

**CISA Tabletop Exercise Package**

**Local Governments**

[Enter Organization Name]

## <Insert Date>

Updated November 2023

## Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc144280811)

[Exercise Overview 5](#_Toc144280817)

[General Information 6](#_Toc144280818)

[Module 1 8](#_Toc144280819)

[Module 2 11](#_Toc144280820)

[Appendix A: Additional Discussion Questions 13](#_Toc144280821)

[Appendix B: Acronyms 16](#_Toc144280822)

[Appendix C: Case Studies 17](#_Toc144280823)

[Appendix D: Attacks and Threats 18](#_Toc144280824)

[Appendix E: Contacts and Resources 20](#_Toc144280825)

# 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 |
| 10 Minutes | Break |
| 60 Minutes | Module 2 |
| 20 Minutes | Hotwash |
| Purpose | Evaluate the cyber resilience of <local government> in the event of a cyber incident. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Examine <local government>’s preparedness to detect, respond to, and manage a cyber incident. 2. Identify areas of improvement in cyber incident response plans. 3. Explore internal and external information sharing processes during a cyber incident. 4. Improve overall organizational cyber resilience. | |
| Threat or Hazard | Cyber Incident | |
| Scenario | A threat actor targets <local government>’s employees through a phishing email as an entry point into networks/systems. Threat actors compromise devices and data using ransomware. Impacts are felt across multiple organizations as additional cyber incidents occur following the ransomware attack. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program (NCEP)**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) | | |

# General Information

## Building Resilience

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

## Using this Situation Manual

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

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Reference section for acronyms used within this situation manual.
* Appendix C: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix D: An explanation of the 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. Suggested players include representatives from the IT, communications, human resources (HR), and legal departments, and any personnel with real-world cyber incident response roles.

**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 representatives from the IT, communications, HR, and legal departments as well as leadership who do not have assigned real-world cyber incident response roles but may be involved in response efforts or have a need-to-know.

**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 facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module addresses the types of cybersecurity alerts that your local government may receive, a suspicious email, and a ransomware attack.
  + **Module 2:** This module includes additional cybersecurity incidents that impact operations throughout your local government.
* 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 local government’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.

# Module 1

### Day 1

The Cybersecurity and Infrastructure Security Agency (CISA) releases an alert regarding phishing campaigns targeting state, local, tribal, and territorial (SLTT) government networks. The phishing emails contain a malicious attachment that automatically installs ransomware. Threat actors gain access to the network and escalate privileges to obtain administrator rights without any action or authorization from the victims.

## Discussion Questions

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

1. What are the greatest cyber threats to <local government>?[[2]](#footnote-3)
2. Discuss <local government>’s cyber resilience planning.[[3]](#footnote-4)
   1. What risk assessments have you conducted to identify specific cyber threats, vulnerabilities, and critical assets?[[4]](#footnote-5)
   2. Describe <local government>’s asset management plan and how you prioritize critical assets.
   3. What improvements have been implemented to enhance cyber resilience following recent risk assessments?
   4. Does <local government> apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[5]](#footnote-6)
3. Describe your <local government>’s review process for your Cyber Incident Response Plan (CIRP).
4. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
5. How are updates to the plan communicated to relevant employees?
6. What cybersecurity threat information does <local government> receive?
   1. What cyber threat information is most useful?
   2. How is information disseminated across <local government> and by whom?
   3. What actions would <local government> take following an alert like the one presented in the scenario?

### Day 4

Employees in the <comptroller/treasurer/finance department> receive an email from human resources (HR) concerning new benefits for fiscal year <20XX>. The email instructs users to sign the document and send it back to HR by close of business to avoid any interruptions in benefits.

Some employees follow the instructions and submit their information, while others report the email as suspicious to the <information technology (IT) department/help desk>.

## Discussion Questions

1. Describe <local government>’s cybersecurity training program for employees.[[6]](#footnote-7)
   1. How often are employees required to complete this training?
   2. Is training required during employee onboarding before granting system/network access?
   3. What additional training is required for employees who have system administrator-level privileges?
   4. What type of training methods or approaches have you found most beneficial? What types of training methods have you found ineffectual?
2. How do employees report suspected phishing attempts or other possible cybersecurity incidents?
   1. What actions does the IT department take when suspicious emails are reported?

### Day 7

The IT department notices unusual traffic to an external internet protocol (IP) address via a hypertext transfer protocol (HTTP) port originating from HR’s payroll servers. The anomaly lasts only a few minutes before stopping abruptly. IT staff initiate an investigation into the anomaly.[[7]](#footnote-8)

## Discussion Questions

1. How does <local government> baseline network activity?
   1. How can you distinguish between normal and abnormal traffic?
2. What steps would the IT department take to investigate the unusual traffic from HR’s payroll servers to an external IP address?[[8]](#footnote-9)

### Day 27

Early in the workday, a number of employees report they cannot log into their <accounts> using their credentials.

