Cyber Incident Detection and Notification Planning Guide for Election Security

July 2020

Contents

Introduction 1

Document Organization 2

Plan Development Guidance 3

- Overview 3
- Development and Implementation 4
- Step 1: Identify Stakeholders 4
- Step 2: Develop Notification Plans 5
- Step 3: Develop Symptom Criticality Tables 5
- Step 4: Review and Finalize Plan 6
- Step 5: Distribute and Integrate the Plan 7
- Step 6: Utilize Available Services and Resources 8

Appendix A: Key Stakeholders and Contact Information Worksheets A-1

Appendix B: Cyber Incident Detection and Notification Plan Template B-1

This Page Intentionally Left Blank

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) provides guidance and technical assistance upon request to officials responsible for safeguarding election infrastructure. Several state and local officials have identified a need for assistance in improving cyber incident response. Effective cyber incident response requires that those with access to elections systems and those responsible for responding to an incident understand how to detect a potential incident, their role in reporting and/or responding to the incident, and what procedures they should follow to mitigate potential impacts. A cyber incident response plan, along with sufficient resourcing, training, and exercising of the plan, is an essential tool for jurisdictions to enable this understanding among system users and incident responders.

There is no one-size-fits-all approach for developing a cyber incident response plan. While some election offices are directly responsible for a large portion of the incident response capability for their systems, many (particularly in small and medium size jurisdictions) rely on vendors or other agencies for activities such as system monitoring, analysis, containment, eradication, and recovery. The structure, scope, and level of detail required for an incident response plan varies widely based on these and other factors. Regardless, **all election offices play a critical role in detection of potential cyber incidents—based on system user observations—and notification of appropriate stakeholders**.

Technical Assistance

CISA offers a range of resources and services—such as assessments, trainings, exercises, and planning assistance—to help state and local election officials evaluate cybersecurity practices and identify opportunities to strengthen security and resilience to threats. These voluntary services are available upon request at no cost. Refer to the CISA's *Elections Infrastructure Security Resource Guide* for additional details.

This *Cyber Incident Detection and Notification Planning Guide* focuses on the common need shared across the election community to effectively recognize and respond to potential cyber incidents. Specifically, the guide builds on existing materials offered by the Nation's election security thought leaders to assist election offices in determining and documenting the following:

- **Key stakeholders and contact information** for incident notification and response
- **Incident notification plans** providing standardized procedures for notifying appropriate stakeholders of a potential cyber incident based on observed symptoms and level of criticality
- **Incident indicators ("symptoms")** system users can reference to detect potential cyber incidents and initiate the appropriate notification plan for escalation and reporting

Election offices can use this information as a basic cyber incident response plan or integrate the information into a broader plan based on their specific needs.

Document Organization

This document consists of the following three sections:

- ***Plan Development Guidance*** provides context and instructions for developing a *Cyber Incident Detection and Notification Plan* using the templates and tools provided in the appendices.
- ***Appendix A – Key Stakeholders and Contact Information Worksheets*** provides a series of worksheets for identifying stakeholders who will be included in the *Cyber Incident Detection and Notification Plan* and their contact information.
- ***Appendix B – Cyber Incident Detection and Notification Plan Template*** provides a fillable template that can be completed by election offices following the instructions in this guide. The template includes prepopulated Symptom Criticality Tables that provide example descriptions of the indicators a system user would observe, corresponding notification plans, and potential troubleshooting/mitigation solutions for a variety of potential incident symptoms. Election officials can utilize, modify, or add to, these examples as appropriate in developing the symptom criticality tables section of their *Cyber Incident Detection and Notification Plan*.

  The completed template serves as a stand-alone "tear-away" product that jurisdictions can distribute to stakeholders in electronic or print format, or as a reference to inform broader incident response plans. Election offices can modify and update these plans as staff and processes change to adapt to the dynamic election environment.

Plan Development Guidance

Overview

Early detection of a security incident and notification to the appropriate stakeholders can be vital to mitigating incident impacts. The *Cyber Incident Detection and Notification Plan* template provided in this guide is designed to expedite incident detection based on the observations of system users and notification through the application of two key concepts—

> ***Security Incident Symptom***
>
> For the purposes of this document, a "symptom" is defined as something users may observe or reported evidence that may be indicative of a potential security threat or incident.

- **Symptoms-based incident detection** focuses on detecting "symptoms" a user would experience during a security incident or other IT-related failure; it does not require the user to diagnose the cause of a system abnormality, only to notify the appropriate stakeholders. This is important for two reasons—(1) many election systems users may not have the expertise to properly diagnose or mitigate an incident such as a cyber-attack, and (2) a symptom that on its own typically indicates a routine or innocuous issue may reveal a more severe criticality if properly reported and observed across multiple systems or in combination with other symptoms.
- **Criticality-based notification procedures** distinguish the appropriate notification procedures and channels based on whether symptoms indicate a routine, suspicious, or potentially critical cyber incident. This helps provide a pathway for all incidents to be tracked, prevents key stakeholders and decision-makers from getting overwhelmed with reports and support requests for low risk incidents, and expedites reporting and response for critical incidents. Table 1 describes the three levels of criticality used in the *Cyber Incident Detection and Notification Plan Template*.

