

**CISA Tabletop Exercise Package Elections – Vote by Mail**

[Enter Organization Name]

<Exercise Date>

Updated January 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc148090375)

[Exercise Overview 5](#_Toc148090381)

[General Information 6](#_Toc148090382)

[Module 1 8](#_Toc148090383)

[Module 2 10](#_Toc148090384)

[Appendix A: Additional Discussion Questions… 12](#_Toc148090385)

[Appendix B: Acronyms 15](#_Toc148090386)

[Appendix C: Case Studies 16](#_Toc148090387)

[Appendix D: Malicious Activity 18](#_Toc148090388)

Appendix E: Contacts and Resources 20

# 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 Schedule | Time | Activity |
| 20 Minutes | Threat briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module Two |
| 20 Minutes | Hot Wash |
| Purpose | Examine identification, protection, and response capabilities for cyber and physical security incidents impacting elections infrastructure. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess election officials' ability to identify, respond to, and recover from cybersecurity incidents. 2. Examine information sharing processes among state and local election officials. 3. Explore processes for sharing accurate elections information with the public. 4. Inform the development or refinement of policies, plans, and procedures to address threats and increase resilience among <state/county/municipality> elections infrastructure. | |
| Threat or Hazard | Cyber and physical security threats | |
| Scenario | * Disruptions of election infrastructure * Vote-by-mail is targeted to alter, disrupt, and destroy the voting process | |
| 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 info | **National Cyber Exercise Program CISA Exercises**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) | | |

# General Information

## Building Resilience

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

## Using this Situation Manual

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

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Reference section for acronyms used within this situation manual.
* Appendix C: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix D: An explanation of the malicious activity presented in this scenario.
* Appendix E: 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, elections, communications, and legal departments, and any personnel with real-world cyber incident response roles. Players should bring a copy of their Cyber Incident Response Plan (CIRP) and any other incident related plans, policies, and procedures to the exercise.

**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, elections, communications, human resources (HR), law enforcement, emergency managers, 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 introduces cybersecurity alerts and events targeting elections officials, including a phishing email, an unwanted program on users’ computers, and foreign influence operations and inaccurate information.
  + **Module 2:** The second module includes damaged and suspicious ballots, website defacements, protests, news media, and inaccurate information concerning elections.
* 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

### 70 Days Before Election

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) release a joint alert concerning an observed increase in attempts via phishing and malware to disrupt the vote-by-mail process. It also highlights foreign influence operations and disinformation targeting the security and integrity of vote-by-mail ballots to undermine trust in the outcome of the election.[[2]](#footnote-3)

### 43 Days Before Election

Election personnel receive an email containing an open public records request. The email demands immediate response to an attachment, accusing officials of not complying with previous open public records requests. Some employees report the email as suspicious, while others download and open the attachment.[[3]](#footnote-4)

### 41 Days Before Election

Employees notice an unusual program has appeared on their computers. The program appears to be a media player that was installed overnight.[[4]](#footnote-5)

### 35 Days Before Election

Employees notice printed test ballots are different from the electronic files.

That same day, errors to the <Chief Election Official’s> website are reported to your office. The web lookup tool for the locations where ballots can be dropped is inaccessible and only shows a blank screen when clicked.[[5]](#footnote-6)

### 23 Days Before Election

Voters throughout the state receive what appear to be their official vote-by-mail ballots. However, some ballots are missing candidates or list the incorrect party for candidates. Voters call their <local election office (e.g., County Clerk Office)> and/or the <State Chief Election Official’s> office to question the legitimacy of their ballots.

## 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 the elections process?
2. How do you identify cybersecurity threats and vulnerabilities affecting vote-by-mail processes?[[6]](#footnote-7)
   1. How does your organization identify and secure critical systems for vote-by-mail processes?
3. Discuss <state/county/municipality>’s cyber resilience planning.
   1. Describe <state/county/municipality>’s asset management plan and how you prioritize critical assets.
   2. What improvements have been implemented to enhance cyber resilience following recent risk assessments?
   3. Does <state/county/municipality> apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[7]](#footnote-8)
   4. How could the <state/county/municipality> use the CISA Zero Trust Maturity Model guide to help facilitate a gradual transition to this more secure type of environment?
4. What cybersecurity threat information does your <state/county/municipality> receive?
   1. What organizations do you receive threat information from?
   2. What cyber threat information is most useful?
   3. How is information disseminated across your organization and by whom?
   4. What actions would your organization take following an alert like the one presented in the scenario?
5. Describe your <state/county/municipality>’s cybersecurity training program for employees.[[8]](#footnote-9)
   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 are most beneficial?
6. 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?
7. How would unofficial ballots be managed?
   1. How would official ballots with printing errors be managed?
8. How would your <state/county/municipality> address incidents of official website defacement?[[9]](#footnote-10)
   1. Who manages the website?
   2. Are all of the state/county/municipality websites on a .gov domain?

