CISA Tabletop Exercise Package Open Source Software

[Enter Organization Name]

<Exercise Date>

Updated March 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

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	To test the effectiveness of cyber incident reporting in support of public-private coordination efforts during a major incident affecting a critical open source project.	
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 open source projects. 2. Familiarize stakeholders in public, private, and non-profit sectors with reporting processes and respective roles and responsibilities during a cyber incident stemming from a critical open source project. 3. Identify areas for improvement in incident reporting processes, policies, and procedures. 4. Examine response coordination efforts between public, private, and community stakeholders during a cyber incident.	
Threat or Hazard	Cyber Incident	
Scenario	A vulnerability is discovered in your open source community's toolchain. Before the patch is completed, cyber threat actors activate ransomware on your systems, causing widespread issues across the open source community.	
Sponsor	Exercise Sponsor	
Participating Organizations	Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.).	

Exercise Name	Exercise Name	
Points of Contact (POC)	Insert Organization POC(s) Contact Information	CISA National Cyber Exercise Program cisa.exercises@cisa.dhs.gov CISA Open Source Software Security OpenSource@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]

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. 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 in the modules contain corresponding resources intended 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 threats presented in this scenario.
- Appendix E: 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 personnel, open source users and contributors (software maintainers, project managers, contributors, developers), 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, open source users and contributors (software maintainers, project managers, contributors, developers), legal personnel, and any other personnel without a defined role in incident response.

[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.

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 vulnerability within your open source community's toolchain that leads to system compromises worldwide. Private and public sector organizations begin working with open source developers to create a patch.
    - **Module 2:** This module continues the scenario with delays in patch development followed by the activation of ransomware and media inquiries. Members of your open source community continue to lose services and suffer a distributed denial-of-service (DDoS) attack.
- 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]

[2] FEMA, "Homeland Security Exercise and Evaluation Program," January 2020, https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

Module 1

Day 1

A major critical infrastructure (CI) entity contacts the Cybersecurity and Infrastructure Agency (CISA) to report an intrusion and exfiltration of data.[3] The CI entity is not exactly sure how the intrusion occurred, and just when they think they have fixed the issue, the intruder seems to reappear and continue their data theft.[4]

Day 10

The investigation reveals a never-before-seen vulnerability of a component deep within your open source community's build toolchain.[5] It affects a core language library that underpins most of your ecosystem and enables remote code execution.

CISA notifies the open source project's Security Point of Contact.

Day 11

CISA notifies the open source project's Security Point of Contact. CISA and the Federal Bureau of Investigation (FBI) jointly release a threat alert related to the compromise.[6]

Day 14 - Morning

In response to the threat alert, additional CI entities perform internal investigations and begin reporting anomalous network activity to CISA.[7]

Day 14 - Afternoon

Minor disruptions to critical infrastructure services across the globe are being reported, but the cause is not publicly disclosed.

Private and public sector organizations begin working with open source developers to prioritize development of a patch.

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. When a government cybersecurity authority issues alerts, what actions does your community take?
    a. Do you or your community play a role in contributing to such alerts?

---

[3] NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST's CPRT, "RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RC.CO-04.
[4] NIST CSF 2.0 via CPRT, "DE.CM: Continuous Monitoring," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=DE.CM.
[5] NIST CSF 2.0 via CPRT, "DE.AE: Adverse Event Analysis," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=DE.AE.
[6] CISA, "Cybersecurity Alerts and Advisories," https://www.cisa.gov/news-events/cybersecurity-advisories.
[7] NIST CSF 2.0 via CPRT, "PR.PS-02: Software is maintained, replaced, and removed commensurate with risk," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.PS-02.