Table 1: Symptom Criticality Levels[1]

Criticality Level	Description
Routine	Incident may cause minor system disruptions that will likely not be visible to the public or affect the elections process.
Suspicious	Possibly due to a cyber incident resulting in a disruption in the election process, but formal notification obligations may not be triggered. The issue begins to become public.

[1]Routine, suspicious, and critical cyber incident criticality levels adapted from cyber incident severity levels (low, medium, high) described in Belfer Center's *Election Cyber Incident Communications Plan Template*.

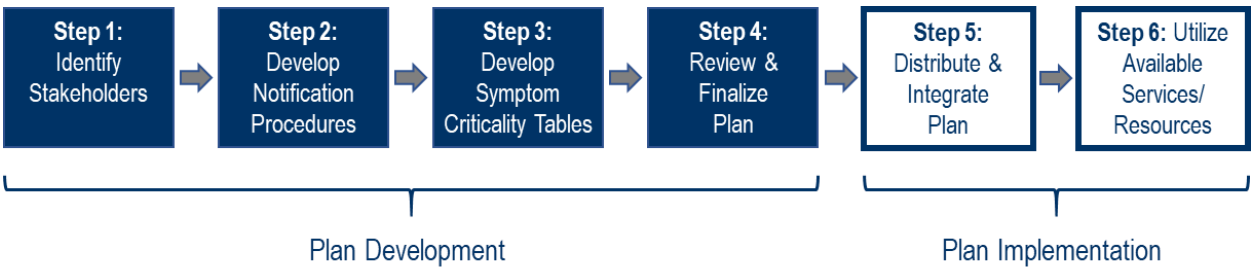
Criticality Level	Description
Critical	Highly likely to be indicative of a cyber incident that triggers national-level reporting obligations, affects a large amount of voter information, and/or is destructive to election operations.

Development and Implementation

This guide outlines a six-step process (Figure 1) election offices can use for developing and implementing a *Cyber Incident Detection and Notification Plan* utilizing the concepts above. This process is envisioned to be led by an election official for the jurisdiction or his/her designee, and each step is designed to be carried out in collaboration with the appropriate Incident Response Team and Incident Response Communications Team, herein referred to collectively as the ***Planning Team***. If these teams have not yet been designated for the jurisdiction, the election official leading this effort should identify a Planning Team composed of individuals such as state and local election staff, IT managers, and vendor representatives who should be involved in determining appropriate stakeholders and procedures for incident reporting and response.

In addition to identifying the Planning Team, the Election Official should determine how and when (e.g., workshop) the Planning Team will collaborate in carrying out each step of the process. You can request CISA resources and direct subject matter expert assistance in facilitating this process by contacting your state election official or regional CISA representative (https://www.cisa.gov/cisa-regional-offices).

Figure 1: Plan Development and Implementation Steps



Step 1: Identify Stakeholders

Election officials should coordinate with applicable state and local elections staff and IT personnel to complete *Appendix A: Key Stakeholders and Contact Information Worksheets*. The worksheet captures names and contact information for individuals and organizations who should be notified of potential security incidents to facilitate effective and timely reporting and response. It is a best practice to identify and train primary and backup points of contacts; as such, the worksheet provides space to record information for both, as applicable. The information collected through this process will be used to support the creation of incident notification procedures in Step 2.

Instructions:

- Using the tables in *Appendix A: Key Stakeholders and Contact Information Worksheets*, designate key stakeholders who should be notified of potential security incidents. You do not need to identify someone for each category if not applicable, and you can add additional rows/categories as needed. Fill out a vendor/system-specific worksheet for each election-related system that has non-governmental individuals who you believe should be included. You can modify and update these plans as staff and processes change to adapt to the dynamic election environment.

Step 2: Develop Notification Plans

Incident notification plans are developed by each jurisdiction to provide election system users and other stakeholders with step-by-step instructions on who to contact and how to contact them when a symptom that may indicate a security incident is observed. Election officials should work with the Planning Team to customize incident notification plans for their jurisdiction. The incident notification plans section of *Appendix B – Cyber Incident Detection and Notification Plan Template* provides a template for creating tiered plans based on the level of criticality—routine, suspicious, or critical—of the observed symptoms.

Instructions:

- Complete all applicable fields in the notification plans section of *Appendix B* using the key stakeholders and contact Information documented in Step 1. Jurisdictions may customize the notification plans to reflect their capacity to manage incidents at various levels of criticality.
- Review and practice all plans with applicable stakeholders to ensure their awareness of roles and responsibilities for incident response and to validate the procedures before finalizing.

