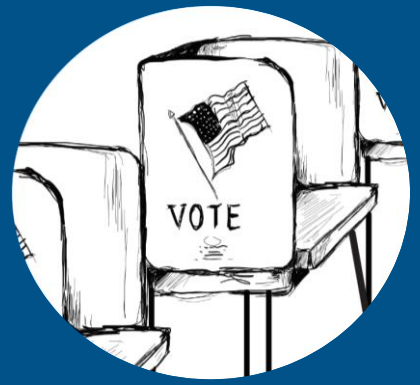
CYBER INCIDENT DETECTION AND RESPONSE DESK REFERENCE

OVERVIEW

CISA
CYBER+INFRASTRUCTURE

Matt Masterson
February 4, 2020

Agenda



1. Cyber Incident Detection and Response Desk Reference Overview
2. Case Study

CISA
CYBER+INFRASTRUCTURE

Desk Reference Overview

The ***Cyber Incident Detection and Response Desk Reference*** provides a go-to resource to support Election Officials respond to incident that could affect the election process.

- **General Emergency Response Steps**
- **Decision Trees** describing observable symptoms that could mean a potential incident has occurred
- **Customized Cyber Incident Notification Plans** for designated Incident Response Team stakeholders

Purpose

Detect **symptoms** of a potential cyber incident

Document response procedures to **minimize impacts**

Improve proficiency in **triaging observations** and mobilizing **Incident Response Team**

Case Study

State uses *Desk Reference* to support decision-making and action

Situation: Jurisdiction website with voting information (dates, locations, times) is showing erroneous information

Symptom Assessment: Erroneous information may be the result of a browser issue or may be indicative of a larger issue

Locate: Election Official leverages the *Desk Reference* and locates “Official Jurisdiction Website or Social Media Account Showing Erroneous Information” Symptom

CISA
CYBER+INFRASTRUCTURE

Case Study

State uses *Desk Reference* to support decision-making and action

Execute: Election Official executes decision tree to support decision-making and appropriate notifications

Case Study

State uses *Desk Reference* to support decision-making and action

Notify: Election Official contacts the designated Incident Response Team to mitigate incident impacts

Phase	Action
Internal Notification	1a. Document issue in Incident Tracker 1b. Observer Contacts Election Division IT support: ***[Input name and contact info]*** 1c. Observer notifies immediate supervisor(s) and supervisory election official of the potential breach: ***[Input name and contact info]*** 1d. **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]*** 1e. **Election official** notifies internal division systems leads to provide mitigation instructions from IT, as applicable ***[Input system, POC name, and contact info]*** ***[Input system, POC name, and contact info]*** ***[Input system, POC name, and contact info]***
Incident Escalation	2a. **Election official** notifies county election executive of suspicious observation; describe potential impacts to business systems and jurisdictional processes. ***[Input name and contact info]*** 2b. **IT Support Lead** determines necessary to contact County and State IT for additional support in diagnosing impacts and determining a resolution. ***County IT [Input name and contact info]*** ***State IT [Input name and contact info]*** 2C. If **IT Support Lead** confirms suspicious observation as critical, **election official notifies** appropriate state and federal POCs ***State Election Authority [Input name and contact info]*** ***CISA POC [Input name and contact info]*** ***EI-ISAC POC [Input name and contact info]***

CISA
CYBER+INFRASTRUCTURE

CISA
CYBER+INFRASTRUCTURE

Matt Masterson
Senior Cybersecurity Advisor
U.S. Department of Homeland Security

CISA

CYBER+INFRASTRUCTURE