Later that day, several workstations display a red screen with a countdown and the following message:

***“Every 24 hours there will be a new attack if <local government> waits to pay the equivalent of $250,000 in Bitcoin. Every 12 hours we will release more sensitive information for sale on the DarkWeb. Pay before the time runs out or your system will be wiped.”***

Due to the ransomware, the <employee payroll system> is not functioning, multiple <local government> facilities are reporting that Wi-Fi and Voice over Internet Protocol systems (VoIP) are unavailable, and constituents are calling to report online bill pay is not working.[[9]](#footnote-10)

## Discussion Questions

1. Explain <local government>’s decision-making process regarding ransomware payment.[[10]](#footnote-11)
   1. Are ransomware policies/procedures included in your CIRP?
   2. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.
   3. Describe the impact the sale or release of sensitive information or Personally Identifiable Information (PII) would have on your response and recovery activities.

# Module 2

### Day 28

Constituents are still unable to access bill-pay online or over the phone and the employee payroll system is still unavailable. Across facilities, desktop computers and Voice over Internet Protocol (VoIP) systems remain unresponsive.

### Day 29

A security researcher contacts <local government> regarding employee PII being advertised for sale on the Dark Web.[[11]](#footnote-12) The alleged threat actor’s account posts employee PII with captions indicating they “hit the jackpot“ and more PII will be for sale.

Discussion Questions

1. Using your CIRP, describe the actions <local government> would take.
   1. How often is the CIRP exercised with incident response personnel?
   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 into your CIRP?
2. What mission essential functions are impacted by the incidents described in the scenario?
3. What redundant systems exist when primary systems are compromised?
4. How long can you perform manual or alternate processes for your critical systems?
5. What security breach notification laws does your state have?
6. What capabilities and resources are required for responding to this scenario?[[12]](#footnote-13)
7. What additional resources outside of <local government> are necessary for responding to the cyber incident?
8. What are the processes or procedures for requesting additional resources?
9. What external partners (e.g., federal, state, local) would you contact for assistance?
10. What alternative communications methods are used if the primary method is inoperable?
    1. How often are these alternative communications methods tested?
11. Does <local government> have backups of vital records stored in a location separate from your primary working files/copies?[[13]](#footnote-14)
12. How frequently do you restore from backups?
13. How long do you keep copies of archived files backed up?
14. How long would it take to restore primary files from backups? Have you tested restoration from backups?

### Day 30 – Afternoon

The deadline for the ransom payment passed. Accounts remain locked, the payroll, bill-pay, and VoIP systems remain unresponsive, and data remains encrypted.

### Day 31

Multiple local media outlets run stories on the ransomware attack, with employees and residents expressing concern that <local government> does not prioritize their safety.[[14]](#footnote-15)

## Discussion Questions

1. Describe <local government>’s processes to respond to media reports and inquiries.
2. What pre-scripted messages exist for cyber incidents?
3. How is public messaging coordinated and disseminated during a cyber incident?
4. How would you preserve and reinforce the public’s confidence and trust in <local government> during a significant cyber incident?
5. When does <local government> consider a cyber incident to be over/closed?[[15]](#footnote-16)
6. Who makes this determination?
7. What post-incident actions or processes would be executed?
8. Based on the discussion, what changes will you implement to increase the resilience of <local government>?[[16]](#footnote-17)

# Appendix A: Additional Discussion Questions

The following section includes supplemental organizational resilience discussion questions designed to guide exercise play. 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 into your current all-hazards preparedness efforts.
2. How does <local government> integrate cybersecurity into the system development life cycle (i.e., design, procurement, installation, operation, and disposal)?
3. Discuss your supply chain concerns related to cybersecurity infrastructure.
4. What cybersecurity language is included within third-party vendor contracts?
5. How do you evaluate the cybersecurity posture of your vendors?
6. How often are contracts reviewed?
7. How do your service level agreements address cyber incident notification?
8. What level of access do your third-party vendors have to the <local government> network?
9. Describe your patch management plan.
10. What considerations (e.g., extended downtime, loss of data, impaired functionality, etc.) are addressed in the plan’s risk management strategy?
11. What is your method for tracking and identifying vulnerabilities in your network?
12. How are IT and business continuity functions coordinated with physical security?
13. What processes do you have to ensure that your external dependencies (e.g., contractors, power, water, etc.) are integrated into your security and continuity planning programs?
14. How is the integrity of your critical data protected and validated?
15. How would those entities report a breach of their systems to your office?
16. How does <local government> maintain availability of key assets (e.g., network connectivity, etc.)?
17. If primary communications are compromised, how do you provide information to internal and external entities?
18. What policies and procedures does <local government> use to decide when and how to restore backed-up data?
    1. How does <local government> incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. Describe your <local government>’s bring your own device (BYOD) policy.
2. What are <local government>’s policies or procedures for IT account management?
3. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?