Step 3: Develop Symptom Criticality Tables

Symptom criticality tables list abnormal system behaviors or activities that a system user may observe, and provides the user with common guidance for initial triaging and troubleshooting of those abnormalities so that they can initiate the appropriate notification plan based on level of criticality—routine, suspicious, or critical. Utilizing *Appendix B – Cyber Incident Detection and Notification Plan Template*, election officials should work with the Planning Team to develop symptom criticality tables for each election system or system type used by their jurisdiction.

The Symptom Criticality Tables included as part of *Appendix B – Cyber Incident Detection and Notification Plan Template* have been prepopulated to provide examples the planning team may use as inspiration for development of custom symptom criticality tables or they can directly reference, utilize, modify, or add to these examples as appropriate in developing the tables for their plan. The example tables provide some common symptoms that may be observed if a cyber incident occurs. The tables are designed to help users recognize the level of criticality, distinguish the correct notification plan, and perform initial troubleshooting steps for specific symptoms they may observe on election systems.

Jurisdictions may elect to use the prepopulated examples but should review and customize the content to align organization policies and IT standard operating procedures and notification requirements.

Note: The examples do not represent all potential threats to election technology infrastructure, and election officials and staff should report any suspicious system or network activity according to their organization's policies.

Instructions:

- Review the prepopulated Symptom Criticality Tables in Appendix B which provide example observations, troubleshooting tips, and notification plans for common symptoms that a user may experience for various asset, system, or system types.
- Use the examples as a reference to help identify each critical asset, system, or system type for which symptom criticality tables will be developed for your jurisdiction.
- Develop a list of potential incident symptoms a user may observe for each of the identified assets, systems, or system types. Use the provided common examples of symptoms as inspiration when developing symptom lists or leverage them directly and modify as appropriate.
- In coordination with the planning team, create a symptom criticality table for each symptom using the *Cyber Incident Detection and Notification Plan* template in Appendix B. The team may choose to leverage the prepopulated example tables in Appendix B as appropriate. Each symptom criticality table should provide the following:
    - ***Observations*** – Specific system behaviors or activities the user may observe that describe the symptom in more detail to help determine the level of criticality.
    - ***Notification Plan*** – The specific plan the user should initiate based on the level of criticality indicated by the observation.
    - ***Possible Troubleshooting*** – Additional actions the entity detecting the incident, or first line responder should take to potentially mitigate impacts of the incident and/or to enable the user to provide additional information helpful to incident responders.

Step 4: Review and Finalize Plan

Once the notification plans and symptom tables are complete, election officials should fill in the remaining customizable fields in *Appendix B – Cyber Incident Detection and Notification Plan Template.* Jurisdictions are encouraged to insert their *Election Day Emergency Response Guide (EDERG)* where indicated in the template if they already have one, or to work with CISA to develop an EDERG that can be included. An EDERG can serve as a tool for developing your planning teams and notification plans, so your jurisdiction may want to consider developing this product in advance of or in conjunction with the development of the *Cyber Incident Detection and Notification Plan*.

Election Day Emergency Response Guide (EDERG)

An EDERG provides response steps and contact information for a variety of election security incidents. This customized product can be developed by state and local election officials with free support from CISA.

Election officials should review the completed plan with every member of the Planning Team, incorporate feedback, and finalize the document.

Instructions:

- ☐ Fill in the remaining customizable fields in Appendix B.
- ☐ Insert EDERG where indicated in Appendix B. Contact CISA if your jurisdiction does not have a current EDERG (see Step 6 for more information).
- ☐ Review draft plan with appropriate stakeholders, incorporate feedback, and finalize document.

Step 5: Distribute and Integrate the Plan

Appendix B – Cyber Incident Detection and Notification Plan Template is designed to be printed or shared electronically as a stand-alone document once completed, and/or the information may be integrated into other incident response planning documents, policies, and procedures as appropriate. Election officials should provide copies of the completed plan to system users, incident responders, and other stakeholders. Election officials should train users and other stakeholders on how to implement the plan, exercise the plan regularly, and update the plan after completing exercises to incorporate the lessons learned in the exercise.

Instructions:

- ☐ Provide printed and/or electronic copies of your final *Cyber Incident Detection and Notification Plan* to system users, incident responders, and other stakeholders who are directly involved in the detection and/or notification process.
- ☐ Integrate the information documented in the *Cyber Incident Detection and Notification Plan* into related plans, policies, procedures, etc. (e.g., existing Incident Response Plans), as appropriate.
- ☐ Develop and implement a training plan to ensure system users and other stakeholders understand how and when to use the *Cyber Incident Detection and Notification Plan.* Contact your CISA representative for additional information or assistance as needed.
- ☐ Develop and implement an exercise plan to recognize resource and training gaps and to ensure system users and other stakeholders are prepared to use the *Cyber Incident Detection and Notification Plan*. Contact your CISA representative for additional information or assistance as

needed. The CISA Exercise Team can also assist in the development and implementation of a custom exercise (see Step 6 for more information).

