



CISA
CYBER+INFRASTRUCTURE



ELECTIONS CYBER TABLETOP EXERCISE PACKAGE

Situation Manual

January 2020

Cybersecurity and Infrastructure Security Agency
Exercise Program



Elections Cyber Tabletop Exercise Package – Situation Manual

Table of Contents

Elections Cyber Tabletop Exercise Package – Situation Manual.....	2	Option C: Election Day/Voting Machines	24
Elections Cyber Tabletop Exercise Package Introduction.....	3	Section 3: Discussion Questions.....	31
Using this Document	3	Section 4: Exercise Appendices.....	49
Traffic Light Protocol Security Marking.....	4	Appendix A: Exercise Schedule	50
Scenario Selection.....	5	Appendix B: Acronyms	51
Section 1: General Information.....	6	Section 5: Informational Appendices.....	53
General Information.....	8	Appendix C: Background Information.....	54
Section 2: Exercise Overview and Scenarios	10	Appendix E: Cybersecurity Doctrine and Resources	56
Option A: Vote-by-Mail	11		
Option B: Early Voting/Same Day or Election Day Registration	18		

Tables

Table 1: <Exercise Date> Exercise Schedule	50
Table 2: Acronyms.....	51

Elections Cyber Tabletop Exercise Package Introduction

The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) designed the Elections Cyber Tabletop Exercise Package (ECTEP) Situation Manual (SitMan) as part of a strategic effort to increase stakeholder cyber exercise design capabilities.

The ECTEP focuses on the Tabletop Exercise (TTX) format. A Cyber TTX is intended to generate discussion of various issues regarding a hypothetical, simulated cyber incident. TTXs can be used to enhance general awareness, validate plans and procedures, rehearse concepts, and/or assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to, and recovery from a defined incident. Generally, TTXs are aimed at facilitating conceptual understanding, identifying strengths and areas for improvement, and/or achieving changes in perceptions.

A Situation Manual (SitMan) is a part of the core documentation needed for a TTX and provides the scenario narrative, discussion questions, and reference material for participants during exercise conduct.

The ECTEP SitMan is designed to align with the Homeland Security Exercise and Evaluation Program (HSEEP) guidance and exercise terminology. More information on HSEEP and exercise design can be found at: https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf.

Using this Document





The ECTEP SitMan can be customized by simply selecting the appropriate sections for your exercise, as outlined below, and deleting unneeded material. Additionally, exercise planners should complete all fields highlighted in yellow with information specific to their exercise and/or jurisdiction.

This SitMan contains five sections:

- [Section 1: General Information](#): include this section in all SitMans.
- [Section 2: Exercise Overview and Scenario](#): select one that best fits your exercise needs and fill in the fields highlighted in yellow.
- [Section 3: Discussion Questions](#): select additional questions to accompany your selected scenario (optional).
- [Section 4: Exercise Appendices](#): include appendices to enhance your situation manual as needed.
- [Section 5: Informational Appendices](#): select one or more appendices to provide additional background information for exercise participants (optional).

Traffic Light Protocol Security Marking

Traffic Light Protocol (TLP) was created to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipients.

Color	When should it be used?	How may it be shared?
 <p>TLP:RED Not for disclosure, restricted to participants only.</p>	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
 <p>TLP:AMBER Limited disclosure, restricted to participants' organizations.</p>	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.
 <p>TLP:GREEN Limited disclosure, restricted to the community.</p>	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
 <p>TLP:WHITE Disclosure is not limited.</p>	Sources may use TLP:WHITE 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:WHITE information may be distributed without restriction.

Chose which TLP designated sharing level best fits your exercise needs. Most exercises are conducted at the TLP:AMBER level to ensure that materials stay within the organization. Adjust the SitMan with the appropriate TLP markings in the right-hand upper and lower corners of the document.

Please consult the following website: <https://www.us-cert.gov/sites/default/files/tlp/tlp-v1-letter.pdf> to determine which marking is appropriate for your SitMan.

TLP:WHITE
TLP:GREEN
TLP:AMBER
TLP:RED

Scenario Selection

The following table provides an overview of each scenario to assist exercise planners in selecting the scenario that best fits their needs. If appropriate, you can take injects from one scenario and use it in another, but you must make sure that you include all necessary information for that inject (for example, if you take an inject from Option B module 2, make sure you also take any related injects from Option B module 1).

Scenario Overview Synopsis	
Option	Scenario
A	Vote-by-Mail Scenario : A threat actor attempts to interfere with vote-by-mail elections. After using phishing to penetrate state and local government systems, they attempt to redirect mailings, alter voter registration data, and deploy ransomware on networks to delay or discredit the election.
B	Early Voting/Same Day or Election Day Registration Scenario : A threat actor targets state and local election officials with a spear phishing campaign and gains access to election assets. Once inside, they attempt to modify voter registration data as well as interfere with legitimate voter registration by promoting fake websites during the whole registration period. Threat actors also deface election websites and install ransomware on host machines at state and local election offices. By modifying voter registration data and impacting the printing of pollbooks, election officials are inundated with an increase of election day registration/same day registration requests.
C	Election Day/Voting Machine Scenario : Threat actors deploy poisoned software updates in an attempt to access voting equipment and alter the vote count. In addition, threat actors conduct a social media campaign to encourage users to launch independent attacks against state and local government networks.

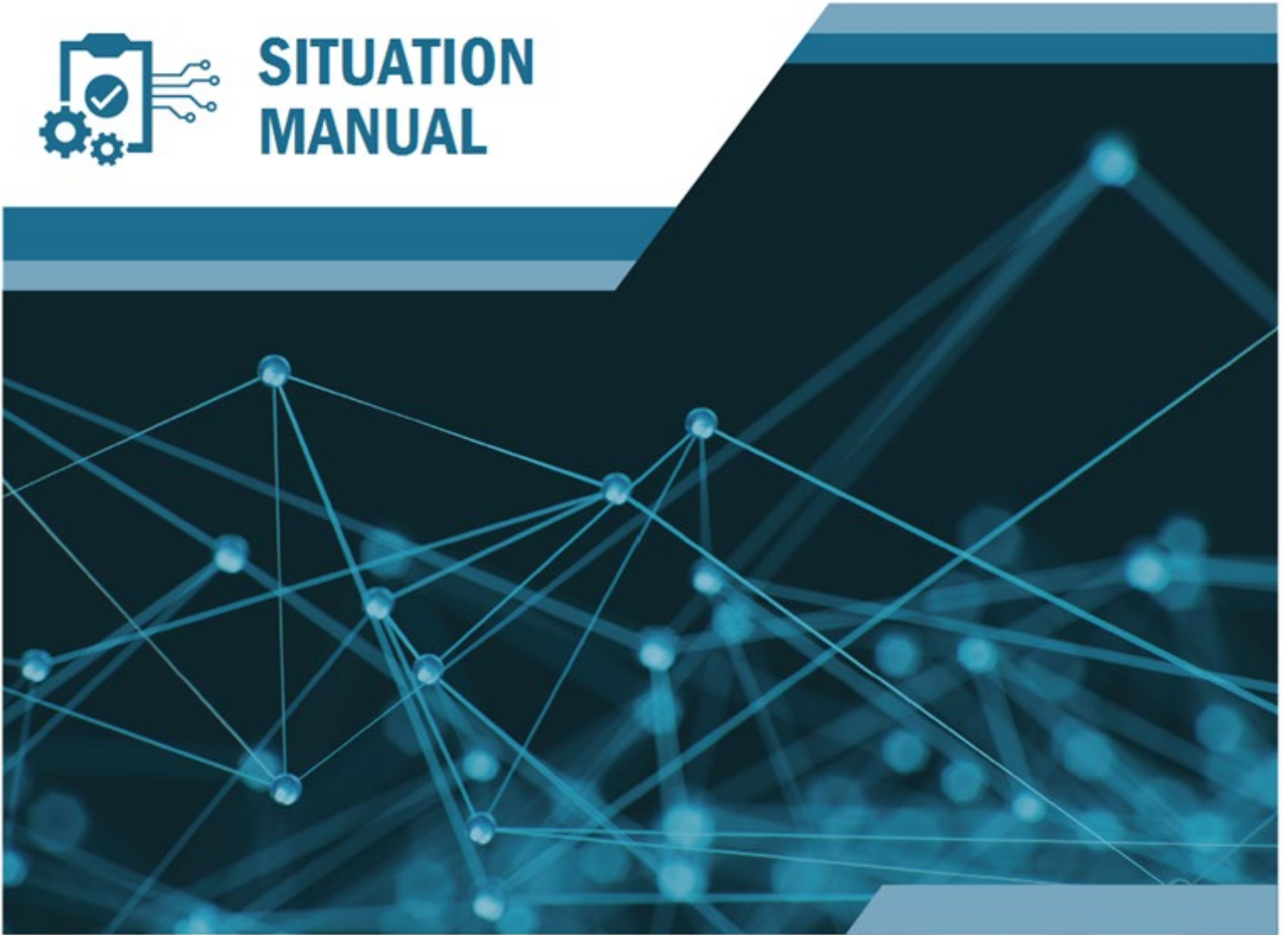
Section 1: General Information

The following sections should be included in all Situation Manuals. Update appropriate fields with exercise specific information or delete if unnecessary. *This instructional page should be deleted.*

<Exercise Title>
SitMan



SITUATION MANUAL



[Enter Exercise Title]

<Exercise Date>

[EXERCISE LOGO]

<Exercise Title>

SitMan

General Information

Participant Roles and Responsibilities

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

- **Players.** Players have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated scenario.
- **Observers.** Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitators.** 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 (SMEs) during the exercise.
- **Evaluators.** Evaluators are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions align to plans, policies, and procedures.

