Cybersecurity Incident & Vulnerability Response Playbooks
Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems

Executive Order on Improving the Nation's Cybersecurity

Issued May 12, 2021 by President Biden

One Key Areas Covered by this Executive Order: Enhancing Software Supply Chain Security

- NIST shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance shall include standards, procedures, or criteria regarding:

  (viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

- To respond to this requirement CISA (Cybersecurity & Infrastructure Security Agency) created the Cybersecurity Incident & Vulnerability Response Playbooks
  - Issued November 2021

Cybersecurity Incident & Vulnerability Response Playbooks Scope

- Provides Federal Civilian Executive Branch (FCEB) agencies with a standard set of procedures to identify, coordinate, remediate, recover, and track successful mitigations from incidents and vulnerabilities affecting FCEB systems, data, and networks
- Response activities in scope of this playbook include those:
  - Initiated by an FCEB agency (e.g., a local detection of malicious activity or discovery of a vulnerability)
  - Initiated by CISA (e.g., a CISA alert or directive) or other third parties, including law enforcement, intelligence agencies, or commercial organizations, contractors, and service providers
- Incident Response Playbook applies to incidents that involve confirmed malicious cyber activity and for which a major incident has been declared or not yet been reasonably ruled out
- Vulnerability Response Playbook applies to vulnerabilities being actively exploited in the wild

Cybersecurity Incident & Vulnerability Response Playbooks Scope

Key Terms

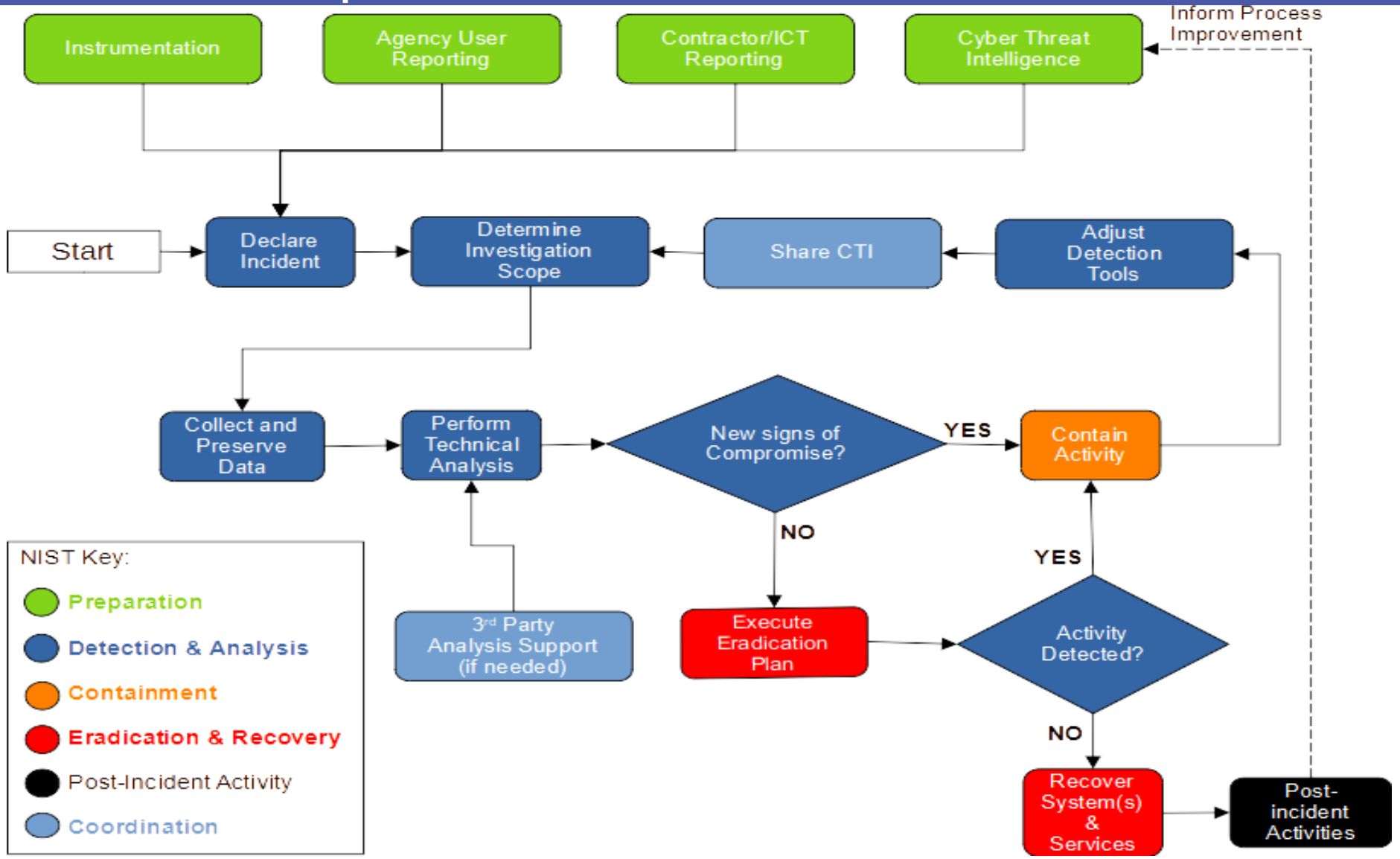
- **FCEB Agencies**: Federal Civilian Executive Branch Agencies (FCEB Agencies) include all agencies except for the Department of Defense and agencies in the Intelligence Community
- **Incident**: An occurrence that— (A)actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B)constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies
- **Major Incident**: Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.Agencies should determine the level of impact of the incident by using the existing incident management process established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide, **or** A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people
- **Vulnerability**: The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control

