Texas Secretary of State

Elections Incident Response Plan

ELECTION SECURITY

Texas Secretary of State

ELECTION INCIDENT RESPONSE PLAN

ELECTION SECURITY BEST PRACTICES GUIDE & DATA CLASSIFICATION SYSTEM

Election Information Security Policy Template	Election Security Incident Response Plan Template	Continuity of Operations Plan Template	Vendor Risk Management Policy Template	

Agenda

- Elections Incident Response Plan Overview
  - Team members
  - Components
  - Process
- Navigation based on the 5 stages of the National Institute of Standards and Technology Framework
  1. Identify 2. Detect 3. Protect 4. Respond 5. Recover
- Must be tailored to the needs of **Your Organization**

EIRP vs COOP

Election Incident Response Plan

- Immediate action and resolution

Continuity of Operations Plan

- Continuing Essential functioning

EIRP Overview: What is it and Why do I need one?

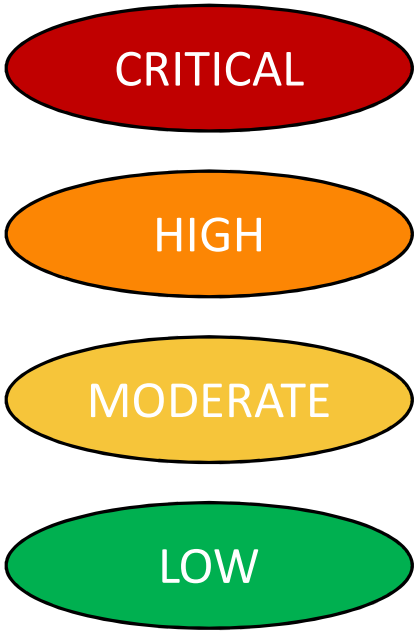
- A detailed step-by-step plan to help you prepare and handle an unexpected incident
  - Stakeholders involved
  - Resources needed
  - Process to follow
  - When to reach out, who to reach out to
- What to do once you ***confirm*** there has been an incident
  - How to handle it, who to inform, how to inform, how to recover
- What to do ***after*** the incident has been handled
  - How to protect against it happening again

Incident Response Team

Incident Handlers

INCIDENT RESPONSE COMMANDER	IT SUPPORT	DIRECTOR OF COMMUNICATIONS	ADDITIONAL SUPPORT
designee) oversees response and leads plan execution	response actions • Execute plan		• Legal Counsel • Human Resources • County/Local Emergency Mgmt. Systems

Severity of an Incident



- Classify incidents according to number of:
  - Voters affected
  - Departments and/or users affected
  - Key personnel impacted

Communications Plan: Internal

- Securely share information about the incident with employees and other internal stakeholders.

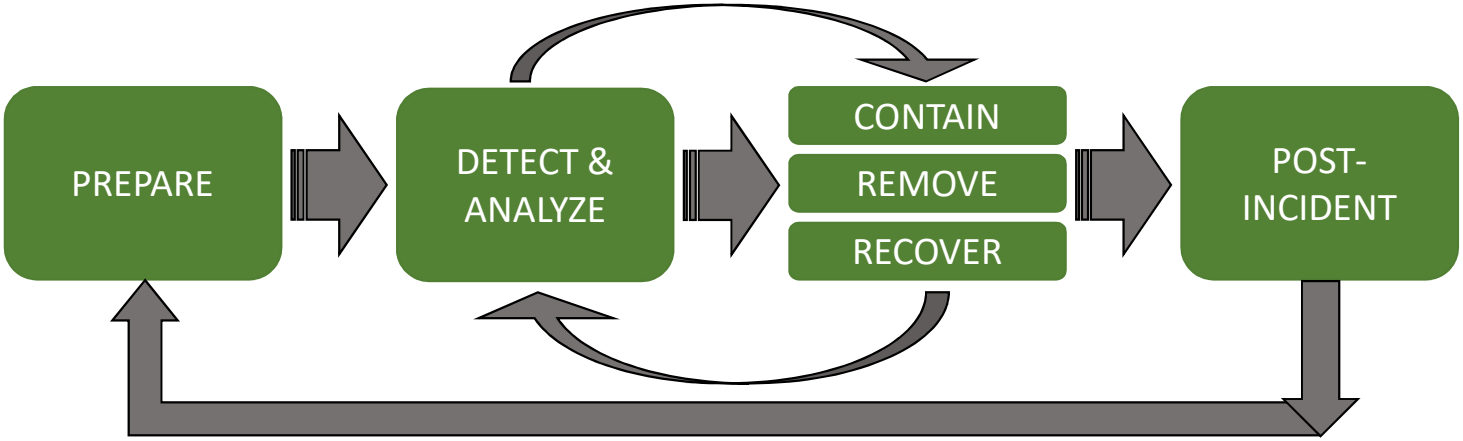
- What happened?
- When did it happen?
- What was compromised?
- What steps should be taken?