Exercise Structure

This exercise will be a multimedia, facilitated exercise. Players will participate in the following:

- Threat briefing
- Scenario modules:
 - **Module 1: Title** Describe overall focus of module.
 - **Module 2: Title** Describe overall focus of module.
 - **Module 3: Title** Describe overall focus of module.

The exercise will be led by a facilitator, who will provide the scenario updates and then moderate discussion generated by the discussion questions.

Exercise Guidelines

- This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of existing plans and capabilities, and insights derived from your training.
- 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 and possible solutions.
- Assume cooperation and support from other responders and agencies.
- Issue identification is not as valuable as suggestions and recommended actions that could improve prevention, protection, mitigation, response, and recovery efforts. Problem-solving efforts should be the focus.
- Situation updates, written materials, and resources provided are the basis for discussion; there are no situational or surprise injects.

<Exercise Title>

SitMan

Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise and should not allow these considerations to negatively impact their participation. During this exercise, the following apply:

- The scenarios are plausible, and events occur in the order they are presented.
- Some adversary events that would occur in real life are not presented as scenario injects.
- There is no hidden agenda, and there are no trick questions.
- All players receive information at the same time.
- The scenario is not derived from current intelligence.

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. Players will also be asked to complete participant feedback forms. Evaluation of the exercise is based on the exercise objectives and aligned <National Institute of Standard and Technology (NIST) Cybersecurity Framework Functions¹ or National Preparedness Goal Mission Areas and Core Capabilities²>. The participant feedback forms, coupled with facilitator observations and notes, should be used to evaluate the exercise and compile an After-Action Report.

¹ <https://www.nist.gov/cyberframework/online-learning/five-functions>

² <https://www.fema.gov/mission-areas>

<Exercise Title>

SitMan

Section 2: Exercise Overview and Scenarios

The following section includes multiple exercise summaries and scenarios. **Planners should choose the option that best fits their exercise needs and delete the rest.** While the Objectives are pre-populated, planners may modify the information to meet their specific needs. Additionally, planners are encouraged to modify the scenario and associated discussion questions to be organization- or jurisdiction-specific. *This instructional page should be deleted.*

Option A: Vote-by-Mail

Exercise Overview

<Insert Exercise Name>	<Insert Exercise Title>
Exercise Date, Time, and Location	
Scope	hour facilitated, discussion-based Tabletop Exercise
Purpose	Identify best practices and areas for improvement in incident planning, identification, and response through simulation of a realistic cyber and physical scenario exploring impacts to voter confidence, voting operations, and the integrity of elections.
<Pick one: NIST Cybersecurity Framework, Mission Areas, or Core Capabilities>	
Objectives	<ol style="list-style-type: none"> 1. Discuss the preparedness of the state and local officials to respond to and manage cybersecurity incidents. 2. Discuss processes for identifying potential cybersecurity incidents or issues. 3. Examine information sharing processes between state and local officials and with external partners. 4. Inform the development of state and local-level processes and plans to address elections-related cyber and physical incidents.
Threat or Hazard	Cyber and Physical
Scenario	<p>The scenario includes:</p> <ul style="list-style-type: none"> • Actions taken upon receipt of cybersecurity alerts; • Disruption of voter registration information systems; • News and social media manipulation related to political candidates and the conduct of elections; • Distributed Denial of Service (DDoS) attacks and web defacements impacting board of election websites; • Targeting of vote-by-mail process to alter, disrupt, and destroy the voting process; and • Ransomware and infection of county computer systems.
Sponsor	Exercise Host
Participating Organizations	Overview of organizations participating in the exercise (e.g. federal, state, local, private sector, etc.).
Points of Contact	<div style="display: flex; justify-content: space-between;"> Insert Exercise Points of Contact Insert Exercise Points of Contact </div>

<Exercise Title>

SitMan

Exercise Scenario**Module 1: Information Sharing****Inject 1**

A security company releases an alert on their website describing a cyber campaign targeted against printers and printing companies. The security company believes that attackers are attempting to assemble a new botnet using printers and other Internet of Things (IoT) devices. Once infected, the devices remain available to be used in denial of service attacks, or as platforms for further attacker access.

Inject 2

A technical alert is released by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) and forwarded by the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) regarding a phishing campaign targeting state and local election officials. The alert contains initial indicator information regarding a ransomware payload included in malicious attachments to emails. An observed phishing lure advertises links to the complete series of the hit TV series, <insert TV series name>, on a popular streaming service.

Inject 3

A new post by the hacktivist group Hippoponymous claims that they will be targeting the upcoming election in several states. They claim that they are conducting “completely free penetration testing” for the upcoming election.

Inject 4

Employees at your office receive a series of messages from colleagues in other city or county departments with links to the <insert TV series name> TV show. These links request that <your entity's> employees install a program to view the upcoming episodes.

Inject 5

An employee at your ballot printing vendor receives an email stating that they need to update their payroll and benefit information, immediately. The email indicates that they need to open the attachment and enable macros to view secure content.

Inject 6

Employees in your office notice an unusual program has appeared on their desktops. The program, named ReVue, appears to be a media player that was installed overnight.

When they are browsing the internet during their downtime, other employees notice that an excessive number of pop-up ads are appearing on normal websites. These pop-up ads advertise new links to the <insert TV series name> TV show.

Inject 7

The voting period for military and overseas voters begins. One <clerk> notices a ballot returned via email requesting that macros be enabled to download secure content. The <clerk> accepts the prompt to enable macros and proceeds to process the ballot normally.

Discussion Questions

Discussion questions included in each module may be modified as desired. Additional questions can be found in Section 3.

1. Would your organization receive the cybersecurity alert information presented in this scenario?
 - a. Through what channels would this information be received and disseminated?

<Exercise Title>

SitMan

- b. Who in the organization is responsible for collating and receiving these alerts?
 - c. What actions, if any, would your organization take based on this information?
2. What other sources of cybersecurity threat intelligence does your organization receive?
3. How do employees report suspected phishing attempts or other cybersecurity incidents?
 - a. What actions does your department take when suspicious emails are reported?
 - b. Are there formal policies or plans that would be followed?
 - c. Does your organization conduct phishing self-assessments?
4. Does your organization have required cybersecurity training for employees?
 - a. Are there additional training requirements for IT managers, system and network administrators, vendors, or other personnel with access to system-level software?
 - b. How often do they receive the training?
5. Are vendors required to report cybersecurity incidents to your organization?
6. Would any of these events be identified as cyber incidents?
7. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
 - a. What are your most significant threats and vulnerabilities?
 - b. What are your highest cybersecurity risks?

<Exercise Title>

SitMan

Module 2: Incident Identification**Inject 8**

The day before official printing of ballots begins, an employee prints a test ballot. Two employees check the ballot information before printing and determine that the information is correct, but when they print the test ballot, they notice that the order of the candidates is different from the test ballot on screen, and a candidate is missing from the U.S. House race.

That same day, an error occurs on the <Chief Election Official's> website. The web page for the <drop box lookup tool> mysteriously fails for two days due to an unknown error. A page on Safebook claims to have updated drop box information during the loss of the website.

Inject 9

Several <counties, municipalities, etc.> have seen an uncharacteristically large number of new voter registrations and registration changes via the online voter registration portal. The volume of requests appears to indicate that some of them are illegitimate.

Since all of the requests have been made using what appears to be legitimate citizen information, it is difficult to determine which requests should be considered invalid.

Inject 10

Voters throughout the state receive envelopes that appear to contain their official ballots. Some ballots, however, include a candidate representing the Hippoonymous party for the U.S. House race.