# Module 2

### 16 Days Before Election

A large number of <mail-in, absentee, vote-by-mail> envelopes are returned to local election offices by the United States Postal Service. A manual review of the envelopes shows that several addresses are incomplete or incorrect.

Voters call and email your office asking when their ballots will be delivered.

### 13 Days Before Election

The incoming election mail for the day arrived at the election office damaged during transport. Postmarks for many of the envelopes are illegible. Additionally, your local post office representative contacts you stating they found voted ballots separated from their envelopes at several post offices.[[10]](#footnote-11)

### 7 Days Before Election

Voters using the <ballot tracking application name> application on the <Chief Election Official’s> website cannot confirm that their ballots were sent by the election office. Voters contact their election office for a replacement ballot. Soon local county offices are sending nearly as many replacement ballots as original ballots, and they begin to worry that they will not have enough ballots for voting locations on election day.[[11]](#footnote-12)

### Election Day – Morning

On Election Day, several <state/county/municipality> websites display inaccurate information regarding locations where ballots can be dropped off. The <State Chief Election Official’s> website is also defaced with an image of “Rigged20<XX>”. IT staff are initially unable to correct the website.[[12]](#footnote-13)

Protests take place at drop box locations throughout the state. The protesters block access to the boxes and refuse to let voters return their ballots unless they “provide proof of citizenship.” Media reports begin circulating about the protests.[[13]](#footnote-14)

### Election Day – Afternoon

As media coverage of the protests continues, media outlets report that <locations where ballots can be dropped off> caught on fire, destroying the ballots.[[14]](#footnote-15) At one county election office, as election employees processed mail ballots, an employee identified a suspicious white powder inside a ballot envelope. Some of the substance fell out of the envelope and came in contact with the election officials, mail processing equipment, and the ballot processing area.

## Discussion Questions

1. Using your CIRP, describe the actions <state/county/municipality> 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 are critical systems and processes incorporated into your CIRP?
2. How would you work through the incomplete ballot envelopes with incomplete or damaged address labels?
3. What are your procedures for correcting misprinted ballots?
4. How would you respond to the issue with the “Track Your Ballot” application?
   1. What is the backup process when there is an issue with the election website(s)?
   2. How quickly can it be deployed?
5. What capabilities and resources are required for responding to this scenario?[[15]](#footnote-16)
6. What additional resources outside of your organization would be necessary for responding to the cyber incident?
7. What are the processes or procedures for requesting additional resources?
8. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?
9. Describe your organizational processes to respond to the media reports and inquiries.[[16]](#footnote-17)
   1. How do you ensure the public has accurate elections information?
   2. How would you preserve and reinforce the public’s confidence and trust in your <state/county/municipality> during a significant incident?
10. What processes or procedures do you have to address the damage to ballot drop locations and the potentially missing ballots?
11. Describe your organizational process for handling suspicious mail at election offices.
    1. What is your protocol for identifying questionable mail pieces before they are opened?
    2. What is your procedure for handling questionable mail?
    3. What is your protocol for notifying law enforcement?
    4. Are these protocols and procedures outlined in your emergency response plan or continuity of operations plan?
12. What are your plans/procedures in the event of a protest at <location used in the scenario>?
13. Based on discussion, what changes will you implement to increase the resilience of the vote by mail process?[[17]](#footnote-18)

# 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 into your current all-hazards preparedness efforts.
2. How does <state/county/municipality> 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 <state/county/municipality> 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 network vulnerabilities?
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 plans?
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 <state/county/municipality> maintain availability of key assets (e.g., network connectivity, etc.)?
17. What is your organization’s communications PACE (primary, alternate, contingency and emergency) plan?
18. If primary communications are compromised, how do you provide information to internal and external entities?
19. What policies and procedures does <state/county/municipality> use to decide when and how to restore backed-up data?
    1. How does <state/county/municipality> incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. Describe your <state/county/municipality>’s bring your own device (BYOD) policy.
2. What are <state/county/municipality>’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 <state/county/municipality>?
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. When are other <state/county> offices notified?
9. Discuss <state/county/municipality>’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
10. What type of hardware and/or software does <state/county/municipality> use to detect and prevent malicious activity on your systems/network?
11. How often is <state/county/municipality>’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?
4. At what point would you contact the state’s chief election official (Secretary of State and/or State Election Director)?