Step 6: Utilize Available Services and Resources

CISA and other entities at the national and state level provide an array of services and resources to assist state and local jurisdictions with their election security needs—often free of charge. In addition to this guide, CISA offers various services and resources to assist election officials with incident response planning, including EDERG development, response plan training and exercises, and information on federal incident response services. For a complete list of CISA services and resources for election officials, go to https://www.cisa.gov/protect2020.

Appendix A: Key Stakeholders and Contact Information Worksheets

Government Stakeholder Contacts Worksheet

Election Division INTERNAL System Leads

Partner/ Stakeholder	Name and Affiliation	Contact Information (Phone and Email)
Director	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Deputy Director	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Election Official	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Program Manager	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Information Technology	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Communications	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
CISO	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Voting System Lead	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
E-Pollbook Lead	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]

Partner/ Stakeholder	Name and Affiliation	Contact Information (Phone and Email)
Website Lead	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
ENR Lead	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Election Day Command Center	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
UOCAVA MOVE Act Solution	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]

NOTES:

Additional County Stakeholders

Partner/ Stakeholder	Name and Affiliation	Contact Information (Phone and Email)
County IT	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
County CISO	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
County Comms	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
County Exec	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]

Partner/ Stakeholder	Name and Affiliation	Contact Information (Phone and Email)
County Legal	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
County Law	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]

NOTES:

State Stakeholders

Partner/ Stakeholder	Name and Affiliation	Contact Information (Phone and Email)
SOS POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
State Elec Dr. POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Elections SOC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Other Emer. Man. POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
State Information Sharing and Analysis Center	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
State IT	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]

Partner/ Stakeholder	Name and Affiliation	Contact Information (Phone and Email)
State Legal	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
State Law	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]

NOTES:

Federal & 3rd Party Partners

Partner/ Stakeholder	Name and Affiliation	Contact Information (Phone and Email)
General CISA Reporting	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Regional CISA POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Social Media POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
EI-ISAC POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Local FBI POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]

NOTES:

Vendor/System-Specific Stakeholder Worksheet

System:	[Insert System Name]
Vendor and Version:	[Insert Vendor and Version]
Components:	[Insert Components]

Partner/ Stakeholder	Name and Affiliation	Contact Information (Phone and Email)
County Web Host POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
County Tech. POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
County Exec. POC.	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Vendor POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Vendor Tech. POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Vendor Exec POC	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]

NOTES:

This Page Intentionally Left Blank

Appendix B: Cyber Incident Detection and Notification Plan Template

The following template can be completed by election jurisdictions following the instructions in this guide. The completed template is intended to serve as a stand-alone "tear-away" product that jurisdictions can distribute to stakeholders in electronic or print format, or as a reference to inform broader incident response plans. Election officials can modify and update these plans as staff and processes change to adapt to the dynamic election environment.

Additional support in developing, training on, or exercising the plan can be requested through your state election official or regional CISA representative (https://www.cisa.gov/cisa-regional-offices).

This Page Intentionally Left Blank

[Insert Jurisdiction Name]

Election Security
Cyber Incident Detection and Notification Plan

Version [Insert Version Number]

Released [Insert Release Date]

Approved by [Insert Approving Authority]

Election Security is a shared responsibility between state and local election administrators, other state and local government entities, vendors, election workers, federal partners, and American citizens. Each of us play a critical role in ensuring that the Nation's election infrastructure, including its systems, networks, physical spaces, and processes, is guarded from adversaries and cybersecurity threats.

The purpose of this plan is to provide election staff, election system users, incident responders, and incident communications responders with a common plan for (1) detection of potential security incidents, and (2) timely notification of the appropriate stakeholders.

The plan is organized into the following sections:

1. **How to use this Plan** ***(Pages [Insert Page Number(s)])***
   Instructions for election officials, staff, and election system users for maintaining and implementing this plan.

2. **Incident Symptom Tables** ***(Pages [Insert Page Number(s)])***
   Election staff and systems users should reference these tables whenever any abnormal or suspicious behavior or activity (i.e., symptom) is observed on an election-related system to determine level of criticality.

3. **Incident Notification Plans** ***(Pages [Insert Page Number(s)])***
   All observed symptoms constitute an incident and must be reported to the appropriate stakeholders using the notification plans in this section. Notification plans are specific to the level of criticality.

4. **(OPTIONAL) Election Day Emergency Response Guide** ***(Pages [Insert Page Number(s)])***
   Provides response steps and contact information for additional incident types including severe weather, fire alarms, and violent incidents.