2. Discuss current information sharing protocols and forums.
    a. What capabilities can your open source community leverage to raise awareness of package vulnerabilities (e.g., to alert consumers to avoid compromised packages)?
    b. If the public sector assisted in amplifying such notifications, would you take advantage of that?
3. What is your community's process for responding to a vulnerability report, or for reporting a vulnerability to another open source project or community?
    a. Within your organization, who authorizes these actions and who is involved in the decision-making process?
    b. If you represent a package repository: do all packages clearly list their security point of contact?
    c. If you represent a package repository: does every maintainer for a package you distribute know who to contact for assistance (e.g., for taking down a malicious package or if their account gets hijacked)?
    d. How much of your organization's time or budget is spent managing these processes daily? Is this adequate?
4. What artifacts are made available to package consumers that provide evidence of your community's secure software development practices (e.g., Software Bill of Materials, build signing, commit signing, reviewer sign-off, automated test results)?
5. What are the roles and responsibilities of your community or package repository when there is a major cyber incident leveraging a vulnerability within a package in your community?

Module 2

Day 17

Developers working to fix the issue determine that it will take about a month to develop, test, and roll out the fix across all affected open source projects. Due to the nature of the vulnerability, the fix requires rebuilding/repackaging of downstream dependencies.[8]

Day 18 – Morning

A threat group publicly claims responsibility, activates ransomware to encrypt several CI entities, and demands payment to stop disruptions and prevent the release of sensitive information they also claim to possess.

Day 18 – Afternoon

Media inquiries bombard CI entities that are affected by the vulnerability. Media reports include a proof of concept for exploiting the vulnerability. Social media posts are critical of the open source community for introducing the vulnerability.

Day 23

Since the vulnerability is now widely known, the broader open source community tries to find a mitigation. A consensus is reached on social media that no work-around is possible that preserves required functionality.[9]

Day 40

Just before patch rollout begins, key maintainers within your open source community notice they have suddenly lost access to their project's service accounts, and some have also lost access to email accounts and other communication tools.

At the same time, the hosting provider for your community's package repository reports a DDoS attack that makes distribution of any fixes more difficult.

Discussion Questions

1. In this scenario, how would your community develop the mitigation and roll-out plan?
    a. Who would be involved in the fix development?
    b. Does your community have the capability to proactively identify and notify community members and other projects that depend on the compromised project?
    c. Who would coordinate the notifications to, or rebuilding of, affected downstream projects?
    d. Would you be able to assist CISA in determining if other public sector entities were affected?

[8] NIST CSF 2.0 via CPRT, "RS.MA: Incident Management," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.MA.
[9] NIST CSF 2.0 via CPRT, "RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RC.CO-04.

2. How would your community respond to this incident?
    a. What support resources are available to handle the additional workload?
    b. Think about the maintainers of indirectly affected projects within your community. What information (or instructions) do they receive, and how do they react?
    c. What steps might you take to address public feedback, questions, criticism, etc.?
3. How would your community mitigate the threats in this scenario?
    a. Does your package repository help protect maintainers against account takeover attacks? Is there more you can do?
    b. Are mitigations already in place to protect your community infrastructure against DDoS?
    c. Do you retain access or system logs that could help with incident response?
    d. Would you be able to coordinate a defense with other package repositories?
4. Do you know how your community handles account access restoration?
    a. If an account was hijacked and used to sign a malicious package, what could the package maintainer do? What could the community do to notify consumers?
    b. If you are the infrastructure operator receiving a request to restore access, how would you authenticate the request (e.g., to prevent social engineering attacks)?
    c. Are these processes clearly documented for your community?
    d. Since account recovery can be time-consuming, is this capability available to all members of your community, or only for certain members?
5. Would you request assistance from the public or private sector?
6. How did your priorities shift as Module 2 progressed?
7. How does your community document or disseminate best practices and lessons learned, once an incident is declared over?
8. Based on discussion, what changes would you implement to increase the resilience of your community?

