CISA INCIDENT RESPONSE SUPPORT FOR ELECTION PARTNERS

SEPTEMBER 2020

CISA INCIDENT RESPONSE SUPPORT FOR ELECTION PARTNERS

This document provides an overview of how Cybersecurity and Infrastructure Security Agency (CISA) election partners can request CISA cyber incident response services. It also outlines the steps partners should take to help CISA determine the type of support to provide. This product also provides best practices on planning for—and handling—cybersecurity incidents.

REQUEST HELP

WE WANT TO HELP—IT'S OUR MISSION! IF YOU EXPERIENCE, OR SUSPECT, MALICIOUS CYBER BEHAVIOR, PLEASE CONTACT US:

1-888-282-0870

CENTRAL@CISA.DHS.GOV

CISA SERVICES

CISA provides incident response services to election partners. Services provided depend upon the specifics of each incident. These services include—but are not limited to—the following:

INCIDENT-SPECIFIC TRIAGE

In order to best understand the severity of the incident, first we scope the incident and determine what resources are required.

HUNT ANALYSIS

Analysis of network and host artifacts—such as logs and digital media—to identify evidence of compromise, potential for persistent adversarial access, and indicators of compromise. We have the ability to scale levels of analysis depending on the incident.

MALWARE ANALYSIS

Reverse engineering of malware artifacts to determine functionality and build indicators to prevent future attacks.

WHAT WE NEED

Determining Severity and Services. We will work with you to understand the severity of the incident and determine the type of support needed using the CISA Cyber Incident Scoring System: https://www.us-cert.gov/CISA-Cyber-Incident-Scoring-System. To maximize the accuracy of this process, please gather and provide—to the extent possible—the following information before we discuss the incident:

- **FUNCTIONAL IMPACT**
  Describe the actual, ongoing impact to your organization. In many cases, such as scans, probes, or a successfully defended attack, little or no impact may be experienced.

- **OBSERVED ACTIVITY**
  Describe what is known about threat actor activity on your network. Sort the observed activity into four categories:

  » **Prepare.** Actions taken to establish objectives, intent, and strategy; identify potential targets and attack vectors; identify resource requirements; and develop capabilities.

  » **Engage.** Actions taken against a specific target or target set prior to gaining—but with the intent to gain—access to the victim's physical or virtual computer or information systems, networks, and data stores.

  » **Presence.** Actions taken by the threat actor after gaining access to the target physical or virtual computer or information systems. These actions establish and maintain conditions for the threat actor to perform intended actions or operate at will against the host's physical or virtual computer or information systems, networks, or data stores.

  » **Effects.** Outcomes of the threat actor's actions on a victim's physical or virtual computer or information systems, networks, and data stores.

- **LOCATION OF OBSERVED ACTIVITY**
  Describe where in the network the observed activity was detected. For example, was the activity spotted in the business demilitarized zone (DMZ), business network, business network management, critical systems DMZ, critical systems management, critical systems, or safety systems—or is it unknown where the activity was observed but the network segment could be identified?

- **INFORMATION IMPACT**
  Describe the type of information and how it was lost, compromised, or corrupted—e.g., the confidentiality and integrity of the information stored or processed by various systems.

- **RECOVERABILITY**
  Identify the scope of resources needed to recover from the incident.

- **POTENTIAL IMPACT**
  Estimate the overall national impact resulting from a total loss of service from the affected entity. Due to the inherent difficulties in accounting for all the various circumstances involved in determining the true potential impact, this should be treated as a "best guess" estimate for incident response prioritization purposes rather than a comprehensive illustration of an entity's importance to the national welfare.

- **ADDITIONAL DETAILS**
  Keep records on as many details about the incident as possible and your current situation at the time you make the report. Also include additional details such as what, if any, cloud services and cloud service providers you are currently using.

INCIDENT CHECKLIST

We also suggest running through the below checklist to ensure you have gathered—and are ready to provide— specific information (as available) before we discuss the incident:

	Yes	No
Are you reporting an active incident?		
Was law enforcement contacted?		
▸ If yes, please be ready to provide a point of contact information.		
Do you have a third-party vendor working with you on this incident?		
▸ If yes, please be ready to provide a point of contact information.		
Do you know the initial attack vector?		
▸ If yes, please be ready to provide a description.		
Do you know where on your network potentially malicious activity was observed?		
▸ If yes, please be ready to provide a description.		
Do you believe any of the following items was affected? **- infrastructure to cast or tally votes** **- voter registration systems** **- pollbooks**		
▸ If yes, please be ready to provide a description.		
Do you have indicators of compromise from this incident?		
▸ If yes, please be ready to provide these. (Examples include attacker IP addresses, suspected malware, etc.).		