1. How to Use This Plan

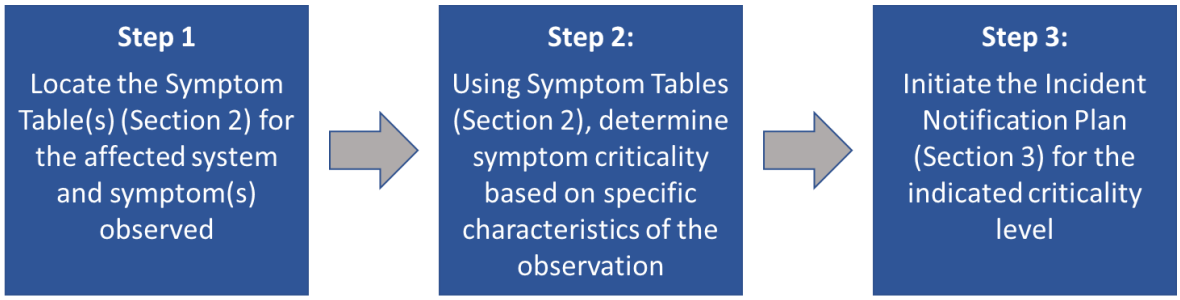
Election Officials

Review this plan periodically to ensure it is up to date, and distribute this plan to all election staff, election system users, incident responders, and incident communications responders. Also ensure these stakeholders are properly trained on this plan and that the plan is exercised regularly. Additional support in updating, training, or exercising the plan can be requested through your state election official or regional CISA representative (https://www.cisa.gov/cisa-regional-offices).

Election Staff and Election System Users

Review this plan upon receipt and at least monthly thereafter to ensure you are familiar with the content. Refer to this plan whenever you observe or are made aware of any abnormality (i.e., symptom) related to an election system. Using the Incident Symptom Tables in Section 2, locate the symptom and specific observation(s) to determine the criticality of the symptom. Based on the indicated level of criticality, initiate the corresponding Incident Notification Plan found in Section 3 as soon as possible.

Whenever you observe or are made aware of any abnormality (i.e., symptom) related to an election system, you must do the following:



How to use the Incident Symptom Tables

- Locate the Incident Symptom Table for the affected system and symptom you are experiencing
- Identify the observation listed in the Symptom Table that most closely describes what you are experiencing to determine the level of criticality
- Initiate the Initiate the Notification Plan found in Section 3 for the indicated criticality level

Note: Symptoms may have explanations unrelated to technology; however, following the relevant notification plan is important to engage the appropriate stakeholders to review and assess the situation. Always follow internal policies and procedures and contact your IT administrator if you are unsure whether you should follow any action described herein.

Symptom Criticality Table Index: [Update Index Below as Needed]

Voter Registration & Polling Observations 5

Symptom: Large Number of Voters Are Not Listed in the Pollbook 5

Symptom: Unusually High Number of Provisional Ballots Distributed 5

Voting Machine & Equipment Observations 6

Symptom: Voting Machine Equipment Not Operating Properly 6

Symptom: Voting Machine Equipment Is Not Accepting/Not Reading Ballots 6

Symptom: Voting Machine Is Not Marking the Vote Selected on Touchscreen 7

Symptom: Voter's Selection on Voting Machine Does Not Match Paper Printout 7

IT Systems & Device Observations 8

Symptom: Files Encrypted and Ransom Requested 8

Symptom: Computer Will Not Load Web-based Software Applications 8

Symptom: Computer Slow to Respond 9

Symptom: Computer Slow When Accessing Local Network 9

Symptom: Computer Crashes or Frequently Displays "Blue Screen of Death" (BSOD) 10

Symptom: Browser Takes You to Strange Webpages 10

Symptom: Unable to Log In to Account 11

Symptom: "Local Storage Is Full" Error 11

Symptom: Dialog Boxes with Strange, Unexpected Text or Gibberish 12

Symptom: Warning That Anti-Virus/Anti-Malware Software Is Disabled 12

Symptom: Warning that the Computer is Infected and a New Anti-Virus Must Be Installed 13

Symptom: Strange System Warnings or a Large Number of Pop-Ups 13

Symptom: Your Cursor Moving on Its Own and/or Programs Are Starting on Their Own 13

Symptom: Unable to Access the Control Panel or Other System Tools on Your Computer 14
Symptom: Desktop Icons Have Changed/Moved or New Icons Have Been Added 14
Symptom: Jurisdiction Website or Social Media Account Showing Erroneous Information 15
Symptom: Non-Official Social Media Accounts Are Presenting Erroneous Information 15
Symptom: Suspicious Email from a Legitimate Company Requesting Sensitive Information 15

Voter Registration & Polling Observations

Symptom: Large Number of Voters Are Not Listed in the Pollbook

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] A large number of voters (self-identified or with registration card) are not listed in the pollbook	**Suspicious**	[Edit as Needed] ▪ Follow jurisdiction policies and procedures for a voter that is not in the pollbook ▪ Report incident to Election Office, which will verify registration in the Voter Registration Database
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Unusually High Number of Provisional Ballots Distributed