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. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
    a. What were the most recent results and action items that followed?
2. Discuss your risk management strategy.
    a. How is it developed/maintained?
    b. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
3. Describe your organization's review process for your cyber incident response plan (CIRP).
    a. How is your CIRP integrated with other incident or emergency response/management plans?
    b. How often is the CIRP reviewed?
    c. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
    d. How are updates to the plan communicated to department or agency employees?
4. What cybersecurity language is included within third-party vendor contracts?
    a. How do you evaluate the cybersecurity posture of your vendors?
    b. How often are contracts reviewed?
    c. How do your service level agreements address cyber incident notification?
5. How is the integrity of your critical data protected and validated?
    a. What external entities have access to your data?
    b. How would those entities report a breach of their systems to your office?
6. What policies and procedures does your organization use to decide when and how to restore backed-up data?
    a. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?
7. What automated and manual methods of DDoS attack detection does your organization employ?
    a. Who is notified by the automated detection tools?
    b. How would your organization manually detect a DDoS attack?
    c. How often are these systems tested?
8. What edge network defenses has your organization acquired to reduce the risk of malicious traffic reaching its target?

Incident Identification

1. How are cyber incidents reported within your organization?
    a. What would trigger the reporting requirements established by regulation, state law, and/or organization policy?
    b. What training do employees receive regarding reporting requirements and your cyber incident response plan?
2. What cybersecurity incident escalation criteria is defined in your cyber incident response plan?
    a. Who is responsible and what actions would they take based on the scenario?
    b. Who needs to be notified internally and externally according to the plan?
    c. When would leadership be notified?
3. Discuss your organization's intrusion detection capabilities and analytics that alert you to a potential cyber incident.
    a. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
4. 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. Explain your organization's decision-making process regarding ransomware payment.
    a. Are ransomware policies/procedures included in your CIRP?
    b. Explain your organization's decision-making process regarding ransomware payment.
    c. Are ransomware policies/procedures included in your CIRP?
3. Using your Cyber Incident Response Plan (CIRP), describe the actions your organization would take to respond to the ransomware attack.
    a. How often is the CIRP exercised with incident response personnel?
    b. What guidance does the plan include on assessing the severity of the incident?
    c. How does incident severity level dictate response?
    d. How are critical systems and processes incorporated into your CIRP?
4. At what point in the scenario would you contact law enforcement?
    a. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
5. What are the processes for contacting critical personnel outside of core hours?
    a. How do you proceed if critical personnel are unreachable or unavailable?

Recovery

1. When does your organization determine a cyber incident is resolved?
    a. Who makes this decision?
    b. What post-incident activities would your organization conduct?

2. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
    a. What is the risk associated with reactivating critical business processes and systems?
    b. Describe the process to completely rebuild these systems.
    c. 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?
    a. What additional training and/or exercise requirements do you require for your incident response staff?
2. How often does your organization exercise its CIRP?
    a. Who is involved in the exercises?
    b. What external agencies are involved in the exercises?
3. Has your organization exercised its CIRP against a DDoS attack?
    a. What lessons learned or areas for improvement were identified?
4. How do your organization's training and exercise efforts address both physical and cyber risks?
5. 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?
    a. How do these goals align with organizational objectives?
2. Describe your organization's cybersecurity culture.
3. At what point would you activate your organization's Security Operations Center/EOC?
4. What is your role during a cyber incident?
    a. What information do you need to support your decision-making process?

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

Appendix B: Acronyms

Acronym	Definition
BYOD	Bring Your Own Device
CI	Critical Infrastructure
CIRP	Cyber Incident Response Plan
CISA	Cybersecurity and Infrastructure Security Agency
CPG	Cybersecurity Performance Goals
CSF	Cybersecurity Function
CTEP	CISA Tabletop Exercise Package
DDoS	Distributed Denial of Service
FBI	Federal Bureau of Investigation
HR	Human Resources
IT	Information Technology
NCEP	National Cyber Exercise Program
NIST	National Institute of Standards and Technology
POC	Point of Contact
TLP	Traffic Light Protocol

Appendix C: Case Studies

Log4j Vulnerabilities Create Unprecedented Impacts Worldwide

In November 2021, critical vulnerabilities were discovered in a widely used, open source Java-based logging framework. The vulnerability set allowed for remote code execution that could be exploited in Java installations worldwide. The vulnerabilities became a zero-day exploit, with an upgraded version made publicly available the day after the first exploit was observed. Mitigation and remediation required unprecedented levels of effort from individual organizations and the broader cybersecurity community. The Java Naming and Directory Interface lookup feature, incorporated into Log4j in 2014, introduced the vulnerable attack surface.

