management plans?

### Day 11

An employee with elevated system access receives an email stating all federal and DoD contract employees are required to view the “DoD Reporting and You” training and fill out a self-report addendum to their SF-86 form by following a provided link. The employee clicks on the link, enters their credentials to view the training, and submits the addendum.

1. 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 include phishing training and assessments?
2. 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. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
   3. What improvements have you implemented to enhance cyber resilience following recent risk assessments?
3. How does your organization mitigate insider threats?
   1. What are some behavioral indicators of an insider threat?
   2. What type of training do employees at your organization receive on identifying a potential insider threat?
4. Describe your organization’s asset management plan and how you prioritize critical assets.
5. Describe your organization’s patch management and vulnerability management plans.
   1. What processes does your organization use to evaluate and maintain an allowed list of patches?
   2. How does risk inform decisions regarding allowed hardware, firmware, and software?
   3. What considerations (e.g., extended downtime, loss of data, impaired functionality, etc.) are addressed in the plan’s risk management strategy?

### Day 24

Employees report experiencing system latency that is impacting their ability to perform assigned tasks. The investigation reveals a larger than normal amount of outbound traffic leaving your network.[[10]](#footnote-11)

1. How does your organization baseline network activity?
   1. How do you distinguish between normal and abnormal traffic?
   2. What are your next steps when abnormal activity is detected or reported?
   3. What indicators of compromise feeds does your organization use?

# Module 2

### Day 30

Screens on several computers go black as they reboot. When the computers restart, employees log on and notice multiple files are unavailable, including <files provided by the government marked Controlled Unclassified Information, customer names, contracts, research and development, patent, proprietary information>.

Later that day, screens go black again but do not reboot. Instead, they show a blank screen with a banner that reads, “encrypted.” Without access to the computers, business operations come to a standstill.

## Discussion Questions

1. Using your organization’s 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?
   4. How are critical systems and processes incorporated within your plan?
2. What are the legal and regulatory notifications required in this scenario?
   1. Which Defense Federal Acquisition Regulation Supplement (DFARS) based reporting requirements apply?
   2. When would notifications be made, and who is responsible for making the notifications?
3. What information are you sharing internally (e.g., employees, leadership)?

### Day 33

Partners/customers reach out to request details regarding the stolen data and your organization’s planned next steps. They state one of your employees warned them that data related to their contracts may have been compromised.

1. 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 caused by these incidents?

### Day 50

Post incident forensics confirm that attackers gained access to systems via stolen credentials. Once in the system, the malware initiated a worm that replicated and spread throughout the system, targeting, exfiltrating, and deleting multiple types of files.[[11]](#footnote-12)

### Day 60

### DoD requests the artifacts/evidence associated with the event to conduct a damage assessment after your organization reported the incident in accordance with DFARS 252.204-7012.[[12]](#footnote-13)

1. Is your organization prepared to provide images of all known affected information systems and all relevant monitoring/packet capture data?
2. How sufficient are your organization’s current internal resources for responding to the cyber incidents in this scenario?
   1. What additional resources outside of your organization are necessary for responding to the cyber incident?
   2. What are the processes or procedures for requesting additional resources?
   3. What external partners (e.g., DoD, CISA, FBI, incident response vendors) would you contact for assistance?
3. How do you determine a cyber event/incident is over?
4. Based on the discussion, what changes will you implement to increase the resilience of your organization against future incidents?

# 

# 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. Describe your organization’s review process for your CIRP.
7. How is your CIRP integrated with other incident or emergency response/management plans?
8. How often is the CIRP reviewed?
9. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
10. How are updates to the plan communicated to department or agency employees?
11. What cybersecurity language is included within third-party vendor contracts?
12. How do you evaluate the cybersecurity posture of your vendors?
13. How often are contracts reviewed?
14. How do your service level agreements address cyber incident notification?
15. How is the integrity of your critical data protected and validated?
16. What external entities have access to your data?
17. How would those entities report a breach of their systems to your office?
18. What essential functions are impacted by the incidents described in the scenario?
19. If primary communications are compromised, how do you provide information to internal and external entities?
20. 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 required 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 token, system administrator’s handbook/manual, keys, identification cards, etc.)?

## Incident Identification

1. How are cyber incidents reported within your organization?
2. What would trigger the reporting requirements established by federal regulation, state law, and/or organization policy?
3. What training do employees receive regarding reporting requirements and your cyber incident response plan?
4. What cybersecurity incident escalation criteria is defined in your CIRP?
5. Who is responsible and what actions would they take based on the scenario?
6. Who needs to be notified internally and externally according to the plan?
7. When would leadership be notified?
8. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
9. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
10. How often is your organization’s data reviewed?
11. 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. What are the processes for contacting critical personnel outside of core hours?
4. How do you proceed if critical personnel are unreachable or unavailable?
5. How would a compromise of vendor(s) affect your organization if they have access to your information?

## Recovery

* 1. When does your organization determine a cyber incident is resolved?