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] High demand for and distribution of provisional ballots	**Suspicious**	[Edit as Needed] ▪ Acquire additional provisional ballots and continue to distribute as needed
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Voting Machine & Equipment Observations

Symptom: Voting Machine Equipment Not Operating Properly

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] Voting machine or equipment is not displaying information or is otherwise not operating as it should, but it was not previously operating as normal	**Routine**	▪ Confirm the machine is plugged in or that the battery is charged ▪ Consult Standard Troubleshooting Protocols ▪ Seek subject matter expert (SME) or vendor support as necessary
[Edit as Needed] Voting machine/equipment is not displaying information or is otherwise not operating as it should. It was previously working as it should and is plugged in or has a charged battery	**Suspicious**	[Edit as Needed] ▪ Seek subject matter expert (SME) or vendor support as necessary
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Voting Machine Equipment Is Not Accepting/Not Reading Ballots

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] Voting equipment is not accepting or reading ballots	**Routine**	[Edit as Needed] ▪ Consult Voting Equipment Standard Operating Procedures ▪ Confirm the equipment is plugged in or has a charged battery ▪ Seek SME or vendor support as necessary
[Insert Observation if Applicable]	**Suspicious**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Voting Machine Is Not Marking the Vote Selected on Touchscreen

Observation	*Notification Plan*	*Possible Troubleshooting*
[Edit as Needed] Voting machine not responding accurately to touch/not registering sections as indicated.	***Routine***	[Edit as Needed] ▪ Refer to Voting Machine Standard Operating Procedures and follow steps to calibrate machine ▪ Return machine to service if recalibration fixed the issue
[Edit as Needed] Voting Machine not responding accurately to touch/not registering sections as indicated after re-calibration.	***Suspicious***	[Edit as Needed] ▪ Alert vendor POC
[Insert Observation if Applicable]	***Critical***	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Voter's Selection on Voting Machine Does Not Match Paper Printout

Observation	*Notification Plan*	*Possible Troubleshooting*
[Edit as Needed] Voters report inconsistencies in vote selections and paper printout generated for submission from a single machine	***Routine***	[Edit as Needed] ▪ Remove affected machine from service
[Edit as Needed] Voters report inconsistencies in vote selections and paper printout generated for submission from several machines.	***Suspicious***	[Edit as Needed] ▪ Resort to contingency plans (i.e., paper ballots) ▪ Remove all machines from service
[Edit as Needed] Voters report inconsistencies in vote selections and paper printout generated for submission from several machines, and there are no contingency plans/processes to collect votes via other methods	***Critical***	[Edit as Needed] ▪ Not Applicable

IT Systems & Device Observations

Symptom: Files Encrypted and Ransom Requested

Observation	*Notification Plan*	*Possible Troubleshooting*
[Insert Observation if Applicable]	***Routine***	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	***Suspicious***	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] You see a screen saying that the files on the computer are encrypted and that you must pay a fine or other payment to get the files back	***Critical***	[Edit as Needed] ▪ Immediately unplug the network cable from the computer ▪ Do NOT unplug or power down the computer

Symptom: Computer Will not Load Web-based Software Applications

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] Your browser will not load a webpage	**Routine**	[Edit as Needed] ▪ Make sure all cables are firmly in their sockets ▪ Restart the device ▪ If using Wi-Fi, make sure you are on the correct network
[Edit as Needed] Your browser will load some webpages but not others	**Routine**	[Edit as Needed] ▪ Refresh unresponsive site ▪ Check for reports of other users having problems with the site ▪ Contact customer support for the website or application for outage information
[Edit as Needed] Your browser will not load any webpages	**Suspicious**	[Edit as Needed] ▪ Make sure all cables are firmly in their sockets ▪ Restart the device ▪ If using Wi-Fi, make sure you are on the correct network
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Computer Slow to Respond

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] Your computer is slow to respond	**Routine**	[Edit as Needed] ▪ Restart the computer ▪ Check to see how many applications are running ▪ Close open applications not in use
[Edit as Needed] You restarted your computer, but it is still slow to respond	**Suspicious**	[Edit as Needed] ▪ Not Applicable
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Computer Slow When Accessing Local Network

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] Your computer is slow when you are trying to print, open, or save files, but you can still access webpages.	**Routine**	[Edit as Needed] ▪ Restart the computer ▪ Make sure you are logged onto the network ▪ Make sure the printer is on and connected
[Edit as Needed] Your computer is slow when you are trying to print, open, or save files, and you cannot access any webpages.	**Suspicious**	[Edit as Needed] ▪ Restart computer ▪ Make sure all cables are firmly in their sockets ▪ Make sure the printer is on and connected ▪ Make sure you are logged onto the network ▪ Make sure you are connected to the right Wi-Fi network
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Computer Reboots or Frequently Displays "Blue Screen of Death" (BSOD)