Log4j is considered an "endemic vulnerability" because vulnerable versions of Log4j will remain in systems for years to come. Organizations should have long-term capabilities to discover and upgrade vulnerable software to reduce the risks created by this endemic vulnerability, to include proactively monitoring for and upgrading vulnerable versions of Log4j, preventing the reintroduction of vulnerable versions of Log4j, and prioritizing applying software upgrades to avoid long-term exposure of vulnerable attack surfaces. All organizations are encouraged to report incidents resulting from Log4j exploitation to CISA or the FBI.[10]

Malicious Packages Uploaded to Software Repository

In March of 2024, an advanced persistent threat (APT) group uploaded four malicious Python software packages to Python Package Index, a repository of open-source software intended to aid developers of software programs. These malicious packages were intended to resemble legitimate, widely used Python packages. The malware was not executed by installation of the malicious package alone. The Japan Computer Emergency Response Team Coordination Center concluded the attacker ran the Python script that executes the crypt function on the target machine. This APT is also believed to be responsible for a similar attack in 2023 that used packages containing the malware Comebacker.[11]

.

[10] Cyber Safety Review Board, "Review of the December 2021 Log4j Event," July 11, 2022, https://www.cisa.gov/resources-tools/resources/csrb-review-december-2021-log4j-event.
[11] Shusei Tomonaga, "New Malicious PyPI Packages used by Lazarus," Japan Emergency Response Team, February 28, 2024, https://blogs.jpcert.or.jp/en/2024/02/lazarus_pypi.html#2.

Appendix D: Attacks and Threats

Ransomware

Ransomware is a type of malicious software designed to deny access to victims' data or systems through encryption with a key only known by the malicious actor who deployed the malware. Once encrypted, the ransomware directs the victim to pay the attacker, typically in the form of cryptocurrency. Ransomware typically spreads through phishing emails or by users unknowingly visiting an infected website. Ransomware and associated data breach incidents can severely impact business processes, leaving organizations unable to access data necessary to function. The economic and reputational impacts of ransomware and data extortion have proven challenging and costly for organizations of all sizes throughout the initial disruption and, at times, extended recovery. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

Additional Resources

- CISA Stop Ransomware Website (https://www.cisa.gov/stopransomware)
- CISA Stop Ransomware Guide (https://www.cisa.gov/resources-tools/resources/stopransomware-guide)
- Protecting Against Ransomware (https://www.cisa.gov/news-events/news/protecting-against-ransomware)

Appendix E: Contacts and Resources

Federal Government Contacts

- CISA (contact: 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)
  - National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; 855-292-3937)

Open Source Software Security Resources

- CISA Open Source Software Security (https://www.cisa.gov/opensource)
  - Open Source Software Security Roadmap (https://www.cisa.gov/sites/default/files/2024-02/CISA-Open-Source-Software-Security-Roadmap-508c.pdf)
  - Software Bill of Materials Resources (https://www.cisa.gov/sbom)
  - Securing the Software Supply Chain: Recommended Practices for Managing Open-Source Software and Software Bill of Materials (https://www.cisa.gov/news-events/alerts/2023/11/09/cisa-nsa-and-partners-release-new-guidance-securing-software-supply-chain)
  - Exploring Memory Safety in Critical Open Source Projects (https://www.cisa.gov/resources-tools/resources/exploring-memory-safety-critical-open-source-projects)
  - Principles for Package Repository Security (https://www.cisa.gov/news-events/alerts/2024/02/08/cisa-partners-openssf-securing-software-repositories-working-group-release-principles-package)
- CISA Secure by Design (https://www.cisa.gov/resources-tools/resources/secure-by-design)

Preparedness Resources

- CISA Cross-sector Cybersecurity Performance Goals (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)
- NIST Cybersecurity Framework Tools (https://www.nist.gov/cyberframework)

State Level Resources

- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; 518-266-3460)
- DHS Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)

Additional 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; contact: operations@certifiedisao.org)
- National Council of ISACs (https://www.nationalisacs.org)