Communications Plan: External

- Critical stakeholders
  - Secretary of State (SOS)
  - Department of Information Resources (DIR)
  - Elections Infrastructure-Information

APPENDIX B: INCIDENT NOTIFICATION PRIORITY CONTACT LIST					
Organization	Name	Title	Phone	Email	When to Contact and Why
Office of the Texas Secretary of State (SOS)	Keith Ingram	Director of Elections	512-463-5650	elections@sos.texas.gov	IMMEDIATELY after a valid incident is confirmed in order to engage in coordinated response
Texas Department of Information Resources (DIR)			512-475-4700	Security-alerts@dir.texas.gov	After valid incident is confirmed for assistance with technical aspects of response
Cybersecurity Service Provider					
Law Enforcement					
Legal Counsel					
Government Officials					
EI ISAC/MS ISAC			1-866-787-4722	soc@cisecurity.org	After incident facts have been collected to share information that helps other agencies guard against similar attacks.

Incident Response Cycle



- Not a linear process
  - Move back and forth between **Detect & Analyze** phase and **Contain, Remove and Recover** phases
  - After **Post-Incident** phase, incorporate lessons learned and adjust **Prepare** phase

EIRP Phases: Preparing your Plan

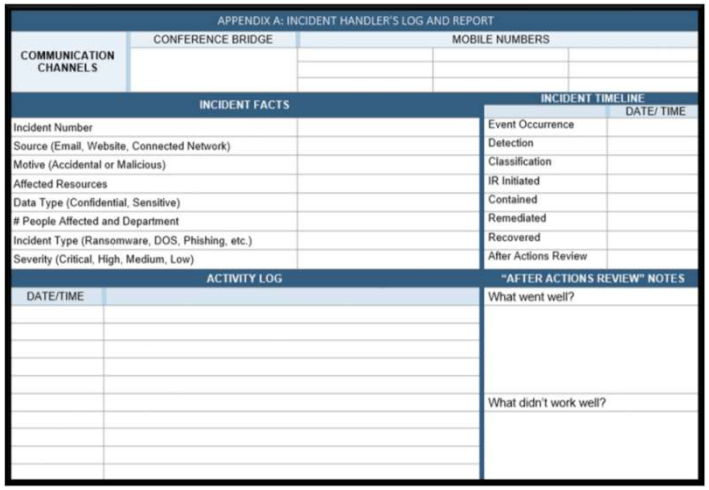
- Events move quickly during an incident
- Gather the resources beforehand

TABLE 2: ELECTION DATA CLASSIFICATION SYSTEM	
DATA CLASSIFICATION LEVEL	DATA TYPE
Confidential	

Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.	• Written Information Security Program
	• Election Information Security Policy
	• Election System Security Plan
	• Cybersecurity Incident Response Plan
	• Continuity of Operations Plan
	• Vendor Risk Management Policy
	• Vendor Risk Assessment Results
	• Election Security Assessment (ESA) Results
	• Employee and Poll Worker Personally Identifiable Information and Financial Data
	• Election Department Critical Infrastructure Information
	• Polling Location Technology Configuration
	• Passwords, Including Login Credentials for All Systems and Election Devices
	• Vulnerability Scan Data
	• Threat Monitoring and Cyber Intelligence Information
	• System Inventory Information
	• System Life Cycle Management Information
	• Security Incident Reports or Event Details
	• Protected Voter Registration Application Information including items Defined in Election Code 13.004 (c) including:
	  ○ Social security number
	  ○ Texas Driver License or TX Personal

EIRP Phases: Detect and Analyze

- Confirm that there has been an incident
- Set up logistics for your incident response team
- Analyze the incident
- Document your actions
- Proceed with internal communications plan
- Alert external stakeholders



APPENDIX A: INCIDENT HANDLER'S LOG AND REPORT

COMMUNICATION CHANNELS	CONFERENCE BRIDGE	MOBILE NUMBERS

INCIDENT FACTS	
Incident Number	
Source (Email, Website, Connected Network)	
Motive (Accidental or Malicious)	
Affected Resources	
Data Type (Confidential, Sensitive)	
# People Affected and Department	
Incident Type (Ransomware, DOS, Phishing, etc.)	
Severity (Critical, High, Medium, Low)	