1. Who makes this decision?
2. What post-incident activities would your organization conduct?
   1. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
3. What is the risk associated with reactivating critical business processes and systems?
4. Describe the process to completely rebuild these systems.
5. 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/exercise requirements do you require for 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 exercises?
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 cybersecurity exercises?

## 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. What training do employees receive on reporting contact with the media?
      2. How do you build and maintain trust with the public?

## Legal

1. What is the role of the legal counsel during a cyber incident?
2. What internal (organizational) legal guidance documents does your organization have for clients to use in planning for and during cyber incidents?
3. What are some examples of documents that you might request your legal counsel to help draft or provide legal review for, in response to a cyber incident?

# Appendix B: Case Studies

## Threat Actors Target Cyber Activity Against US Defense Industrial Base

On September 7, 2023, Microsoft reported an increase in cyber activity from threat actors against the US defense industrial base. Microsoft noted that the activity for one such group included “resource development, collection, initial access, and credential access.”[[13]](#footnote-14) The threat groups, Circle Typhoon, Volt Typhoon, and Mulberry Typhoon, used multiple attack vectors, including zero-day exploits targeting small office and home network devices such as routers. Microsoft suggested mitigation strategies, including enforcing strong multifactor authentication, reducing attack surfaces, network monitoring, and closing or changing the credentials of compromised accounts.[[14]](#footnote-15)

## Third-Party Vendor Vulnerability Creates Leaks in UK Defense Sector

In August of 2023, threat actors with suspected links to a nation-state compromised the United Kingdom’s (UK) Ministry of Defense through a third-party vendor. Military data was stolen in a compromise of a third-party vendor responsible for security at multiple sensitive sites. The group responsible for this incident previously compromised other UK state institutions, including Scotland Yard and the postal service.[[15]](#footnote-16) The threat actor exploited known vulnerabilities in a legacy Windows 7 machine connected to the vendor’s network. Sensitive stolen data was posted on the Dark Web. The vendor reported they disrupted the incident and prevented the encryption of their server.[[16]](#footnote-17)

Threat Actors Target European Aerospace Company Suppliers

In 2019, a major European aerospace company was the victim of multiple cyber incidents via their suppliers. The threat actor targeted virtual private networks (VPNs) used by suppliers of the aerospace company in a series of incidents. The incidents resulted in unauthorized access to data, including the theft of documents related to military transport planes designed with one of the most powerful propeller engines in the world.[[17]](#footnote-18) The threat actors targeted weak links in the supply chain and compromised four suppliers via a shared VPN. A hacker using the name “USDoD” targeted the same aerospace company in 2023. The hacker gained access to company systems using a compromised account belonging to a Turkish airline employee. After obtaining the employee’s credentials via malware, the threat actor gained access to information on 3,200 people associated with the aerospace company’s vendors. Compromised data included names, job titles, addresses, email addresses, and phone numbers. The information was found on the Dark Web by a cybercrime firm, which notified the aerospace company.[[18]](#footnote-19)

# Appendix C: Malicious Activity

## Social Engineering and Phishing

One of the most prominent tactics cyber threat actors use to exploit network and system vulnerabilities is social engineering, defined as the manipulation of users through human interaction in order to compromise proprietary information. Common social engineering techniques involve the use of phishing, vishing, and smishing. Phishing uses email and/or malicious websites to solicit personal information or to trick individuals into downloading malicious software. Vishing uses voice communication to convince a victim to share sensitive information. Advanced vishing incidents can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity to be spoofed. Smishing uses SMS/text messages to send malicious links, email addresses, and phone numbers.

Social engineering is effective for compromising networks and evading intrusion detection systems without leaving a log trail. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, including training personnel to be cautious of suspicious emails, providing instruction on where to forward them, and keeping software and systems up to date. Organizations can also implement software designed to safeguard sensitive information, detect unsafe URLs, block phishing websites, detect known phishing and malware, and implement Multi-Factor Authentication (MFA) to guard against the use of stolen credentials.

### Additional Resources

* Avoiding Social Engineering and Phishing Attacks

(<https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>)

* Phishing Guidance: Stopping the Attack Cycle at Phase One (<https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one>)

## Insider Threat

An insider threat is the potential for someone with authorized access or understanding of an organization to harm the organization. This cyber threat includes theft, espionage, violence, and sabotage of anything related to technology, virtual reality, computers, devices, or the internet. Unintentional threats are the non-malicious (accidental or inadvertent) exposure of an organization’s IT infrastructure, systems, and data that causes unintended harm to an organization. Intentional threats are malicious actions performed by insiders with malintent who use technical means to disrupt or halt an organization’s business operations, identify IT weaknesses, gain protected information, or otherwise further an attack plan via access to IT systems. This action can involve changing data or inserting malware or other pieces of offensive software to disrupt systems and networks. Successful mitigation of insider threats and insider threat programs requires the detection and identification of observable, concerning behaviors or activities and the subsequent implementation of measures to manage the risk of potential harmful actions.