Voters call their <local election office (e.g., County Clerk Office)> and the <State Chief Election Official's> office to complain about their ballots.

Later that day, <local election employees (e.g., county clerk)> employees attempting to use the popular search engine, Poogle, are redirected to an unknown merchant's website.

Inject 11

Multiple ballots are returned to local election offices by the Postal Service. They indicate that the mailing address does not exist. A manual review of a portion of the envelopes shows that several addresses are incomplete or incorrect or the ballot is addressed to someone who does not live at that address.

A local media outlet, acting on a complaint from a resident, submits an inquiry to your office asking if all the ballots have been mailed out correctly.

Inject 12

A social media post from Hippoonymous encourages their followers to set up a "party at the box." Parties should have Hippoonymous logos and partygoers are encouraged to demonstrate against the Hippoonymous candidate's lack of representation on the ballots due to a failure to qualify.

Discussion Questions

1. What actions would be taken at this point? By whom?
2. What resources and intrusion detection capabilities are available to analyze anomalies on your network(s) and alert you to a cyber incident?
 - a. Internally (e.g., is your staff routinely trained to read and analyze your intrusion detection system logs)?
 - b. Externally (e.g., through government partners)?

<Exercise Title>

SitMan

3. How would your organization know which voter registration entries are valid? How does your organization monitor activity in the statewide voter registration database?
4. What actions, if any, would you take based on the ballot addresses being incomplete or ballots being mailed to voters who have moved?
5. How would you handle the misprinted ballots?
6. Which scenario event would prompt you or someone in your organization to report a cybersecurity incident?
 - a. Are individuals aware of where to report cybersecurity incidents?
7. Are cyber incident response procedures documented in an incident response plan?
 - a. Who has the authority to activate the cyber incident response plan?
 - b. Are employees familiar with and have they received training on the plan?
8. What are your public affairs concerns? Who is responsible for coordinating the public message and how would you get your message out?
9. What capabilities and resources are required for responding to this series of incidents?
 - a. What internal resources do you depend on? Are your current resources sufficient?
 - b. Whom do you contact if you need additional third-party assistance?
 - c. What resources are available within the state or locally? How do you request these resources?

<Exercise Title>

SitMan

Module 3: Incident Response*Inject 13 – Election Day – Morning*

On Election Day, several <county, local, municipal> websites have been altered with inaccurate information regarding drop box locations and hours. The <State Chief Election Official's> website is also defaced with an image of the hashtag #Rigged20<20>. IT staff at the state and the local jurisdictions are initially unable to access the sites to revert the changes.

Hippoponymous party protests surround drop boxes throughout the state. The protestors refuse to let voters return their ballots, claiming they are having a party. Media reports begin circulating about the parties on the box.

Inject 14 – Election Day – Afternoon

The news media begins contacting both state and <county, local, municipal> officials for comment regarding rumors of the vote tabulation system being hacked and social media allegations of election rigging.

Later in the afternoon, media outlets report that a ballot drop box at a party location erupted in flames. The outlet reports that the ballots were completely destroyed.

Inject 15 – Election Day – Evening

At <poll closing time> staff begin the process to close the <polls, voting period, etc.>. When local election office staff are about to transfer <the final set or final count of> vote totals to the state, multiple <county, local> systems lock up and computer screens display a demand for a ransom of \$50,000 to regain control of the infected devices. The vote totals are also encrypted and cannot be transferred.

Discussion Questions

1. What is your priority given the events of Module 3? How would these events affect election processes?
2. What alternative means of communication are used in the event primary methods (e.g., internet, email, etc.) of communicating with each other and the public are inoperable?
3. What public messaging efforts would be made concerning the events of Module 3?
 - a. Has your organization created any public messages in advance of an incident?
 - b. What organizations would you coordinate your public messaging efforts with?
4. What systems would be prioritized for recovery efforts? Would this be decided before an incident occurs?
5. What backup systems are utilized by participants?
 - a. How quickly can they be deployed?
 - b. How often are backups created or updated?
6. Does the situation described in Module 3 change your previous answer regarding your organization's ability to respond?
7. What processes are in place to collect evidence and maintain the chain of custody?
8. What is the decision process to determine if the ransom should be paid or not?
 - a. Who decides?

<Exercise Title>

SitMan

- b. What is the process?
- c. What are the advantages/disadvantages to?
- d. What are the political ramifications?
- e. What outside partners/entities do you need to contact?

<Exercise Title>

SitMan

Option B: Early Voting/Same Day or Election Day Registration

Exercise Overview

<Insert Exercise Name>	<Insert Exercise Title>
Exercise Date, Time, and Location	
Scope	1 hour facilitated, discussion-based Tabletop Exercise
Purpose	Identify best practices and areas for improvement in incident planning, identification, and response through simulation of a realistic cyber scenario exploring impacts to voter confidence, voting operations, and the integrity of elections.
<Pick one: NIST Cybersecurity Framework, Mission Areas, or Core Capabilities>	
Objectives	<ol style="list-style-type: none"> 1. Assess the preparedness of the state and local officials to respond to and manage cybersecurity incidents. 2. Discuss processes for identifying potential cybersecurity incidents or issues. 3. Examine information sharing processes between state and local officials and with external partners. 4. Inform the development of state and local-level processes and plans to address elections-related cyber and physical incidents.
Threat or Hazard	Cyber
Scenario	<p>The scenario includes:</p> <ul style="list-style-type: none"> • Actions taken upon receipt of cybersecurity alerts; • Disruption and alteration of voter registration information systems; • News and social media manipulation; • Distributed Denial of Service (DDoS) attacks and web defacements impacting election entity websites; and • Ransomware and infection of county computer systems.
Sponsor	Exercise Host
Participating Organizations	Overview of organizations participating in the exercise (e.g. federal, state, local, private sector, etc.).
Points of Contact	Insert Exercise Points of Contact Insert Exercise Points of Contact

<Exercise Title>

SitMan

Exercise Scenario

Module 1: Information Sharing

Inject 1

A technical alert is released by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) and forwarded by the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) regarding a phishing campaign targeting state and local election officials. The alert contains initial indicator information regarding a ransomware payload included in malicious attachments to the emails.

In addition, a security company releases an alert on their website describing a cyber campaign targeted against printers and printing companies. The security company believes that attackers are attempting to assemble a new botnet using printers and other Internet of Things (IoT) devices. Once infected, the devices remain available to be used in denial of service attacks, or as platforms for further attacker access.

Inject 2

<Department of Motor Vehicles (DMV), county election office, all of the above, etc.> employees receive an email from the state election office reminding them to expect an influx of citizens arriving at <DMV, county election office, etc.> locations to register to vote. The email includes an attachment consisting of a tip sheet with some helpful reminders about voter registration.

Inject 3

State and local election employees receive an email from their election management system (EMS) vendor. It includes guidance on performing updates to EMS software and firmware updates for <electronic voting equipment (e.g., tabulators, BMDs, DREs, as appropriate)>. The email references a prior meeting with the state election office.

Inject 4

A newly formed online news website “WeGotTheScoop.Biz” claims that one of the candidates accepted illegal campaign contributions from abroad and bribed <Your state’s> election officials to alter ballots so that the candidate will get more votes. Their stories are being shared by a series of Safebook accounts that belong to a group called “Citizens for Truthful Elections”.

Discussion Questions

Discussion questions included in each module may be modified as desired. Additional questions can be found in Section 3.

1. Would your organization receive the cybersecurity alert information presented in this scenario?
 - a. Through what channels would this information be received and disseminated?
 - b. Who in the organization is responsible for collating and receiving these alerts?
 - c. What actions, if any, would your organization take based on this information?
2. What other sources of cybersecurity threat information does your organization receive?
3. How do employees report suspected phishing attempts or other cybersecurity incidents?
 - a. What actions does your department take when suspicious emails are reported?
 - b. Are there formal policies or plans that would be followed?
 - c. Does your organization conduct phishing self-assessments?

<Exercise Title>

SitMan

4. Does your organization utilize multi-factor authentication (e.g. something you know, something you have, something you are) to mitigate the potential effects of phishing?
5. Does your organization have required cybersecurity training for employees?
 - a. Are there additional training requirements for IT managers, system and network administrators, vendors, or other personnel with access to system-level software?
 - b. How often do they receive the training?
6. Are vendors required to report cybersecurity incidents to your organization?
7. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
 - a. What are your most significant threats and vulnerabilities?
 - b. What are your highest cybersecurity risks?
8. What entities connect to your state or county's voter registration database?
 - a. Does your organization maintain contact information with all relevant parties in case of an incident?
 - b. What entity is responsible for securing the voter registration database?