Incident Response Playbook

Incident Response Playbook

- Provides a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2, Computer Incident Handling Guide
- Describes the process FCEB agencies should follow for confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out

Incident Response Process



Incident Response Process Phases

Preparation Phase

- Define baseline systems and networks before an incident occurs to understand the basics of “normal” activity. Establishing baselines enables deviations.
- Preparation also involves:
  - Having infrastructure in place to handle complex incidents, including classified and out-of-band communications
  - Developing and testing courses of action (COAs) for containment and eradication
  - Establishing means for collecting digital forensics and other data or evidence

Incident Response Process Phases

Preparation Phase Activities

- Develop and implement Incident Response Policies and Procedures
- Develop and maintain an accurate picture of infrastructure (systems, networks, cloud platforms, and contractor-hosted networks) by widely implementing telemetry to support system and sensor-based detection and monitoring capabilities
- Train personnel to respond to cybersecurity incidents
- Actively monitor cyber intelligence feeds for threat or vulnerability advisories from government, trusted partners, open sources, and commercial entities
- Establish active defense capabilities—such as the ability to redirect an adversary to a sandbox or honeynet system for additional study
- Establish local and cross-agency communication procedures and mechanisms for coordinating major incidents with CISA and other sharing partners
- Take steps to ensure that IR and defensive systems and processes will be operational during an attack
- Implement capabilities to contain, replicate, analyze, reconstitute, and document compromised hosts; implement the capability to collect digital forensics and other data
- Leverage threat intelligence to create rules and signatures to identify the activity associated with the incident and to scope its reach

Incident Response Process Phases

Detection & Analysis Phase

- Accurately detect and assess cybersecurity incidents
- Determine whether an incident has occurred and, if so, the type, extent, and magnitude of the compromise within cloud, operational technology (OT), hybrid, host, and network systems
- Implement defined processes, appropriate technology, and sufficient baseline information to monitor, detect, and alert on anomalous and suspicious activity.
- Ensure there are procedures to deconflict potential incidents with authorized activity (e.g., confirm that a suspected incident is not simply a network administrator using remote admin tools to perform software updates)

Incident Response Process Phases

Detection & Analysis Phase Activities

- Declare an incident by reporting it to CISA at https://www.us-cert.cisa.gov/ and alerting agency IT leadership to the need for investigation and response
- Identify the type of access, the extent to which assets have been affected, the level of privilege attained by the adversary, and the operational or informational impact
- Collect and preserve data for incident verification, categorization, prioritization, mitigation, reporting, and attribution
- Develop a technical and contextual understanding of the incident
- Acquire, store, and analyze logs to correlate adversarial activity
- Assess and profile affected systems and networks for subtle activity that might be adversary behavior
- Identify the root cause of the incident and collect threat information that can be used in further searches and to inform subsequent response efforts

Incident Response Process Phases

Detection & Analysis Phase Activities

- Identify the conditions that enabled the adversary to access and operate within the environment
- Compare TTPs to adversary tactics, techniques & procedures (TTPs) documented in the MITRE ATT&CK® framework and analyze how the TTPs fit into the attack lifecycle (TTPs describe "why," "what," and "how.")
- Identify any additional potentially impacted systems, devices, and associated accounts
- Obtain Third-Party support if needed
- Use its developing understanding of the adversary's TTPs to modify tools to slow the pace of the adversarial advance and increase the likelihood of detection

.