### Additional Resources

* CISA Insider Threat Mitigation Guide (<https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide>)
* Insider Threat Mitigation (<https://www.cisa.gov/topics/physical-security/insider-threat-mitigation>)

# Appendix D: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* Department of Defense Cyber Crime Center (DC3); (877) 838-2174; dc3.dcise@us.af.mil
* Federal Bureau of Investigation (FBI)
* Field Offices (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complaint 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)

Defense Industrial Base Sector Resources

* Defense Industrial Base Cybersecurity Portal (<https://dibnet.dod.mil/>)
* Department of Defense Cyber Exchange (<https://public.cyber.mil/)>
* Department of the Air Force’s Blue Cyber Program (<https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/>)
* National Defense ISAC (<https://ndisac.org/>)
* National Defense Industrial Association (<https://www.ndia.org/events/2021/9/16/cybersecurity-for-small-and-medium-sized-businesses-project-spectrum)>
* NSA Cybersecurity Collaboration Center (https://www.nsa.gov/CCC/)
* Project Spectrum (<https://www.projectspectrum.io/)>

Preparedness Resources

* CISA Find Help Locally (<https://www.cisa.gov/audiences/find-help-locally>)
* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>)
* NIST Cybersecurity Framework Tools (<https://www.nist.gov/cyberframework>)
* NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (<https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final>)

Additional Resources

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

# Appendix E: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| BYOD | Bring Your Own Device |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| COOP | Continuity of Operations Plan |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| CTEP | CISA Tabletop Exercise Package |
| DFARS | Defense Federal Acquisition Regulation Supplement |
| DIB | Defense Industrial Base |
| DIBCAC | Defense Industrial Base Cybersecurity Assessment Center |
| DOD | Department of Defense |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| IT | Information Technology |
| MFA | Multi Factor Authentication |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| OT | Operational Technology |
| POC | Point of Contact |
| TLP | Traffic Light Protocol |
| TTP | Techniques, Tactics, and Procedures |
| VoIP | Voice Over Internet Protocol |
| VPN | Virtual Private Network |
| ZTA | Zero Trust Architecture |

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. “Homeland Security Exercise and Evaluation Program,” FEMA, February 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-3)
3. This document does not intend to map directly to any regulatory or contractual requirements to which members of this sector may be subject, nor is it intending to suggest that compliance with the CPGs would be sufficient to meet any such regulatory or contractual requirements. [↑](#footnote-ref-4)
4. FEMA, “Homeland Security Exercise and Evaluation Program,” January 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-5)
5. Joint Advisory, “Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-Phishing Campaigns,” <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a> [↑](#footnote-ref-6)
6. CISA CPG Checklist, “3.A – Detecting Relevant Threats & TTPs,” [<https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist>](https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist) [↑](#footnote-ref-7)
7. Defense Industrial Base Cybersecurity Portal, <https://dibnet.dod.mil/dibnet/#resources-resources-3> [↑](#footnote-ref-8)
8. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model> [↑](#footnote-ref-9)
9. CISA CPG Checklist, “2.I – Basic Cybersecurity Training,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-10)
10. NIST CSF 2.0, “DE.AE: Adverse Event Analysis,” <https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters> [↑](#footnote-ref-11)
11. NIST CSF 2.0, “Incident Analysis (RS.AN),” <https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters> [↑](#footnote-ref-12)
12. Department of Defense, DFARS 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting,” <https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.> [↑](#footnote-ref-13)
13. Microsoft, “Digital threats from East Asia increase in breadth and effectiveness,” *Microsoft Security,* September 7, 2023,<https://www.microsoft.com/en-us/security/business/security-insider/reports/nation-state-reports/digital-threats-from-east-asia-increase-in-breadth-and-effectiveness/?msockid=16d8f2809ac667381f37e6b59b76666a>. [↑](#footnote-ref-14)
14. Microsoft, “Volt Typhoon targets US critical infrastructure with living-off-the-land techniques,” *Microsoft Security*, May 24, 2023, <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>. [↑](#footnote-ref-15)
15. Krishi Chowdhary, “Pro-Russian Hackers Attack UK MoD, Leak Thousands of Sensitive Military and Defense Documents Online” *Tech Report*, September 4, 2023, <https://techreport.com/news/pro-russian-hackers-attack-uk-mod-leak-thousands-of-sensitive-military-and-defense-documents-online/>. [↑](#footnote-ref-16)
16. Michael Hill, “Russia-linked attackers hit UK Ministry of Defense, leak stolen data” *CSO Online,* September 4, 2023, <https://www.csoonline.com/article/650994/russia-linked-attackers-hit-uk-ministry-of-defence-leak-security-data.html>. [↑](#footnote-ref-17)
17. Council on Foreign Relations, “Compromise of Airbus suppliers,” <https://www.cfr.org/cyber-operations/compromise-airbus-suppliers>. [↑](#footnote-ref-18)
18. Eduard Kovacs, “Airbus Launches Investigation After Hacker Leaks Data,” *Security Week,* September 13, 2023,<https://www.securityweek.com/airbus-launches-investigation-after-hacker-leaks-data/>. [↑](#footnote-ref-19)