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] The computer, which is new and has had new programs installed, reboots more than 1x per day without notice and/or displays the BSOD	**Routine**	[Edit as Needed] ▪ Not Applicable
[Edit as Needed] The computer reboots more than 1x per day without notice and/or displays the BSOD. The computer is not new and has not had new programs installed	**Suspicious**	[Edit as Needed] ▪ Not Applicable
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Browser Takes You to Strange Webpages

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] The web browser is redirecting you to sites that you did not type in or choose to go to	**Routine**	[Edit as Needed] ▪ Do NOT click on any links or files in the site that the browser takes you to ▪ Do NOT visit important sites while the browser is acting strangely ▪ IT staff can remove what may be browser hijacker malware
[Insert Observation if Applicable]	**Suspicious**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Unable to Log In to Account

Observation	Notification Plan	Possible Troubleshooting
[Edit As Needed] You are locked out of your computer; your current username and password are not working. You recently received a notification that your password will expire soon or a notice to reset it.	**Routine**	[Edit as Needed] ▪ Confirm with IT and have account reset
[Edit as Needed] You are locked out of your computer; your current username and password are not working. You have received a notification about a password expiring or being changed, even though the password has been working.	**Suspicious**	[Edit as Needed] ▪ IT will help reset account and determine if additional investigation is needed ▪ Pay special attention to how the computer acts over the next week and report any odd behavior to IT
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: "Local Storage Is Full" Error

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] You receive a warning that the local storage on the computer is nearly full after storing large amounts of data on the computer (e.g. image or video files)	**Routine**	[Edit as Needed] ▪ Look at the space being consumed by large files and move some (or all) to a backup device if possible
[Edit as Needed] You receive a warning that the local storage on the computer is nearly full, but you are not storing large amounts of data on the computer	**Suspicious**	[Edit as Needed] ▪ Not Applicable
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Dialog Boxes with Strange, Unexpected Text or Gibberish

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] You receive dialog boxes with strange, unexpected text or gibberish	**Suspicious**	[Edit as Needed] ▪ Do NOT click anywhere in the box – not even in the 'X' in the upper corner to close the box ▪ Take a screenshot of the box and right-click on the toolbar at the bottom of the screen to close only if you must continue to work ▪ Leave the computer alone until IT staff arrive
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Warning That Anti-Virus/Anti-Malware Software Is Disabled

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] You receive a warning that the anti-virus/anti-malware software is disabled after recently installing a piece of legitimate software that prompted you to disable anti-virus protection for the installation	**Routine**	[Edit as Needed] ▪ Not Applicable
[Edit As Needed] You receive a warning that the anti-virus/anti-malware software is disabled but do not remember recently installing a piece of legitimate software that prompted you to disable anti-virus protections for the installation	**Suspicious**	[Edit as Needed] ▪ Not Applicable
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Warning that the Computer is Infected and a New Anti-Virus Must Be Installed

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	**Suspicious**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] You receive a warning that your computer is infected, and a new anti-virus program must be installed to clean the infection	**Critical**	[Edit as Needed] ▪ Do NOT click anywhere in or near the dialog, pop-up, or warning box ▪ If you must continue to work, close the box by right-clicking the toolbar at the bottom of the screen and selecting "close"

Symptom: Strange System Warnings or a Large Number of Pop-Ups

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] You receive strange system warnings or a large number of pop-ups	**Suspicious**	[Edit as Needed] ▪ Not Applicable
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Your Cursor Moving on Its Own and/or Programs Are Starting on Their Own

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	**Suspicious**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] Your Cursor is moving on its own, and/or programs are starting that you have not opened	**Critical**	[Edit as Needed] ▪ Not Applicable

Symptom: Unable to Access the Control Panel or Other System Tools on Your Computer

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] You are unable to access the control panel or other system tools (e.g. task manager, settings). However, you have not been able to access these in the recent past	**Routine**	[Edit as Needed] ▪ Not Applicable
[Insert Observation if Applicable]	**Suspicious**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] You are unable to access the control panel or other system tools (e.g. task manager, settings), which you have been able to access in the recent past	**Critical**	[Edit as Needed] ▪ Not Applicable

Symptom: Desktop Icons Have Changed/Moved or New Icons Have Been Added

Observation	Notification Plan	Possible Troubleshooting
[Edit as Needed] Desktop icons have changed or moved, or new icons have been added, and you had trouble logging in to the computer	**Routine**	[Edit as Needed] ▪ Confirm that you logged in with the correct account and that you are connected to the network
[Edit as Needed] Desktop icons have changed or moved, or new icons have been added. You logged in with the correct account and are connected to the network	**Suspicious**	[Edit as Needed] ▪ Not Applicable
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Jurisdiction Website or Social Media Account Showing Erroneous Information

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] Jurisdiction website or official social media account with voting information (e.g. dates, locations, times) is showing erroneous information	**Suspicious**	[Edit as Needed] ▪ IT will determine the cause of the erroneous information (malicious or accidental)
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Non-Official Social Media Accounts Are Presenting Erroneous Information