## Recovery

1. What actions would <state/county/municipality> 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 <state/county/municipality>’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 <state/county/municipality> 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 <state/county/municipality> 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 <state/county/municipality> have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| EI-ISAC | Elections Infrastructure Information Sharing and Analysis Center |
| FBI | Federal Bureau of Investigation |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| SOS | Secretary of State |
| TLP | Traffic Light Protocol |

# Appendix C: Case Studies

## Vote By Mail Disputes

Lack of signatures on mail-in ballots in a state led to legal action by two candidates after elections in 2021 and 2022. The state law requires voters to fill out, date, and sign a declaration that they are qualified to vote. The form is found on the outside of the return envelope. The race for a Republican nomination for Senate, held in May of 2022, went into a recount that included undated mail-in ballots.[[18]](#footnote-19) The recount did not change the outcome of the race.[[19]](#footnote-20)

In November 2021, a candidate for a judgeship in a county in the same state lost the election by 75 votes. The results were disputed because 257 of the mail-in ballots were undated, which violated the state’s election code. The state’s Board of Elections voted to count the undated ballots—a decision later confirmed in state court. Plaintiffs then filed suit in federal court, arguing that the disputed ballots should be rejected. However, the court held that the ballots should be counted under the Civil Rights Act of 1964, which contains provisions created to ensure that qualified voters would not be disenfranchised by meaningless requirements that have nothing to do with their voting qualifications.

## Voting Tabulation System Installation Error

In November 2022, a voting tabulation system error caused double counting of votes in six voting districts within a county. The error led to a change in the outcome of a local school board race. A third-party vendor responsible for voting machine maintenance reinstalled the voting tabulation software in July of 2022. However, they failed to ensure that the Universal Serial Bus (USB) flash drives, containing votes, could only be uploaded once.[[20]](#footnote-21) The problem was not detected during the post-election audit of the system. The investigation into the voting results were only conducted because of an unrelated Board of Elections internal investigation.

## Fentanyl Letters Mailed to Election Offices Nationwide Highlight Potential To Disrupt Election Process

Letters containing fentanyl and other powders sent to election offices across the United States in early November 2023 temporarily disrupted ballot counting in several offices. This malicious use of the postal system is consistent with previous attempts to send letters with suspicious substances to election-related offices and other government buildings during past elections with the intent to intimidate workers or disrupt procedures. Prior to the November incidents, the most recent case occurred during an August 2023 state primary election, in which an election office received letters containing trace amounts of fentanyl. Suspicious letters containing white powder were mailed in early November to election offices across five states. At least four of the letters tested positive for fentanyl in preliminary tests and at least one of the letters contained baking soda, according to open-source reporting and the US Postal Inspection Service.[[21]](#footnote-22),[[22]](#footnote-23)

# Appendix D: 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, the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. A common social engineering technique involves the use of phishing. Phishing uses email, text messaging, and/or malicious websites to solicit personal information or to trick individuals into downloading malicious software. 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, to include 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

* Cybersecurity Toolkit and Resources to Protect Elections (<https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections>)
* Phishing Guidance: Stopping the Attack Cycle at Phase One (<https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one>)
* Avoiding Social Engineering and Phishing Attacks (<https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>)

## Mail Containing Toxins

Over the past two decades in the United States, multiple instances of attempted attacks against government officials and employees using toxic substances in mail. The toxic substances anthrax and ricin were used in these attacks. Anthrax is the spore form of a bacterium (an organism) that can be dried, purified, and made into a powder that can be inhaled. After anthrax spores are inhaled, they can become active, reproduce in the body, and cause disease. The spore can stay in the body for weeks before becoming active and causing illness, which is why antibiotics to prevent anthrax are administered for 60 days after a person is exposed. Ricin is a poison found naturally in castor beans. Ricin can be made from the waste material left over from processing castor beans and then purified and treated to form a powder that can be inhaled. Most ricin poisonings occurr when the ricin is injected or when the person swallowed ricin. Symptoms of ricin poisoning are most likely to occur within 4 to 12 hours if the ricin is inhaled or swallowed.

There were multiple instances of mail containing fentanyl sent to election offices in 2023. Fentanyl, similar to anthrax and ricin, presents a potential hazard to election officials handling mail. Fentanyl is a powerful synthetic opioid 50 to 100 times more potent than morphine.1 As little as two milligrams, about the size of 5 grains of salt, can cause negative health effects including trouble breathing, dizziness, and possible overdose. The election community should remain vigilant and exercise caution when handling the mail. Call 911 to report an immediate threat. Please report any threats or suspicious mail to the FBI, either through the local FBI Field Office or 1-800-CALL-FBI.