## Incident Identification

1. How are cyber incidents reported within <local government>?
2. What would trigger the reporting requirements established by regulation, law, and/or organization policy?
3. What training have employees received regarding reporting requirements and your CIRP?
4. What cybersecurity incident escalation criteria are 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 is leadership notified?
8. Discuss <local government>’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
9. What type of hardware and/or software does <local government> use to detect and prevent malicious activity on your systems/network?
10. How often is <local government>’s data integrity reviewed? How would you determine whether unauthorized manipulation of data has occurred?

## Incident Response

1. What are the roles of your network operations center/security operations center during a cyber incident?
2. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
3. At what point in the scenario would you contact law enforcement?

## Recovery

1. What actions would <local government> take if IT/incident response staff could not confirm the integrity of your systems/data?
2. What is the risk associated with re-activating critical business processes and systems?
3. How long and costly would the process be to completely rebuild these systems?
4. 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?
   1. What additional training and/or exercise requirements do you require for your incident response staff?
2. How do <local government>’s training and exercise efforts address both physical and cyber risks?
   1. Have senior staff participated in a cybersecurity exercise?

## Senior Leaders

1. As a leader in <local government> what cybersecurity resilience goals have you set?
2. What cybersecurity training is required for senior leadership?
3. What is your role during a cyber incident?
4. What information do you need to support your decision-making process?
5. What are the gaps in your cybersecurity workforce?
6. How does your <local government> recruit, develop, and retain cybersecurity staff?

## Public Information

* + - 1. What training is provided to employees regarding reporting any contact with the media to the appropriate public information personnel?
      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?
2. What legal issues need to be addressed based on the scenario?
3. What legal documentation should <local government> have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| BYOD | Bring Your Own Device |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Framework |
| DHS | U.S. Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| HTTP | Hyper Text Transfer Protocol |
| HR | Human Resources |
| IP | Internet Protocol |
| IT | Information Technology |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| PII | Personally Identifiable Information |
| TLP | Traffic Light Protocol |
| VoIP | Voice over Internet Protocol |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

## Royal Ransomware Attack

The Royal ransomware group launched a ransomware attack against a large U.S. city in May 2023. The computer systems used by the police, fire department, courts, and libraries were compromised. The IT team immediately disconnected systems, services, and devices from the network to prevent the spread of the ransomware.[[17]](#footnote-18) The ransomware note sent to the city’s printers stated the group downloaded sensitive data from the city’s servers and promised to restore network access and keep the attack confidential if they paid the ransom. The investigation showed the ransomware group accessed the servers for three weeks prior to the ransomware attack and downloaded the personal information of over 27,000 people. The city sent letters to current employees, retirees, and their relatives notifying them that their names, Social Security numbers, dates of birth, and medical records were exposed. The City Council approved over $8 million to cover hardware, software updates, and incident response.[[18]](#footnote-19)

## Ransomware Attack and Secondary Data Leak

A large U.S. city declared a state of emergency in February 2023 after a ransomware attack resulted in network outages for the city’s systems. The city took its network offline to prevent the spread of the ransomware. Internal city government impacts included internet outages at City Hall and no access to payroll systems. Constituent facing processes normally handled electronically reverted to paper processes, slowing services such as filing police reports. Most services were restored within days of the attack, however some services such as city employee email and voicemail remained unavailable for three months following the initial attack. Two months after the initial attack, the ransomware group that claimed responsibility for the initial attack leaked additional PII and personal financial information of employees and residents on the Dark Web. The city never paid the ransom.[[19]](#footnote-20) City employees filed a class-action lawsuit against the city after the second data leak, claiming the city did not adequately protect their information.[[20]](#footnote-21)

# Appendix D: Attacks and Threats

## Ransomware

Ransomware is a type of malware that denies 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, so the victim can receive a decryption key. Ransomware typically spreads through phishing emails or by 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>)

## Social Engineering and Phishing

One of the most prominent tactics threat actors use to exploit network and system vulnerabilities is social engineering, which is the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing. Phishing is often executed via email or malicious websites that solicit personal information by posing as a trustworthy source. Social engineering is effective for compromising networks and evading intrusion detection systems without leaving a log trail, and it is completely dependent on the operating system platform. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the involvement of human emotions. Organizations should take steps towards strengthening employee cybersecurity awareness training by incorporating trainings on identifying suspicious emails, instructing personnel on how to report them, and emphasizing the importance of keeping software systems up to date.