Incident Response Process Phases

Containment Phase

- Prevent further damage and reduce the immediate impact of the incident by removing the adversary's access
- Need to consider:
  - Any additional adverse impacts to mission operations, availability of services (e.g., network connectivity, services provided to external parties)
  - Duration of the containment process
  - Resources needed, and effectiveness (e.g., full vs. partial containment; full vs. unknown level of containment)
  - Any impact on the collection, preservation, securing, and documentation of evidence

Incident Response Process Phases

Containment Phase Activities

- Isolating impacted systems and network segments from each other and/or from non-impacted systems and networks
- Capturing forensic images to preserve evidence for legal use (if applicable) and further investigation of the incident
- Updating firewall filtering
- Blocking (and logging) of unauthorized accesses; blocking malware sources
- Closing specific ports and mail servers or other relevant servers and services.
- Changing system admin passwords, rotating private keys, and service/application account secrets where compromise is suspected and revocation of privileged access
- Directing the adversary to a sandbox (a form of containment) to monitor the actor's activity, gather additional evidence, and identify attack vectors
- Ensure that the containment scope encompasses all related incidents and activity — especially all adversary activity

Incident Response Process Phases

Eradication & Recovery Phase

- Allow the return of normal operations by eliminating artifacts of the incident (e.g., remove malicious code, re-image infected systems) and mitigating the vulnerabilities or other conditions that were exploited
- Ensure that all means of persistent access into the network have been accounted for, that the adversary activity is sufficiently contained, and that all evidence has been collected

Incident Response Process Phases

Eradication and Recovery Phase Activities

- Execute Eradication Plan - Take actions to eliminate all evidence of compromise and prevent the threat actor from maintaining a presence in the environment; Ensure evidence has been preserved as necessary
- Continue with detection and analysis activities to monitor for any signs of adversary re-entry or use of new access methods
- Restore systems to normal operations and confirm that they are functioning normally
- Ensure that have enhanced vigilance and controls in place to validate that the recovery plan has been successfully executed and that no signs of adversary activity exist in the environment

Incident Response Process Phases

Post-Incident Phase

- Document the incident, inform agency leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents
- Activities
  - Add enterprise-wide detections to mitigate against adversary TTPs that were successfully executed during the incident
  - Identify and address “blind spots” to ensure adequate coverage moving forward
  - Closely monitor the environment for evidence of persistent adversary presence
  - Provide post-incident updates as required by law and policy
  - Conduct a lessons-learned analysis to review the effectiveness and efficiency of incident handling

Incident Response Process Phases

Coordination Phase

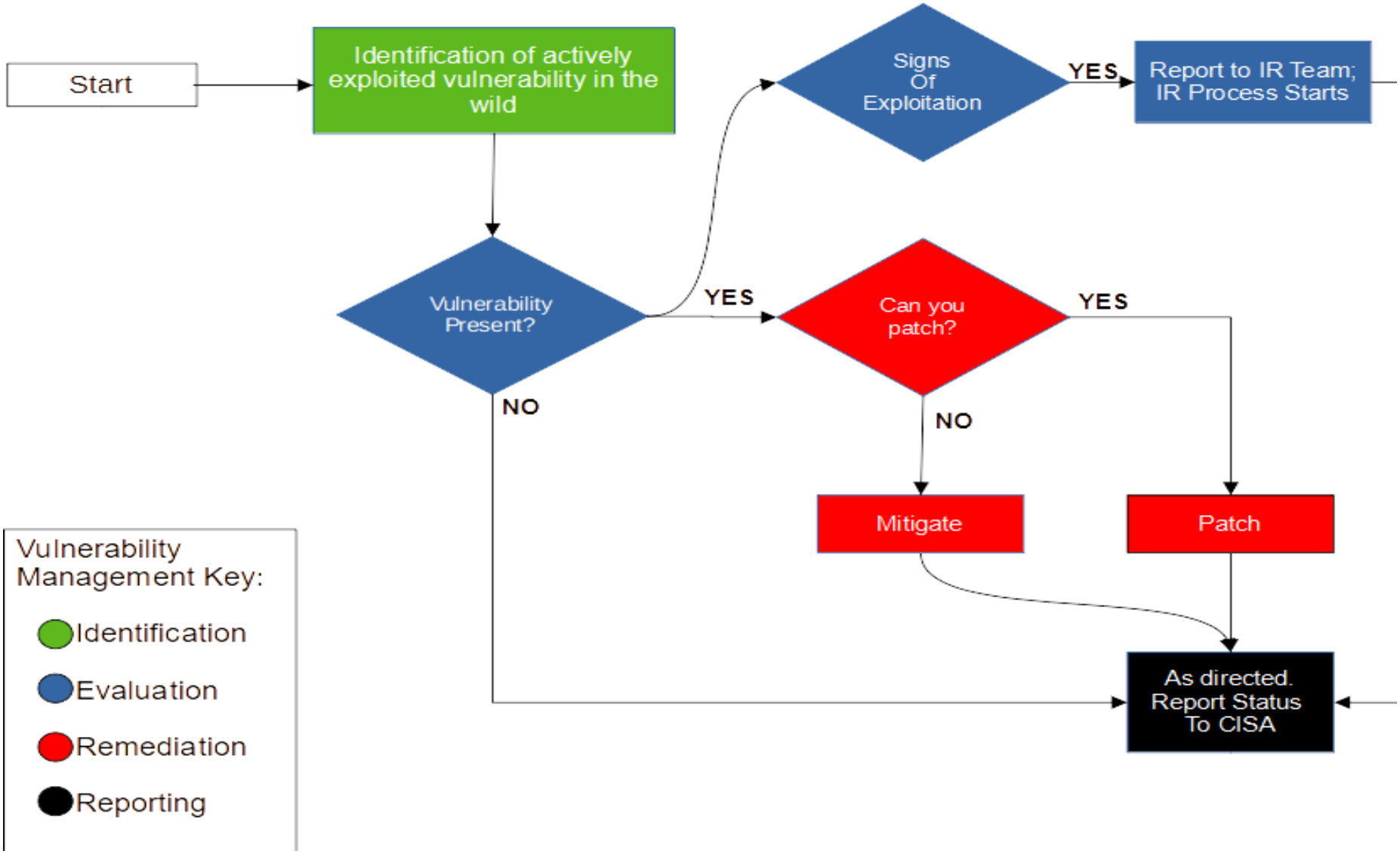
- Ensure that FCEB agency experiencing the incident and CISA coordinate early and often throughout the response process
- Activities
  - Coordinate with CISA throughout the various Incident Response phases
  - Perform intergovernmental coordination based on the roles and responsibilities of the Federal agencies that need to be involved