	Yes	No
Do you have current and historical log data?		
▸ If yes, please preserve the log data for further analysis. This includes all host and network logs.		
Were potentially compromised systems powered down?		
▸ If no, please leave them online and powered on until we can discuss further with you.		
Can you take a live forensic memory capture and disk image of the compromised system(s)?		
▸ If yes, please do so and preserve them.		
Do you have a recovery timeframe objective?		
▸ If yes, please be ready to provide this information.		
Do you have a count of how many endpoints are on your network?		
▸ If yes, please be ready to provide this information.		
Do you believe your incident is ransomware?		
▸ If yes, please refer to https://www.cisa.gov/ransomware for further information.		
Are you using cloud services or infrastructure?		
▸ If yes, please be ready to identify what services or infrastructure you are using and the name of the service and/or infrastructure provider.		

INCIDENT RESPONSE PLANNING

No one can predict when an incident will occur or how severe it will be; however, there are best practices we can all follow to better handle cybersecurity incidents. One of these practices is developing and maintaining an incident response plan. For guidance in developing an incident response plan, CISA recommends using the CISA Cyber Incident Detection and Notification Planning Guide for Election Security (https://www.cisa.gov/publication/protect2020-cyber-incident-guide). The guide addresses the election community's need to effectively recognize and respond to potential cyber incidents and 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

You should also consider the following points when developing or reviewing incident response plans:

PLAN CAREFULLY

Consider what network locations are most at risk and could, if affected, most impact operations. Also ensure network documentation, such as topology diagrams, are up to date and as accurate as possible. This includes receiving and maintaining network documentation and updates from third-party providers who may be managing your network. Addressing these ahead of time will help prioritize resources during an incident.

DEVELOP PROCESSES AND PROCEDURES

Establishing processes and procedures for implementing the incident response plan will help ensure the response is accurate and thorough. These include documents such as technical processes, checklists, and forms used by incident responders.

PUBLIC AFFAIRS IS IMPORTANT

Engaging the press and public while also addressing an incident is difficult. Create an external affairs plan beforehand to ensure you are prepared to communicate clearly.

EXERCISE, EXERCISE, EXERCISE

It is vital to ensure your incident responders know how to use all the tools at their disposal before an incident occurs. You can do this by conducting tabletop exercises and simulating scenarios, such as taking forensic images and collecting and preserving forensic data. For detailed guidance, see CISA's Elections Cyber Tabletop in a Box (https://www.cisa.gov/publication/elections-cyber-tabletop-box).

INCIDENT HANDLING— COMMON MISTAKES.

WE ALL MAKE MISTAKES.

BUT BEING AWARE OF COMMON ONES BEFORE AN INCIDENT OCCURS HELPS US AVOID THEM.

ATTEMPTING TO MITIGATE impacts to the affected systems before incident responders can protect and recover data

- Doing so can cause the loss of volatile data, such as memory and other host-based artifacts
- The adversary may notice and change their tactics, techniques, and procedures

TOUCHING ADVERSARY INFRASTRUCTURE (Pinging, NSlookup, Browsing, etc.)

- These actions can tip off the adversary that they have been detected

PREEMPTIVELY BLOCKING adversary infrastructure

- Network infrastructure is fairly inexpensive. An adversary can easily change to new command and control infrastructure, and you will lose visibility of their activity

PREEMPTIVELY RESETTING PASSWORD

- An adversary likely has multiple credentials, or worse, access to your entire Active Directory
- An adversary will use other credentials, create new credentials, or forge tickets

FAILING TO PRESERVE OR COLLECT LOG DATA that could be critical to identifying access to the compromised systems

- Instead, be prepared by learning now what log types would be critical to an investigation in your organization and start collecting and retaining these logs for as long as possible

CISA INCIDENT RESPONSE SUPPORT FOR ELECTION PARTNERS