Appendix A: Key Stakeholders and Contact Information Worksheets

The following worksheet can be completed by election jurisdictions following the instructions in the Cybersecurity and Infrastructure Security Agency (CISA) *Cyber Incident Detection and Notification Planning Guide for Election Security*.

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]

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

Partner/ Stakeholder	Name and Affiliation	Contact Information (Phone and Email)
	Backup: [Insert Backup Name and Affiliation]	
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 the Cybersecurity and Infrastructure Security Agency (CISA) *Cyber Incident Detection and Notification Planning Guide for Election Security*. 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

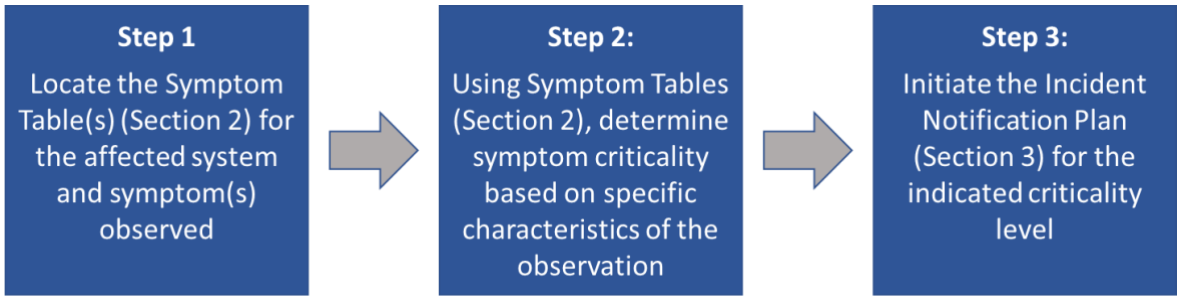
Election Officials

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

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]

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]