Cyber Incident Detection and Notification Planning Guide for Election Security

July 2020

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Contents

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 four 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*.

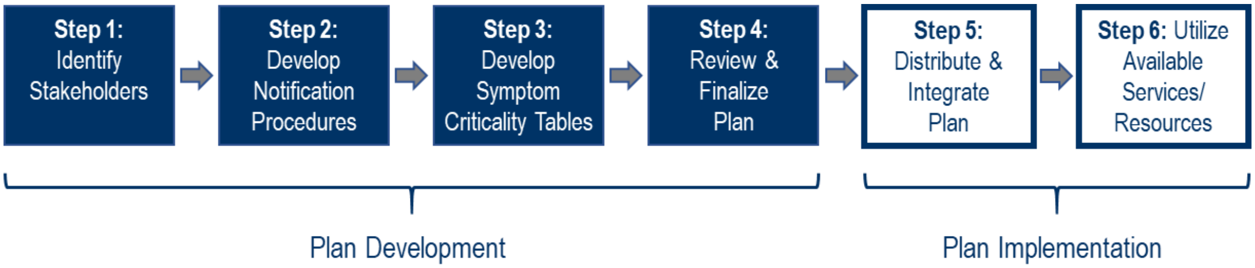
Criticality Level	Description
Critical	Highly likely to be indicative of a cyber incident that triggers national-level reporting obligations, affects a large amount of voter information, and/or is destructive to election operations.

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
Step 2: Develop Notification Procedures
Step 3: Develop Symptom Criticality Tables
Step 4: Review & Finalize Plan
Step 5: Distribute & Integrate Plan
Step 6: Utilize Available Services/ Resources
Plan Development
Plan Implementation

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.