<Exercise Title>

SitMan

Module 2: Incident Identification*Inject 5*

<Before the end of the voter registration period or three weeks before Election Day>

“WeGotTheScoop.Biz” posts a story claiming that you can register to vote through their website via a link in the story. The link resolves to <https://elections.<yourstate>.biz/OnlineVoterRegistration>. Social media posts on various platforms circulate advertising the registration site.

Inject 6

A breach of <Your State’s Department of Motor Vehicles or other entity with any connection to the Voter Registration Database> occurs and is reported by media outlets. An internal investigation reveals that voter registration data may have been compromised.

Inject 7

Your state’s <online voter registration or other state elections website> website is the subject of sporadic high-bandwidth distributed denial of service (DDoS) attacks over the course of a week before the <new voter registration deadline or two weeks before Election Day>. As a result, the site becomes intermittently inaccessible. News reports emerge online tying the DDoS attacks to the upcoming election and questioning your state’s preparedness to address the issue and secure the upcoming election, as well as attributing them to a foreign actor.

Inject 8

The day before your <state/local jurisdiction> plans to send pollbook information to be <printed or uploaded to e-pollbooks, or both> in preparation for the election, host machines at your state and local election offices are “locked up,” and the contents of their storage media encrypted by ransomware. Initial indications are that the ransomware is a variant of the well-known RamRam ransomware previously used in the opportunistic targeting of other state and municipal entities.

Discussion Questions

1. What actions would be taken at this point? By whom?
2. Are cyber incident response procedures documented in an incident response plan?
 - a. Who has the authority to activate the cyber incident response plan?
 - b. Are employees familiar with and have they received training on the plan?
3. How do you protect the integrity of your voter registration database?
4. What inject, if any, would prompt you or someone in your organization to report a cybersecurity incident?
 - a. How would reports flow between different levels of government (e.g. local reporting to state, or state to federal)?
5. What are your public affairs concerns? Who is responsible for coordinating the public message and how would you get your message out?
6. In the event of complete failure of your entity’s general network or election network, what systems would you need to successfully run an election?
7. What capabilities and resources are required for responding to this series of incidents?
 - a. What internal resources do you depend on? Are your current resources sufficient?
 - b. Whom do you contact if you need additional third-party assistance?

<Exercise Title>

SitMan

- c. What resources are available within the state or locally? How do you request these resources?

<Exercise Title>

SitMan

Module 3: Incident Response**Inject 9 – First Day – Early Voting – Morning**

On the first day of early voting, several <county or local election> websites have been changed with inaccurate information regarding early voting locations and hours. The state elections website is also defaced with an image of the hashtag #Rigged20<20>. IT staff are initially unable to access the sites to revert the changes.

Later that day, the hacktivist group Arbiters of Darkness claim to have done their part to protect the nation by successfully purging “all unnecessary voters” from the pollbooks.

Poll workers report a larger than normal number of voters arriving to vote without appearing in the pollbooks and that some voters’ addresses are not correct.

Inject 10 – First Day – Early Voting – Afternoon

The news media begins contacting both state and <county or local> officials for comments regarding rumors of the penetration of the state’s voter registration system and claims concerning the loss of election integrity.

Inject 11 – First Day – Early Voting – Evening

Before polls close after the first day of early voting, all host machines at the local level are “locked up” by a variant of the RamRam ransomware.

Discussion Questions

1. What is your priority given the events of Module 3? How would these events affect election processes?
2. What alternative means of communication are used in the event primary methods (e.g., internet, email, etc.) of communicating with each other and the public are inoperable?
3. How are voters able to vote in the event the voter registration database is compromised?
4. What public messaging efforts would be made concerning the events of Module 3?
 - a. Has your organization created any public messages in advance of an incident?
 - b. What organizations would you coordinate your public messaging efforts with?
5. What systems would be prioritized for recovery efforts? Would this be decided before an incident occurs?
6. What backup systems are utilized by participants?
 - a. How quickly can they be deployed?
 - b. How often are backups created or updated?
7. What is the decision process to determine if the ransom should be paid or not?
 - a. Who decides?
 - b. What is the process?
 - c. What are the advantages/disadvantages?
 - d. What are the political ramifications?
 - e. What outside partners/entities do you need to contact?
8. Does the situation described in Module 3 change your previous answer regarding your organization’s ability to respond?
9. When is an incident determined to be over?

<Exercise Title>

SitMan

Option C: Election Day/Voting Machines

Exercise Overview

<Insert Exercise Name>	<Insert Exercise Title>
Exercise Date, Time, and Location	
Scope	
Purpose	Identify best practices and areas for improvement in incident planning, identification, and response through simulation of a realistic cyber scenario exploring impacts to voter confidence, voting operations, and the integrity of elections.
<Pick one: NIST Cybersecurity Framework, Mission Areas, or Core Capabilities>	
Objectives	<ol style="list-style-type: none"> 1. Assess the preparedness of the state and local election officials to respond to and manage cybersecurity incidents. 2. Examine information sharing processes amongst state and local election officials. 3. Inform the development of state and local-level processes and plans to address elections-related cyber incidents. 4. Explore processes for addressing news and social media manipulation related to elections. 5. Explore processes for requesting external response resources in the event state or local resources are exhausted.
Threat or Hazard	Cyber
Scenario	<p>The scenario includes:</p> <ul style="list-style-type: none"> • Actions taken upon receipt of cybersecurity alerts; • Disruption and alteration of voting machines and vote tabulators; • News and social media manipulation; and • Ransomware and infection of voting machines.
Sponsor	
Participating Organizations	
Points of Contact	

<Exercise Title>

SitMan

Exercise Scenario

Module 1: Information Sharing

Inject 1

A technical alert is released by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the FBI and forwarded by the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) regarding a phishing campaign targeting voting machine companies and other third-party service providers. The alert contains initial indicator information regarding the use of false system updates to lure users into downloading a malware package onto their system. Other observed lures include the use of tax forms, billing statements, receipts, and order forms.

Inject 2

News media outlets report on a series of breaches impacting one of the largest merchant stores in the United States. At least 200 million records that included unencrypted passwords, credit card numbers, password reset questions, birthdates, and Social Security numbers were exposed. News media coverage labels this breach as the greatest loss of Personally Identifiable Information (PII) this year.

Inject 3

<State, county, local, or municipal> election employees receive an email from their election management system (EMS) vendor. It includes guidance on performing updates to EMS software and firmware updates for <tabulators, BMDs, DREs>.

Inject 4

A newly formed online news website “WeGotTheScoop.Biz” claims that the voting equipment in your state is not secure. They also claim that voting in the upcoming election is pointless and that the outcome has already been determined. The stories are being circulated on Chirper with the hashtag #DontVote20<20> and on Safebook.

Discussion Questions

Discussion questions included in each module may be modified as desired. Additional questions can be found in Section 3.

1. Would your organization receive the cybersecurity alert information presented in this scenario?
 - a. Through what channels would this information be received and disseminated?
 - b. Who in the organization is responsible for collating and receiving these alerts?
 - c. What actions, if any, would your organization take based on this information?
2. What other sources of cybersecurity threat information does your organization receive?
3. How do employees report suspected phishing attempts or other cybersecurity incidents?
 - a. What actions does your department take when suspicious emails are reported?
 - b. Are there formal policies or plans that would be followed?
 - c. Does your organization conduct phishing self-assessments?
4. Does your organization utilize multi-factor authentication (e.g. something you know, something you have, something you are) to mitigate the potential effects of phishing?

<Exercise Title>

SitMan

5. Does your organization have required cybersecurity training for employees?
 - a. Are there additional training requirements for IT managers, system and network administrators, vendors, or other personnel with access to system-level software?
 - b. How often do they receive the training?
6. Are vendors required to report cybersecurity incidents to your organization?
7. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
 - a. What are your most significant threats and vulnerabilities?
 - b. What are your highest cybersecurity risks?
8. How would you respond to the attempts to discredit the elections process on social media?

<Exercise Title>

SitMan

Module 2: Incident Identification**Inject 5**

“WeGotTheScoop.Biz” claims that <your state, another state, or outside states> <has/have> asked for the assistance of outside parties to conduct port scans of state networks as a test of their security. Social media posts on various platforms circulate the story and the results of the scans with the hashtag #PlanScan.

Inject 6

In preparation for programming the election, election operations personnel test moving election data between electronic voting machines (e.g., <direct recording electronic (DRE), optical scan, etc.>), the election management system (EMS) host machine, and another PC used to post unofficial election results.

Inject 7

Various state and local agencies, including elections offices, are subjected to an unusual number of port scans by several unknown entities over the week. IT staff also note multiple attempts to login to state systems remotely using specific combinations of usernames and passwords.