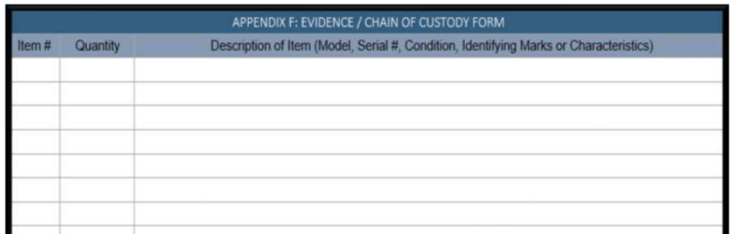
INCIDENT TIMELINE	DATE/ TIME
Event Occurrence	
Detection	
Classification	
IR Initiated	
Contained	
Remediated	
Recovered	
After Actions Review	

ACTIVITY LOG	
DATE/TIME	

"AFTER ACTIONS REVIEW" NOTES
What went well?
What didn't work well?

EIRP Phases: Contain

- Stop the attack from spreading and protect the rest of your network



APPENDIX F: EVIDENCE / CHAIN OF CUSTODY FORM

Item #	Quantity	Description of Item (Model, Serial #, Condition, Identifying Marks or Characteristics)

EIRP Phases: Remove

- Remove the threat
  - Remove malware
  - Change account passwords
- Document your actions
- Improve your defenses

Continue monitoring for malicious activity and return to the **Detect & Analyze** phase if you are still having issues

EIRP Phases: Recover

- Once threat is contained, work on more permanent fixes
  - Restore and rebuild systems
  - Recover your data
  - Replace infected files
  - Re-enable account
  - Install patches
- Confirm systems are working normally

Continue monitoring for malicious activity and return to the **Detect & Analyze** phase if you are still having issues

EIRP Phases: Post-Incident

- Use your Handler's Log to identify lessons learned and update your plan if necessary
- Coordinate Handler's Logs to

- What worked?
- What didn't
- What should have been done sooner?
- What would stop this from happening again?

Customizing the Plan: Adaptation

- Read through the entire plan template
- Establish roles and responsibilities with your county

Customizing the Plan: Updating

- Review your plan and establish a schedule for updates
- Keep a record of all reviews and changes

PLAN REVIEW LOG

ORIGINAL EFFECTIVE DATE <Date>					
Drafted By	<Name, Title>	Signature	<Signature>	<Date>	
Approved By	<Name, Title>	Signature	<Signature>	<Date>	

REVIEW AND REVISION LOG

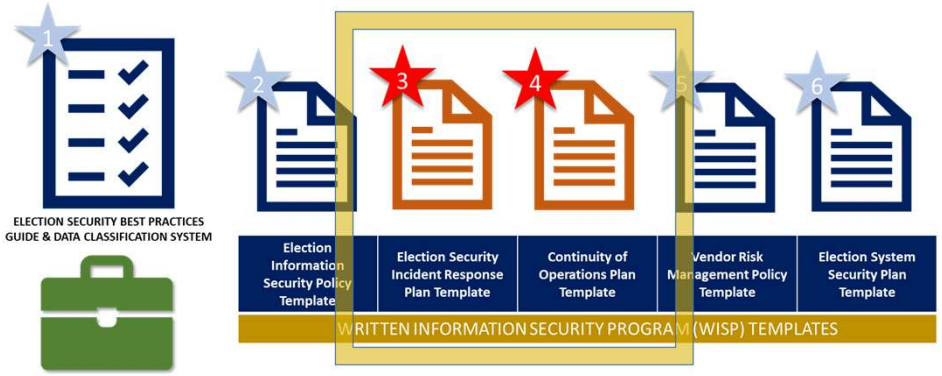
REVIEW SCHEDULE		General Election Years: December after elections		Legislative Session Years: July after SOS Law Conference		After an incident or practice drill
Review Date	Revision Date	Revision Description	Drafted By: Name, Title	Signature, Date	Approved By: Name, Title	Signature, Date

Customizing the Plan: Implementing

Once you have made the plan your own:

- Work with your organization to implement it
- Train your staff
- Continue working on the other documents in the Election Security Toolkit

Upcoming Webinars: WISP Mini-Series



- Elections Incident Response Plan Workshop – **February 23rd** 2:00pm
- Continuity of Operations Plan Webinar – **March 8th** 2:00pm
- Continuity of Operations Plan Workshop – **March 9th** 2:00pm
- Election Official as an IT Manager – **March 23rd** 2:00pm

Texas Secretary of State

ELECTION INCIDENT RESPONSE PLAN

AVAILABLE SUPPORT

WEBINARS

TRAINING

RESOURCES

ELECTION SECURITY TRAINERS
ElectionSecurity@sos.texas.gov

Q&A