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] It appears that social media accounts not controlled by a government jurisdiction are maliciously or accidentally providing erroneous voting-related information	**Suspicious**	[Edit as Needed] ▪ Contact IT and the Social Media Liaison to coordinate with the social media provider to have the content and/or page removed
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: Suspicious Email from a Legitimate Company Requesting Sensitive Information

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Edit as Needed] The email is not addressed to the recipient. The email is in regard to an action that you have not performed (i.e., exceeded the number of login attempts for an account). The email request sensitive or personal identifiable information (PII) via email.	**Suspicious**	[Edit as Needed] ▪ Do not click any links or enter sensitive or PII ▪ Contact IT and report email. IT will determine which other users (if any) received the same email, if anyone fell victim to it, etc., and block/share associated indicators.
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

[Insert Additional System/Asset Name or Type]

Symptom: [Insert Additional Cyber Incident Symptom]

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	**Suspicious**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: [Insert Additional Cyber Incident Symptom]

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	**Suspicious**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: [Insert Additional Cyber Incident Symptom]

Observation	Notification Plan	Possible Troubleshooting
[Insert Observation if Applicable]	**Routine**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	**Suspicious**	▪ [Insert Possible Troubleshooting Actions if Applicable]
[Insert Observation if Applicable]	**Critical**	▪ [Insert Possible Troubleshooting Actions if Applicable]

Symptom: [Add additional Systems/Assets and Symptom Tables as needed]

Incident Notification Plans

The following Incident Notification Plans specify the procedures that must be followed when an incident symptom has been observed and contact information for the designated stakeholders who must be contacted. Plans are provided for the following levels of criticality:

- Routine IT Observations *(Page [Insert Page Number(s)])*
- Suspicious IT Observations *(Page [Insert Page Number(s)])*
- Critical IT Observations *(Page [Insert Page Number(s)])*

How to use the Incident Notification Plans

Initiate the Incident Notification Plan that corresponds to the level of criticality determined from the Incident Symptom Tables in Section 2. The selected plan should be completed in full.

Routine IT Observation Notification Plan

Phase	Action
Internal Alerting	**1a. Initial Observer Contacts Election Division IT support:** [Input Name and Contact Information]
Incident Escalation	**2a. Escalation actions likely not applicable** **Note:** *IT support staff may determine that it is necessary to contact IT Support Lead for diagnosis.* **2b. If IT diagnosis results in suspicious or critical incident proceed to implement communication and escalation actions in "Suspicious" or "Critical" tables, as applicable.**

Suspicious IT Observation Notification Plan

Phase	Action
Internal Alerting	**1a. Observer contacts Election Division IT support:** [Input Name and Contact Information] **1b. Observer notifies immediate supervisor(s) and supervisory Election Official of the potential breach:** [Input Name and Contact Information] **1c. Election Official identifies and assess potential impacts to business systems and initiates business continuity plans as necessary:** [Plan #1 – Input Execution Considerations] [Plan #2 – Input Execution Considerations] **1d. Election Official notifies internal division systems leads to provide mitigation instructions from IT, as applicable:** [Input System, POC Name, and Contact Information] [Input System, POC Name, and Contact Information]
Incident Escalation	**2a. Election Official notifies state division systems leads to provide mitigation instructions from IT, as applicable:** [Input Name and Contact Information] **2b. IT Support Lead determines if necessary to contact County and State IT for additional support in diagnosing impacts and determining a resolution:** [Input County IT Name and Contact Information] [Input State IT Name and Contact Information] **2C. If IT Support Lead confirms suspicious observation as critical, Election Official notifies appropriate state and federal POCs:** [Input State Election Authority Name and Contact Information] [Input CISA POC Name and Contact Information] [Input EI-ISAC POC Name and Contact Information]

Critical IT Observation Notification Plan

Phase	Action
Internal Alerting	**1a. Observer contacts Election Division IT Support Lead:** [Input Name and Contact Information] **1b. Observer notifies supervisor(s) and supervisory Election Official of the critical incident:** [Input Name and Contact Information] **1c. Election official identifies and assesses potential impacts to business systems and initiates business continuity plans as necessary:** [Plan #1 – Input Execution Considerations] [Plan #2 – Input Execution Considerations] **1d. Communications Director coordinates internal team to review and implement applicable emergency public relations and media communications strategies.**
Incident Escalation	**2a. Election Official immediately notifies appropriate state and federal partners of critical incident:** [Input State Election Authority Name and Contact Information] [Input State Information Sharing and Analysis Center Name and Contact Information] [Input State Emergency Management Name and Contact Information] [Input CISA POC Name and Contact Information] [Input EI-ISAC POC Name and Contact Information] [Input Local FBI POC Name and Contact Information] **2b. IT Support Lead contacts County and State counterparts to implement IT system mitigation actions:** [Input County IT Name and Contact Information] [Input State IT Name and Contact Information]

[Optional – Insert Election Day Emergency Response Guide]