Inject 8

The #PlanScan hashtag shows that a volunteer tester found a <voting machine or tabulator> online, which allows an individual remote access to the device without the need to authenticate. They provide a complete set of information for others to locate the machine along with the exploit needed to access the machine.

Inject 9

Your <state, county, municipality> conducts the standard logic and accuracy testing of voting machines before the upcoming election. Some local jurisdictions report that a candidate for the U.S Senate race was not properly recorded by the machine. After a consultation with the vendor, election officials are able to fix the issue. Subsequent testing shows no issues with the device.

Discussion Questions

1. What actions would be taken at this point? By whom?
2. Are cyber incident response procedures documented in an incident response plan?
 - a. Who has the authority to activate the cyber incident response plan?
 - b. Are employees familiar with and have they received training on the plan?
3. What resources and intrusion detection capabilities are available to analyze anomalies on your network(s) and alert you to a cyber incident?
 - a. Internally (e.g., is your staff routinely trained to read and analyze your intrusion detection system logs)?
 - b. Externally (e.g., through government partners)?
4. What inject, if any, would prompt you or someone in your organization to report a cybersecurity incident?
 - a. How would reports flow between different levels of government (e.g., local reporting to state, or state to federal)?
5. How do you protect the integrity of your voting machines?
 - a. What entities have access to your <state, county, local> voting machines?

<Exercise Title>

SitMan

- b. What entity is responsible for securing the voting machines?
 - c. Does your organization maintain contact information with all relevant parties in case of an incident?
6. How would your organization respond to the emerging news and social media issues?
- a. Does your organization have pre-approved messages for immediate release as part of a larger communications plan?

<Exercise Title>

SitMan

Module 3: Incident Response*Inject 10 – Election Day – Morning*

About 20 minutes after the polls open, the <Chief Election Official's> website is defaced with a picture of clowns and a claim that the election outcome has been determined by the state's governor. IT staff attempt to revert the changes but are unable to do so.

Inject 11 – Election Day – Early Afternoon

Several voters in one of the largest <precincts, wards> in your state claim that <they are not able to select or mark their desired candidate, or their candidate is not present on the printed ballot>. In addition, some voters notice that a <physical security measure (e.g. lock, seal, etc.)> for the <voting machine/tabulator/ballot box > appears to have been altered.

Inject 12 – Election Day – Late Afternoon

In the late afternoon, the <voting machines, tabulators, entity networks> become “locked up” and display a laughing clown face. The machine asks for a ransom of \$100 in cryptocurrency to unlock the machine.

Voters take to social media and begin asking what has happened to their vote, with some claiming that they cannot vote. “WeGotTheScoop.Biz” and other media outlets begin circulating a post claiming that the election has been hacked and that voting is pointless.

Inject 13 – Election Day – Evening

After the polls close, your EMS and vote tabulation systems are also “locked up” and display a laughing clown face. When the early return results are not posted, media outlets begin submitting inquiries asking if there have been further issues with the voting process.

Discussion Questions

1. What is your priority given the events of Module 3? How would these events affect election processes?
2. What capabilities and resources are required for responding to this series of incidents?
 - a. What internal resources do you depend on? Are your current resources sufficient?
 - b. Whom do you contact if you need additional third-party assistance?
 - c. What resources are available within the state or locally? How do you request these resources?
3. What are your public affairs concerns? Who is responsible for coordinating the public message?
4. What backup systems are utilized by participants?
 - a. How quickly can they be deployed?
 - b. How often are backups created or updated?
5. What is the decision process to determine if the ransom should be paid or not?
 - a. Who decides?
 - b. What is the process?
 - c. What are the advantages/disadvantages?
 - d. What are the political ramifications?
 - e. What outside partners/entities do you need to contact?
6. What processes are in place to collect evidence and maintain the chain of custody?

<Exercise Title>

SitMan

7. When is an incident determined to be over?

<Exercise Title>

SitMan

Section 3: Discussion Questions

The following section includes supplemental discussion questions to guide exercise play. Exercise planners are encouraged to select additional, applicable discussion questions to the chosen scenario to bolster participant conversation. The questions are organized by topic; some are scenario specific, but some can apply to multiple scenarios. *This instructional page, as well as undesired discussion questions, should be deleted.*

<Exercise Title>

SitMan

Cyber Preparedness and Planning

1. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
 - a. What are your most significant threats and vulnerabilities?
 - b. What are your highest cyber security risks?
2. How does your organization 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.
4. How do you communicate your cybersecurity concerns to your vendors and how do you evaluate their cybersecurity performance?
5. What role does organizational leadership play in cybersecurity? Does this role differ during steady-state and incident response?
6. What level of funding and/or resources are devoted to cyber preparedness? Based on your risk assessment, what is the range of potential losses from a cyber incident?
7. Discuss cyber preparedness integration with your current all-hazards preparedness efforts. Who are your cyber preparedness stakeholders (public, private, non-profit, other)?
8. What mission essential functions depend on information technology and what are the cascading effects of their disruption?
9. Have you had any external review or audit of your IT plans, policies, or procedures within the last year?
10. Are background checks conducted for IT, security and key supporting personnel?
11. Is there a manager/department in charge of cybersecurity management? If yes, is this the primary function of that manager?
12. How does your organization recruit, develop, and retain cybersecurity staff?
13. How well-defined is cybersecurity in relation to contracts with third-party support vendors and crucial suppliers?
 - a. How often are contracts reviewed?
 - b. How well do your service level agreements address incident response?
14. Discuss the status of cyber preparedness planning within your organization.
 - a. Have you completed a business impact analysis? Does the analysis include information technology (IT) infrastructure supporting mission essential functions identified in continuity of operations and continuity of government plans?
 - b. Is cybersecurity integrated in your business continuity plans? Does your business continuity and/or disaster recovery planning have a prioritized list of information technology infrastructure for restoration?
 - c. How have IT specific plans been coordinated with other planning efforts such as an Emergency Operations Plan or Continuity of Operations Plan?

<Exercise Title>

SitMan

15. How is cybersecurity integrated into both organizational and project risk assessments and management?
16. Does your organization employ a formal sanctions process for personnel failing to comply with established information security policies and procedures? If so, has this been communicated to employees?
17. Does your organization have a cybersecurity incident response plan? When was it issued? When was the incident response plan last revised? What authorities require which departments or agencies to follow the plan?
18. Does your organization utilize multi-factor authentication?
19. Does your IT department have a patch management plan in place? If so,
 - a. Are risk assessments performed on all servers on the network?
 - b. Are processes in place to proactively evaluate each server's criticality and applicability to software patches?
 - c. Does this plan include a risk management strategy that addresses the following considerations?
 - i. The risks of not patching reported vulnerabilities?
 - ii. Extended downtime?
 - iii. Impaired functionality?
 - iv. The loss of data?
20. Do you have a method for tracking and/or identifying problematic pieces of firmware in your organization, should a vulnerability be identified?
21. What processes does your organization have in place for when an employee is terminated or resigns?
 - a. Are there any additional processes that are implemented if the employee's termination is contentious?
 - b. Does your organization retrieve all information system-related property (e.g., authentication key, system administration's handbook/manual, keys, identification cards, etc.) during the employment termination process?
22. Do any third-party vendors have unmitigated access into your network?
 - a. What protections do you have in place to protect against malicious intent by those vendors or outside parties that have access to your network?
23. What are your identified responsibilities for, and capabilities to, prevent cyber incidents?
24. Who is responsible for network and information security management?
25. Can you identify key documents that support cyber preparedness at a federal, state, or local level?
26. Does your organization follow a cybersecurity standard of practice (NIST Cybersecurity Framework/800 Series, ISO/IEC, etc.)? If so, which?

