U. S. ELECTION ASSISTANCE COMMISSION
Voting System Testing and Certification Program
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Cyber Incident Response Best Practices

In its continued effort to provide resources for managing election technology, the U.S. Election Assistance Commission (EAC) has collaborated with election officials and other partners to provide best practices on topics of interest to the election community.

Since the 2016 Federal Election, there has been widespread concern in the election community about what to do if a cyber incident were to occur. With election officials increasingly becoming de-facto IT Managers, they are often placed in charge of securing a variety of election technologies. Election officials from across the country have reached out to the EAC requesting resources and best practice for creating and implementing Cyber Incident Response Plans. This document provides an overview of items that election officials should take into consideration when developing these policies and plans. Additionally, it provides usable checklists and other resources designed to help develop more in-depth procedures for implementing cyber incident response policies and procedures.

The information contained in this document is derived from documents developed, vetted, and published by the EAC's federal partners, including the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS). Further, each bullet is titled after a recommendation provided in NIST Special Publication (SP) 800-61 Revision 2: *Computer Security Incident Handling Guide*.

- **Creating an incident response policy and plan –** Election officials should be prepared to respond quickly and effectively to a cyber incident. The first step of developing a policy or plan is to identify which events are considered incidents and provide an organizational structure, including roles and responsibilities, for responding to these events. This may also include incidents that occur on systems the organizations uses but are outside of their physical control, such as service-oriented systems provided by vendors.

- **Developing procedures for performing incident handling and reporting –** The incident handling and reporting procedures provide a detailed process for carrying out the incident response policy and plan. It should cover all phases detailed in the *Incident Handling Checklist* (attached) from the NIST SP 800-61.

- **Setting guidelines for communicating with outside parties regarding incidents –** Election officials should create a communications plan that describes which incidents need to be reported to which outside parties such as the media, law enforcement agencies, and incident reporting organizations. The guidelines should also address the timeframe for this reporter, as well as identify the members of the incident response team that are integral in implementing the plan, such as public affairs office, legal department, and management.

- **Selecting a team structure and staffing model –** There are many resources for developing a team structure and staffing model, but the first consideration an organization should make is whether it will create an internal incident response team or outsource it. Many factors will play into that decision, but organizations should take into account that an incident can occur at any time, response can require specific expertise across a multitude of technical and non-technical sectors of the organization, and these incidents can often be both stressful and costly.

- **Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies) –** Every incident will require collaboration and cooperation of multiple team members and groups. The relationships and credibility of each team member and group is vital to a successful recovery from an incident.

- **Determining what services the incident response team should provide** – Having well defined roles for which members and teams will provide what services will facilitate a smoother implementation.

- **Staffing and training the incident response team –** Training staff and the incident response team ensures that the incident response procedures are accurately carried out. Additionally, the training should provide specific details on the transition from incident response to recovery.

Conclusion:

The number of attempts to infiltrate computer systems rises every day. Election officials work hard to mitigate risk and no organization wants a cyber incident to occur, but should an occurrence happen the greatest risk is to not have policies and plans to respond to the incident. All organizations are different and need to develop policies and plans that align with their unique needs. Election officials should remember that cyber incidents are not the only type of incidents they may face, so cyber incident response plans should be integrated into an overall incident response plan that includes physical incidents. It should also correlate with the organization's continuity of operations and recovery plans.

Resources:

For additional technical resources, reference the following documents that were utilized to develop this document.

- National Cyber Incident Response Plan
- NIST, SP 800-61 Revision 2, Computer Security Incident Handling Guide
- NIST, SP 800-86, Guide to Applying Forensic Techniques to Incident Response
- NIST, SP 800-94 Revision 1 (DRAFT), Guide to Intrusion Detection and Prevention Systems (IDPS)
- NIST, SP 800-184, Guide for Cybersecurity Event Recovery

Incident Handling Checklist

Step	Action	Completed
	Detection and Analysis	
1	**Determine whether an incident has occurred**	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2	**Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)**	
3	**Report the incident to the appropriate internal personnel and external organizations**	
	Containment, Eradication, and Recovery	
4	**Acquire, preserve, secure, and document evidence**	
5	**Contain the incident**	
6	**Eradicate the incident**	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7	**Recover from the incident**	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8	**Create a follow-up report**	
9	**Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)**	