### 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>)

## Threat Mitigation

Successful threat mitigation programs employ practices and systems that limit or monitor access across organization functions. CISA developed the Continuous Diagnostics and Mitigation (CDM) Program in 2012 to assist SLTT stakeholders with threat mitigation. The CDM program provides cybersecurity tools, integration services, and dashboards to participating .gov agencies to improve their cybersecurity posture. All qualifying SLTT stakeholders are eligible to apply for a no-cost .gov domain.

### Additional Resources

* Continuous Diagnostics and Mitigation (CDM) Program (<https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program>)
* .gov Domain Application (<https://get.gov/registration/>)

# Appendix E: Contacts and Resources

Federal Government Contacts

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

State Level Resources

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

Preparedness Resources

* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist>)
* NIST Cybersecurity Framework Tools ([<https://www.nist.gov/cyberframework>](https://www.nist.gov/cyberframework))
* SLTT:
  + State and Local Cybersecurity Grant Program (<https://www.cisa.gov/state-and-local-cybersecurity-grant-program>)
  + CISA CDM Program (<https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program>)
  + CISA Find Help Locally (<https://www.cisa.gov/audiences/find-help-locally>)

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](http://www.certifiedisao.org/); contact: [operations@certifiedisao.org](mailto:operations@certifiedisao.org))
* National Council of ISACs ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

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. NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST’s CPRT, “ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-02>. [↑](#footnote-ref-3)
3. NIST CSF 2.0 via CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM-04>. [↑](#footnote-ref-4)
4. NIST Cybersecurity Framework, v2.0 (CSF 2.0) via NIST’s CPRT, “ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.AM-05>. [↑](#footnote-ref-5)
5. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model>. [↑](#footnote-ref-6)
6. NIST CSF 2.0 via CPRT, “PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AT-01>. [↑](#footnote-ref-7)
7. NIST CSF 2.0 via CPRT, “DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=DE.CM-03>. [↑](#footnote-ref-8)
8. NIST CSF 2.0 via NIST’s CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM-04>. [↑](#footnote-ref-9)
9. NIST CSF 2.0 via CPRT, “PR.DS-11: Backups of data are created, protected, maintained, and tested,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS-11> [↑](#footnote-ref-10)
10. CISA, “Stop Ransomware,” <https://www.cisa.gov/stopransomware>. [↑](#footnote-ref-11)
11. NIST CSF 2.0 via CPRT, “RS.CO-03: Information is shared with designated internal and external stakeholders,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.CO-03>. [↑](#footnote-ref-12)
12. NIST CSF 2.0 via CPRT, “GV.RM: Risk Management Strategy – The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.RM>. [↑](#footnote-ref-13)
13. NIST CSF 2.0 via CPRT, “PR.DS-11: Backups of data are created, protected, maintained, and tested,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS-11>. [↑](#footnote-ref-14)
14. NIST CSF 2.0 via CPRT, “RS.CO-03: Information is shared with designated internal and external stakeholders,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.CO-03>. [↑](#footnote-ref-15)
15. NIST CSF 2.0 via NIST’s CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM-04>. [↑](#footnote-ref-16)
16. NIST CSF 2.0 via CPRT, “ID.IM: Improvements – Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM>. [↑](#footnote-ref-17)
17. Alanna Quillen, Larry Collins and Lili Zheng, “Dallas releases technology accountability report following ransomware attack,” *NBC DFW,* June 9, 2023, <https://www.nbcdfw.com/news/local/dallas-to-release-technology-accountability-report-following-ransomware-attack/3274570/>. [↑](#footnote-ref-18)
18. Ken Kalthoff, “Dallas pays millions for ransomware expenses after May attack,” *NBC DFW*, June 9, 2023, <https://www.nbcdfw.com/news/local/dallas-pays-millions-for-ransomware-expenses-after-may-attack/3313643/>. [↑](#footnote-ref-19)
19. Stephanie Sierra, “Did Oakland have right cyber insurance before the ransomware hack? Here’s what experts say,” *ABC7 San Franciso,* May 12, 2023,<https://abc7news.com/oakland-ransomware-attack-hacked-cyber-insurance-san-bernardino-county/13240537/#:~:text=Four%20months%20after%20the%20%22Play,Team%20no%20payment%20was%20made.> [↑](#footnote-ref-20)
20. Shomik Mukherjee,“Oakland hit with class-action lawsuit by city employees over ransomware attack,” *Easy Bay Times,* May 31, 2023, <https://www.eastbaytimes.com/2023/05/31/oakland-hit-with-class-action-lawsuit-over-ransomware-attack/>. [↑](#footnote-ref-21)