<Exercise Title>

SitMan

27. Are there flowcharts showing the high-level relationships and crisis lines of communication (i.e., who calls who) specifically for a cyber incident? Are they part of the response or continuity planning documents?
28. Does your organization have a formal or informal policy or procedures pertaining to IT account management?
 - a. Do these policies or procedures include protocols for establishing, activating, modifying, disabling, and removing accounts?
 - b. Do these policies or procedures include protocols/steps for notifying IT account managers/administrators when users are terminated?
29. Are IT and business continuity functions coordinated with physical security? Are all three then collaborating with public relations, human resources, and legal departments?
30. Do you have processes to ensure that your external dependencies (contractors, power, water, etc.) are integrated into your security and continuity planning and programs?
31. Describe the decision-making process for protective actions in a cyber incident. What options are available? Have these options been documented in plans? How are they activated?
32. What immediate protective and mitigation actions would be taken at your organization in this scenario? Who is responsible for those actions?
33. What protective actions would you take across non-impacted systems or agencies in the scenario presented? Who is responsible for protective action decision-making? How are actions coordinated across parts of the organization?
34. Compare and contrast physical and cyber incident notifications and protective action decision-making.
35. What systems or processes are the most critical to running elections?
 - a. Is this decision codified in an incident response plan?
 - b. What processes are in place to run elections in the event computer systems are compromised?
36. How do you protect the integrity of your voter registration database?
 - a. What entities have access to the database?
 - b. How would those entities report a breach of their systems to your office?
37. How do you protect the integrity of your voting equipment?
 - a. What entities have access to your <state, county, local> voting equipment?
 - b. What entity is responsible for securing the voting equipment?
 - c. Does your organization maintain contact information with all relevant parties in case of an incident?
38. What is your planned cyber incident management structure?
 - a. Who (by department and position) leads incident management and why?
 - b. How are they notified?
 - c. When did they last exercise their role?

<Exercise Title>

SitMan

- d. What is the length of your operational period (i.e., your “battle rhythm”)?
- e. What are the primary and contingency communication mechanisms necessary to support incident management?

<Exercise Title>

SitMan

Information Sharing

1. Would your organization receive the information presented in the scenario?
 - a. Through what channels would this information be received and disseminated?
 - b. Are there established mechanisms to facilitate rapid information dissemination?
 - c. Are there known communication gaps? If so, who in your organization is responsible for addressing those gaps?
 - d. What actions, if any, would your organization take based on this information?
2. What sources of cybersecurity threat intelligence does your organization receive? For example, information from the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), open source reporting, security service providers, others?
 - a. What cyber threat information is most useful?
 - b. Is the information you receive timely and actionable?
 - c. Who is responsible for collating information across the organization?
3. What mechanisms and products are used to share cyber threat information within your organization and external to your organization (e.g., distribution lists, information sharing portals)?
4. Describe how variables in threat information (timeframe, credibility, and specificity) impact decision-making.
5. How do local government entities report information to state partners?
6. What information, if any, would be shared between the local government IT offices, local election officials, and state officials?
 - a. How would this information be shared and is this process documented and/or formalized?
7. How is information shared among your internal and external stakeholders? Through formal or informal relationships? What information sharing mechanisms are in place?
8. What are some challenges that are experienced by information technology and business continuity planning in terms of information sharing? Is information flowing in both directions?

<Exercise Title>

SitMan

Incident Identification

1. How do employees report suspected phishing attempts?
 - a. What actions does your department take when suspicious emails are reported?
 - b. Are there formal policies or plans that would be followed?
 - c. Does your department conduct phishing self-assessments?
2. Would any of these issues be considered a cyber incident at this point?
3. What process does the general workforce follow to report suspected cyber incidents? Is this a formal process on which they have been trained?
4. What would cause you or someone in your organization to report a cybersecurity incident?
 - a. How are incidents reported?
 - b. What would trigger the reporting requirements established by State law and policy?
 - c. Are cyber incident procedures documented in an incident response plan?
 - d. Who has the authority to create and enforce cybersecurity policies in your organization?
 - e. Are employees familiar with and have they received training on the plan?
5. Do you have defined cybersecurity incident escalation criteria, notifications, activations, and/or courses of action?
 - a. If so, what actions would be taken at this point? By who?
 - b. Would leadership be notified?
6. How does your organization baseline network activity? How would you be able to distinguish between normal and abnormal traffic?
7. Does the organization report cybersecurity incidents to outside organizations? If so, to whom? What, if any, mandatory reporting requirements do you have?
8. Do detection and analysis procedures differ for loss of personally identifiable information (PII), phishing attempts, data exfiltration, data modification, or other incidents?
9. Who is responsible for correlating information across different organizational-level incidents?
10. Discuss your organization's intrusion detection capabilities and analytics that alert you to a cyber incident.
11. What type of hardware and/or software does your organization use to detect/prevent malicious activity of unknown origin on your systems/network?
12. What is your organization's primary concern at this time?
13. What inject, if any, would prompt you or someone in your organization to report a cybersecurity incident?
 - a. How would reports flow between different levels of government (e.g., local reporting to state, or state to federal)?

<Exercise Title>

SitMan

14. Do you have someone within your organization who monitors the Dark Web? If so, how would you verify the security researcher's claims and confirm authenticity of the sensitive information in question?

<Exercise Title>

SitMan

Incident Response

1. What level of leadership/management would be notified at this point in the scenario? Is there a plan in place detailing the thresholds at which different notifications are made and what information is provided?
2. What is your department or agency's primary concern? Mitigation of the incident (resolving the issue) or investigation (preserving the evidence to build a criminal case)? Who would make this decision? Are these mutually exclusive?
3. What response actions would your organization have taken at this point? Are these actions driven by a plan?
4. What impact will the sale of sensitive or Personally Identifiable Information (PII) have on your response and recovery activities?
 - a. Will it alter priorities? Have your public relations priorities changed?
 - b. Will it trigger any additional legal or regulatory notifications?
5. Whom will you notify, internally and externally, of these incidents?
 - a. Is there a process or plan in place that outlines the severity thresholds for which different notifications are made and what information is to be conveyed?
 - b. Are you keeping senior leadership updated? What information is provided and how is it communicated?
 - c. Would you make any notification to the public?
 - i. If so, how are you coordinating your messaging within your organization?
 - ii. Do you have pre-canned messaging or holding statements for such an event?
 - d. How are you ensuring unity of message between your organization, the public sector, and elected officials?
6. How would these events affect your organization's business operation/processes?
7. Do these incidents generate any concerns that have not been addressed?
8. How would your organization respond to the discovery of a malicious, unauthorized administrator account on your systems? Who would be informed internally? Who would be informed externally (e.g., law enforcement, cybersecurity insurance partners, etc.)?
9. What resources are required for incident investigation and attribution? Are sufficient resources available in-house?
10. Would the events presented in the scenario trigger activation of your cyber incident response plan or similar document (e.g., emergency operations plan cyber incident annex)? If so, would that alter any roles and responsibilities?
11. At what point in the scenario would you contact law enforcement and/or the state Attorney General?
 - a. How would relationships with law enforcement and other partners be managed? Where is the process documented?
 - b. How does a law enforcement investigation impact containment, eradication, and recovery efforts?

<Exercise Title>

SitMan

- c. Are processes and resources in place for evidence preservation and collection?
12. Discuss the difference between network and host forensics. How are you equipped and staffed to address this?
13. Do you have a network operations center? Security operations center? What are their roles during a response?
14. What are your essential elements of information and key information questions necessary for operational and executive-level responses to cyber incidents?
15. What mission essential functions are impacted by the incidents described in the scenario?
16. Is there a way to maintain service availability of key assets (e.g., network connectivity, etc.)?
17. What capabilities and resources are required for responding to this series of incidents?
- What internal resources do you depend on? Are your current resources sufficient?
 - Whom do you contact if you're in need of additional third-party assistance?
 - What resources are available within the state or locally? How do you request these resources?
 - Do you have personnel tasked with incident response or a designated cyber incident response team within your organization?
 - If so, what threshold must be reached for the cyber incident response personnel to be activated? Does this scenario reach that threshold?
 - Who is responsible for activating the cyber incident response personnel and under what circumstances?
 - What are the cyber incident response team/personnel's roles and responsibilities?
18. Does this scenario exceed your organization's ability to respond?
- If so, are there established procedures to request additional support?
19. What are your organization's response priorities?
- Who would be notified at this point in the scenario? Is there a plan in place detailing the thresholds at which different notifications are made and what information is provided?
 - What response actions would the IT/IS department take at this point? Are these actions driven by a plan?
 - What response capabilities and resources are required to respond to these incidents?
20. What actions would be taken when the exfiltration is discovered? Does your organization have written plans that would be implemented?
21. What is the decision process to determine if the ransom should be paid or not?
- Who decides?
 - What's the process?
 - What are the advantages/disadvantages?