### Additional Resources

* United States Postal Inspection Service Election Mail Security Resources (<https://www.uspis.gov/election-mail-security>)

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>)
* United States Postal Inspection Service 24-hour National Law Enforcement Communications Center (contact: 877-876-2455; select option 4 for Election Mail issues)
* Federal Bureau of Investigation (FBI)
* Field Office Cyber Task Forces (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)

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))
* CISA Cybersecurity Toolkit and Resources to Protect Elections (<https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections>)
* CISA Guide to Operational Security for Election Officials (<https://www.cisa.gov/resources-tools/resources/guide-operational-security-election-officials>)
* 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>)
* Elections Infrastructure Information Sharing and Analysis Center (<https://www.cisecurity.org/ei-isac>)

Resources for State and Local Entities

* Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* National Governors Association (NGA) Resource Center for State Cybersecurity (<https://www.nga.org/statecyber/>)
* 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/>)

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>)

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. CISA Cybersecurity Alerts & Advisories, <https://www.cisa.gov/news-events/cybersecurity-advisories>. [↑](#footnote-ref-3)
3. 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-4)
4. NIST CSF 2.0 via CPRT, “ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-07>. [↑](#footnote-ref-5)
5. 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-6)
6. NIST CSF 2.0 via CPRT, “ID.RA-03: Internal and external threats to the organization are identified and recorded,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-03>. [↑](#footnote-ref-7)
7. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model>. [↑](#footnote-ref-8)
8. 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-9)
9. NIST CSF 2.0 via CPRT, “PR.IR-01: Networks and environments are protected from unauthorized logical access and usage,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.IR-01>. [↑](#footnote-ref-10)
10. 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>. [↑](#footnote-ref-11)
11. NIST SP 800-53 Rev. 5.1.1 via NIST CPRT, “CP: Contingency Planning,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=CP>. [↑](#footnote-ref-12)
12. NIST CSF 2.0 via NIST CPRT, “PR.IR-01: Networks and environments are protected from unauthorized logical access and usage,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.IR-01>. [↑](#footnote-ref-13)
13. NIST CSF 2.0 via CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM-04>. [↑](#footnote-ref-14)
14. NIST CSF 2.0 via CPRT, “RC.RP: Incident Recovery Plan Execution,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RC.RP>. [↑](#footnote-ref-15)
15. NIST CSF 2.0 via CPRT, “GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving,“ <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.RR-01>. [↑](#footnote-ref-16)
16. NIST CSF 2.0 via CPRT, “RS.CO: Incident Response Reporting and Communication,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.CO>. [↑](#footnote-ref-17)
17. NIST CSF 2.0 via CPRT, “ID.IM: Improvement,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM>. [↑](#footnote-ref-18)
18. N. Vigdor, “Pennsylvania’s G.O.P. Senate primary is officially headed to a recount*,” The New York Times*, May 25, 2022, <https://www.nytimes.com/2022/05/25/us/politics/oz-mccormick-pennsylvania-recount.html>. [↑](#footnote-ref-19)
19. T. Gabriel, “David McCormick Concedes to Dr. Oz in the G.O.P. Primary for Senate in Pennsylvania,” *The New York Times*, June 3, 2022, <https://www.nytimes.com/2022/06/03/us/elections/pennsylvania-senate-oz-mccormick.html>. [↑](#footnote-ref-20)
20. New Jersey School Board Association, “Monmouth County Election Offices: Error Could Change the Result in Ocean Township’s Board of Education General Election,” last modified January 18, 2023, <https://www.njsba.org/news-publications/school-board-notes/january-18-2023-vol-xl-no-22/monmouth-county-election-offices-error-could-change-the-result-in-ocean-townships-board-of-education-general-election/>. [↑](#footnote-ref-21)
21. Christina Cassidy, Ed Komenda, and Gene Johnson, “Election Officers are Sent Envelopes with Fentanyl or Other Sybstances,” *Associated Press*, November 9, 2023, <https://apnews.com/article/election-offices-letters-evacuations-fentanyl-threats-5d39155be4b2fcd5481b570cc109cb9c>.

    <https://apnews.com/article/election-offices-letters-evacuations-fentanyl-threats-5d39155be4b2fcd5481b570cc109cb9c> [↑](#footnote-ref-22)
22. “Fentanyl Letters Mailed to Election Offices Nationwide Highlight Potential to Disrupt Election Process,” Department of Homeland Security Office of Intelligence and Analysis, 30 November 2023. [↑](#footnote-ref-23)