Vulnerability Response Playbook

Vulnerability Response Playbook

- Standardizes the high-level process that agencies should follow when responding to urgent and high-priority vulnerabilities
  - Ensure that agencies, including CISA, can understand the impact of these critical and dangerous vulnerabilities across the federal government
- Ensure that effective vulnerability management practices are being followed
- Have a process in place to understand the relevance of vulnerabilities to the environment by tracking operating systems and other applications for all systems

Vulnerability Response Process



Vulnerability Response Process Phases

Identification Phase

- Proactively identify reports of vulnerabilities that are actively exploited in the wild by monitoring threat feeds and information sources, including but not limited to:
  - CISA/US-CERT National Cyber Awareness System (NCAS) products, which include the weekly bulletins containing vulnerability summaries
  - CISA Binding Operational Directive (BOD) 22-01, Managing Unacceptable Risk of Known Vulnerabilities, which is continually updated with vulnerabilities being exploited in the wild
  - External threat or vulnerability feeds, such as NIST's National Vulnerability Database
  - FCEB agencies
- Capture additional information about the vulnerability to help with the rest of the response process, including the severity of the vulnerability, susceptible software versions, and indicators of compromise (IOCs) or other investigation steps that can be used to determine if it was exploited

Vulnerability Response Process Phases

Evaluation Phase

- Determine whether the vulnerability exists in the environment and how critical the underlying software or hardware is
- If the vulnerability exists in the environment, address the vulnerability itself and determine whether it has been exploited in the agency's environment
- If the vulnerability was exploited in the environment, immediately begin incident response activities as described in the Incident Response Playbook
- At the end of the Evaluation phase, the goal is to understand the status of each system in the environment as:
  - **Not Affected.** The system is not vulnerable.
  - **Susceptible.** The system is vulnerable, but no signs of exploitation were found, and remediation has begun
  - **Compromised.** The system was vulnerable, signs of exploitation were found, and incident response and vulnerability remediation has begun

Vulnerability Response Process Phases

Remediation Phase

- Remediate all actively exploited vulnerabilities that exist on or within the environment in a timely manner
- In most cases, remediation should consist of patching. In other cases, the following mitigations may be appropriate:
  - Limiting access
  - Isolating vulnerable systems, applications, services, profiles, or other assets
  - Making permanent configuration changes
- In cases where patches do not exist, have not been tested, or cannot be immediately applied promptly, take other courses of action to prevent exploitation, such as:
  - Disabling services
  - Reconfiguring firewalls to block access
  - Increasing monitoring to detect exploitation
- As systems are remediated, keep track of their status for reporting purposes

Vulnerability Response Process Phases

Reporting and Notification Phase

- Share information about how vulnerabilities are being exploited by adversaries to help defenders across the federal government understand which vulnerabilities are most critical to patch.
- Ensure CISA maintains awareness of the status of vulnerability response for actively exploited vulnerabilities
- Report to CISA in accordance with Federal Incident Notification Guidelines, Binding Operational Directives, or as directed by CISA in an Emergency Directive