<Exercise Title>

SitMan

- d. What are the political ramifications?
 - e. What outside partners/entities do you need to contact?
22. Where do you receive cyber response technical assistance? Do you have plans, procedures or policies in place to access this assistance?
23. Have you proactively identified and established the service provider relationships needed for incident/breach response issues (e.g., credit counseling, forensic/computer security services)?
24. What processes are used to contact critical personnel at any time, day or night?
- a. How do you proceed if critical personnel are unreachable or unavailable?
25. If your pollbook or other critical election information system were disabled how would you continue elections operations?
- a. What, if any, additional resources would you need to conduct elections if your elections information was unrecoverable?
 - b. Do you have mechanisms in place (e.g., MOU/MOA, contract, etc.) for arranging additional surge support of both personnel and resources on Election Day, should it be needed?
26. How would your organization respond to misprinted <ballots, envelopes, or other printed election materials>?
27. How would a breach of another agency affect the <your entity> if they potentially have access to your information?
- a. Is the agency required to notify <your entity> of their breach or suspected breach? If so, what are the notice requirements?
28. Given the events of <Election Day, early voting> what is your greatest priority?
29. If the networks were found to be infected with ransomware, how would this impact the certification of election results?
- a. If election results from your <precinct, municipality, county> cannot be certified, how would you proceed?
30. How would voters locate their <polling location> if the locator were vandalized or disabled?
31. How would you determine whether unauthorized manipulation of election data has occurred?
- a. How would you address the absence or alteration of voter data in the pollbooks?
 - b. How would reconcile a greater number of voter versus available voters registered?
32. How would you respond to the allegations that the election <data, results, or other assets> were damaged or destroyed?
- a. What partners would you involve in the response?
 - b. Have you drafted messaging in advance of an incident?

<Exercise Title>

SitMan

33. If primary communications are compromised, how do you provide information to internal and external entities?
34. What actions, if any, would you take based on the ballot addresses being incomplete or ballots being mailed to voters who have moved?
35. How would you handle the misprinted ballots?
36. How are voters able to vote in the event the voter registration database is compromised?
37. In the event of complete failure of your entity's general network or election network, what systems would you need to successfully run an election?
38. How would you respond to the attempts to discredit the elections process on social media?

<Exercise Title>

SitMan

Recovery

1. When does your organization determine a cyber incident is closed?
 - a. Who makes this decision?
 - b. Would your organization engage in any post-incident activities?
2. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
 - a. Would senior leaders consider re-activating critical business processes and systems? What is the risk associated with doing so?
 - b. Would your organization consider a complete rebuild of these systems? How long and costly would that process be?
 - c. What factors do you consider when making these decisions?
3. What formal policies and procedures does your organization use to decide when and how to restore backed-up data, including measures for ensuring the integrity of backed-up data before restoration?
4. Does your organization have back-ups of vital records (e.g., the voter registration database, etc.) in a location that is separated from your primary working copies of your files?
 - a. How frequently do you run backups?
 - b. How long do you keep any copies of archived files backed up?
 - c. How long of a downtime would exist between your primary files and the restoration of files via your back-up?
5. Are redundant systems in place if the impacted system(s) is compromised?
 - a. Are alternative systems or manual processes in place to continue operations if a critical system is unavailable for a significant period of time?
 - b. Who can authorize use of alternate systems or procedures?
6. What backup systems are utilized by participants?
 - a. How quickly can they be deployed?
 - b. How often are backups created or destroyed?
7. Describe your role in post-incident activity.
8. How would you work with critical infrastructure providers to determine the incident is over?
9. How does post incident-activity differ when critical infrastructure is involved?
10. Does your organization have a continuity of operations plan (COOP) for conducting its functions at a location other than your main building?
 - a. If so, how would a suspected cyber incursion impact your organization's ability to activate its COOP Plan?
11. Are there further concerns that have not be discussed?

<Exercise Title>

SitMan

Training and Exercises

1. Does your organization provide basic cybersecurity and/or IT security awareness training to all users (including managers and senior executives)?
 - a. How often is training provided?
 - b. Does it cover:
 - i. Review of department and/or agency acceptable use and IT policies,
 - ii. Prominent cyber threat awareness,
 - iii. Password procedures, and
 - iv. Whom to contact and how to report suspicious activities?
 - c. Is training required to obtain network access?
 - d. What security-related training does your department or agency provide to, or contractually require of, IT personnel and vendors with access to your city's or county's information systems? How often do they receive the training?
2. Do you regularly train elections personnel, including volunteers, on cybersecurity threats such as phishing?
 - a. Does your organization provide basic cybersecurity and/or IT security awareness training to all users (including managers, senior executives, and vendors)?
 - b. How often is training provided?
 - c. What topics are covered in the training sessions?
3. Do your cybersecurity incident response team members undergo any special training to detect, analyze, and report this activity? If so, can you describe this training?
 - a. Is your staff sufficiently trained to read and analyze your intrusion detection system logs?
4. What training do you provide in support of your Cybersecurity Incident Response Plan, Business Continuity Plan, Emergency Operations Plan Cyber Incident Plan, or other related plans?
 - a. Do employees know what constitutes suspicious cybersecurity activities or incidents? Do they know what actions to take when one arises?
5. If you have a cyber incident response plan, how often does your organization exercise the plan?
 - a. Who is responsible for the exercise planning?
 - b. What agencies are involved in the exercise?
 - c. What level of the organization is required to participate?
 - d. What actions follow the exercise?
6. What are your cybersecurity incident response team's exercise requirements?
7. Do your organization's exercise efforts include both physical and cyber risks?
8. Have senior or elected officials participated in a cybersecurity exercise?
9. Are there additional training and/or exercising requirements for your organization?

<Exercise Title>

SitMan

Senior Leaders and Elected Officials

1. What is your cybersecurity culture? As a leader in your organization, what cybersecurity goals have you set? How have they been communicated?
2. As it relates to your jurisdiction, what cybersecurity information do you request? What do you receive?
3. What are your cybersecurity risks?
4. Who develops your jurisdiction's cybersecurity risk profile? What are their reporting requirements? Are they directed to, required by statute, or other? How often do they report?
5. Is your cybersecurity risk integrated with physical risk for an integrated jurisdictional risk assessment?
6. What is your jurisdiction's greatest cybersecurity concern? Why do you rate this concern as your greatest concern? Who reports to you on cyber threats?
7. What, if any, infrastructure does your jurisdiction own, operate, and/or regulate?
8. What relationships do you have with critical infrastructure owners and operators?
9. What priorities have you set related to the cybersecurity of critical infrastructure?
10. What is your most important critical infrastructure?
11. What are your regulatory requirements related to critical infrastructure, if any?
12. What is the greatest threat facing your critical infrastructure? What, if anything, is your jurisdiction able to do to mitigate it?
13. When did you last receive a cyber threat briefing for your jurisdiction?
14. How has your jurisdiction prepared for a cyber incident? Does your jurisdiction have cybersecurity plans in place? How many information security officers do you have? Does the plan indicate how they will work together?
15. Have your information security officers and emergency managers jointly planned for cybersecurity incidents?
16. What are your cybersecurity workforce gaps? How does your jurisdiction recruit, develop, and retain cybersecurity staff?
17. What cybersecurity training do you have planned for cybersecurity staff, managers, and general workforce?
18. What magnitude of incident would require you be notified? How does that notification process work? Is it planned?
19. What requirements or agreements, if any, exist for critical infrastructure to notify you of a cyber incident?
20. Who advises you on cyber threats? What are your essential elements of information or critical information requirements?

<Exercise Title>

SitMan

21. What is your planned role in protective action decision-making?
22. What is your planned cyber incident management structure? What parts of the government need to be engaged?
23. Would your jurisdiction's Emergency Operations Center be activated in a cyber incident? How? Why?
24. What is your role in a cyber incident?
25. How does a law enforcement investigation impact your response?
26. What is your role in communicating to the public?
27. How are costs of the response calculated?
28. What information do you need to support your decision-making process?
29. Who is your jurisdiction's cybersecurity liaison to privately-owned and operated critical infrastructure?
30. What are your expectations of the State and Federal Government?
31. Describe your role in post-incident activity.
32. What is your role in restoring and/or maintaining public confidence?

<Exercise Title>

SitMan

Public Affairs

1. What are your public affairs concerns? Who is responsible for coordinating the public message? Is this process a part of any established plan?
 - a. How would your department respond to the local media reports?
 - b. What information are you sharing with citizens? Employees?
 - c. Are public information personnel trained to manage messaging related to cyber incidents?
 - d. Does your department have pre-drafted statements in place to respond to media outlets?
 - e. Are they trained to manage your social media presence?
 - f. Are all personnel trained to report any contact with the media to appropriate public information personnel?
2. What information would your organization communicate to the public? How would you communicate it?
3. Who is responsible for public information related to the incident? What training or preparation have they received?
4. How would your organization respond to the attempts at disinformation/misinformation concerning elections?
 - a. Does your organization have established public messaging processes as part of a larger communications plan?
 - b. How would your organization respond to the social media posts/rumors and local media reports? Would you use social media or respond by drafting statements?
 - c. What message are you sending employees?
 - d. Are personnel trained to report any contact with the media to the appropriate public information personnel?
5. How would you inform other entities of the fake websites and social media pages?
 - a. How would you contact social media platforms?
 - b. What issues or challenges have you had in working with them?
6. How would your organization respond to the emerging news and social media issues?
 - a. Does your organization have pre-approved messages for immediate release as part of a larger communications plan?
7. What steps are you taking before an incident to build relationships with the media and with voters before an incident happens?

<Exercise Title>

SitMan

Legal

1. What are the legal issues you must address?
2. What policies should your organization have? Does it exercise these policies? If so, how often?
3. What legal documents should your organization have in place (for example with third-party vendors)?
4. What is the role of the legal department in this scenario?
5. Does your state have security breach notification laws? If so, what do they include?
6. What are the consequences if you are unable to certify the official election results?
7. What processes are in place to collect evidence and maintain the chain of custody?

<Exercise Title>
SitMan

Section 4: Exercise Appendices

Planners are encouraged to fill in highlighted fields with exercise specific information. *This instructional page should be deleted.*

<Exercise Title>

SitMan

Appendix A: Exercise Schedule

Table 1: <Exercise Date> Exercise Schedule

Time	Activity
8:00 a.m.	Registration
8:30 a.m.	Welcome and Opening Remarks
8:45 a.m.	Cyber Threat Landscape Briefing
9:15 a.m.	Module 1
10:00 a.m.	Break
10:15 a.m.	Module 2
11:00 a.m.	Hotwash
11:30 a.m.	Closing Comments
12:00 p.m.	Adjourn

<Exercise Title>

SitMan

Appendix B: Acronyms

Table 2: Acronyms

Acronym	Definition
AAR	After-Action Report
APT	Advanced Persistent Threat
BMD	Ballot Marking Device
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
CTEP	Cyber Tabletop Exercise Package
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
DMV	Department of Motor Vehicles
DNS	Domain Name System
DRE	Direct Recording Electronic
EI-ISAC	Elections Infrastructure Information Sharing and Analysis Center
EMS	Election Management System
FBI	Federal Bureau of Investigation
HR	Human Resources
HSEEP	Homeland Security Exercise and Evaluation Program
ICS	Industrial Control System
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IS	Information Systems
IT	Information Technology
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCCIC	National Cybersecurity and Communications Integration Center
NCIRP	National Cyber Incident Response Plan
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NRF	National Response Framework
PII	Personally Identifiable Information
PPD	Presidential Policy Directive
SitMan	Situation Manual
SME	Subject Matter Expert
SLTT	State, Local, Tribal, and Territorial

<Exercise Title>
SitMan

Acronym	Definition
TA	Technical Alert
TLP	Traffic Light Protocol
TTX	Tabletop Exercise

Section 5: Informational Appendices

The following section includes background and example information related to cybersecurity threats and attacks, as well as relevant doctrine. Planners are encouraged to include relevant information as desired. *This instructional page should be deleted.*

Appendix C: Background Information

Phishing

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as:

- National disasters
- Epidemics and health scares
- Economic concerns
- Major political elections
- Holidays

Additional Resources

- <https://www.us-cert.gov/ncas/tips/ST04-014>
- <https://www.us-cert.gov/report-phishing>
- <https://www.dhs.gov/be-cyber-smart>
- <https://www.dhs.gov/stophinkconnect>

Distributed Denial of Service

Distributed Denial of Service (DDoS) attacks overload bandwidth and connection limits of hosts or networking equipment, specifically through a network of computers making excessive connection requests. DDoS attacks unfold in stages. First, a malicious actor infects a computer with malware that spreads across a network. This infected computer is known as the “master” because it controls any subsequent computers that become infected. The other infected computers carry out the actual attack and are known as “daemons.” The attack begins when the master computer sends a command to the daemons, which includes the address of the target. Large numbers of data packets are sent to this address, where extremely high volumes (floods) of data slow down web server performance and prevent acceptance of legitimate network traffic. The cost of a DDoS attack can pose severe loss of revenue or reputation to the victim.

More information on DDoS attack possibilities within each layer of the Open Systems Interconnection (OSI) Model, as well as traffic types and mitigation strategies, can be found in the resource list below.

Additional Resources

- <https://www.us-cert.gov/ncas/tips/ST04-015>
- <https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf>
- <https://www.cisecurity.org/wp-content/uploads/2017/03/Guide-to-DDoS-Attacks-November-2017.pdf>

Social Engineering

One of the most prominent tactics attackers 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. Techniques for uncovering this information largely involve the use of phishing, i.e. email or malicious websites that solicit

<Exercise Title>

SitMan

personal information by posing as a trustworthy source. Social engineering is effective for breaching networks, evading intrusion detection systems without leaving a log trail, and is completely operating system platform dependent. 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, know where to forward them and keeping software and systems up-to-date.

Additional Resources

- <https://www.us-cert.gov/ncas/tips/ST04-014>

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. 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

- <https://www.us-cert.gov/Ransomware>
- https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf
- https://www.us-cert.gov/sites/default/files/2019-07/Ransomware_Statement_S508C.pdf
- <https://www.us-cert.gov/ncas/tips/ST19-001>

Appendix D: Cybersecurity Doctrine and Resources

Federal Laws

- National Cybersecurity Protection Act of 2014 (Dec 2014)
<https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf>
- Federal Information Security Modernization Act of 2014 (Dec 2014)
<https://www.dhs.gov/fisma>

Presidential Directives

- Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017)
<https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>
- Presidential Policy Directive-41: United States Cyber Incident Coordination (Jul 2016)
<https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>
- Annex to Presidential Policy Directive-41: Annex to the Directive on United States Cyber Incident Coordination (Jul 2016)
<https://www.hsdl.org/?view&did=797545>
- Presidential Policy Directive-8: National Preparedness (Mar 2011), (Updated Sep 2015)
<https://www.dhs.gov/presidential-policy-directive-8-national-preparedness>
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Feb 2013)
<https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013)
<https://www.hsdl.org/?view&did=731040>

Strategies and Frameworks

- National Cyber Incident Response Plan (Dec 2016)
<https://www.us-cert.gov/ncirp>
- National Cyber Strategy of the United States of America (Sep 2018)
<https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
- U.S Department of Homeland Security Cybersecurity Strategy (May 2018)
<https://www.hsdl.org/?view&did=810462>
- Framework for Improving Critical Infrastructure Cybersecurity (Apr 2018)
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- National Protection Framework, Second Edition (Jun 2016)
https://www.fema.gov/media-library-data/1466017309052-85051ed62fe595d4ad026edf4d85541e/National_Protection_Framework2nd.pdf

<Exercise Title>
SitMan

- A Guide to Critical Infrastructure Security and Resilience (Nov 2019)
<https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience>

Key Points of Contact

- Department of Homeland Security/Cybersecurity and Infrastructure Security Agency (CISA) (contact: CISAServiceDesk@cisa.dhs.gov; (888) 282-0870)
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) (contact: SOC@cisecurity.org; (866) 787-4722)
- 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>)
 - National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; (855) 292-3937)
- United States Secret Service Field Offices and Electronic Crimes Task Force (ECTFs) (contact: <https://www.secretservice.gov/contact/field-offices/>)

Other Available Resources

- Best Practices for Securing Election Systems (<https://www.us-cert.gov/ncas/tips/ST19-002>)
- Best Practices for Victim Response and Reporting of Cyber Incidents (<https://www.justice.gov/criminal-ccips/file/1096971/download>)
- Election Security Resource Library (<https://www.dhs.gov/publication/election-security-resource-library>)
- The War on Pineapple: Understanding Foreign Interference in 5 Steps (https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf)
- Handbook for Elections Infrastructure Security (<https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf>)
- Cybersecurity and the States (National Association of State Chief Information Officers [NASCIO]) (<http://www.nascio.org/Advocacy/Cybersecurity>)
- National Association of State Election Directors (NASED) (<https://www.nased.org/>)
- National Association of Secretaries of State (NASS) (<https://www.nass.org/>)
- NASS Cyber Resource Guide (https://www.nass.org/sites/default/files/Cybersecurity/10.11_NASS_Cyber_Resource_Guide.pdf)
- Belfer Center Defending Digital Democracy State and Local Election Cybersecurity Playbook (<https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook>)

<Exercise Title>
SitMan

- National Governors Association (NGA) Resource Center for State Cybersecurity ([https://www.nga.org/bestpractices/divisions/hspss/statecyber/DHS Cybersecurity Fusion Centers](https://www.nga.org/bestpractices/divisions/hspss/statecyber/DHS%20Cybersecurity%20Fusion%20Centers)) (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)
- InfraGard (<https://www.infragard.org/>)
- Internet Security Alliance (<http://www.isalliance.org/>)