Cybersecurity Incident & Vulnerability Response Playbooks

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

Publication: November 2021

Cybersecurity and Infrastructure Security Agency

CONTENTS

INTRODUCTION

The Cybersecurity and Infrastructure Security Agency (CISA) is committed to leading the response to cybersecurity incidents and vulnerabilities to safeguard the nation's critical assets. Section 6 of Executive Order 14028 directed DHS, via CISA, to "develop a standard set of operational procedures (playbook) to be used in planning and conducting cybersecurity vulnerability and incident response activity respecting Federal Civilian Executive Branch (FCEB) Information Systems." [1]

Overview

This document presents two playbooks: one for incident response and one for vulnerability response. These playbooks provide 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. In addition, future iterations of these playbooks may be useful for organizations outside of the FCEB to standardize incident response practices. Working together across all federal government organizations has proven to be an effective model for addressing vulnerabilities and incidents. Building on lessons learned from previous incidents and incorporating industry best practices, CISA intends for these playbooks to evolve the federal government's practices for cybersecurity response through standardizing shared practices that bring together the best people and processes to drive coordinated actions.

The standardized processes and procedures described in these playbooks:

- ☐ Facilitate better coordination and effective response among affected organizations,
- ☐ Enable tracking of cross-organizational successful actions,
- ☐ Allow for cataloging of incidents to better manage future events, and
- ☐ Guide analysis and discovery.

Agencies should use these playbooks to help shape overall defensive cyber operations to ensure consistent and effective response and coordinated communication of response activities

Scope

These playbooks are for FCEB entities to focus on criteria for response and thresholds for coordination and reporting. They include communications between FCEB entities and CISA; the connective coordination between incident and vulnerability response activities; and common definitions for key cybersecurity terms and aspects of the response process. 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

The Incident Response Playbook applies to incidents that involve confirmed malicious cyber activity and for which a major incident (as defined by the Office of Management and Budget [OMB] in

---

[1] Executive Order (EO) 14028: Improving the Nation's Cybersecurity

Memorandum M-20-04[2] or successor memorandum) has been declared or not yet been reasonably ruled out. The Vulnerability Response Playbook applies to vulnerabilities being actively exploited in the wild. As required by EO 14028, the Director of OMB will issue guidance on FCEB agency use of these playbooks.

Note: these playbooks do not cover response activities that involve threats to classified information or National Security Systems (NSS) as defined by 44 U.S.C.3552(b)(6). See CNSSI1010[3] for coordination/reporting guidance for incidents specific to NSS or systems that process classified information.

Audience

These playbooks apply to all FCEB agencies, information systems used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency. It is the policy of the federal government that information and communications technology (ICT) service providers who have contracted with FCEB agencies must promptly report incidents to such agencies and to CISA.[4]

---

[2] Office of Management and Budget (OMB) Memorandum M-20-04: Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements

[3] Committee on National Security Systems

[4] EO 14028, Sec. 2. *Removing Barriers to Sharing Threat Information*

INCIDENT RESPONSE PLAYBOOK

This 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,[5] including preparation, detection and analysis, containment, eradication and recovery, and post-incident activities. This playbook 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 can be initiated by several types of events, including but not limited to:
☐ Automated detection systems or sensor alerts
☐ Agency user report
☐ Contractor or third-party ICT service provider report
☐ Internal or external organizational component incident report or situational awareness update
☐ Third-party reporting of network activity to known compromised infrastructure, detection of malicious code, loss of services, etc.
☐ Analytics or hunt teams that identify potentially malicious or otherwise unauthorized activity

When to use this playbook

Use this playbook for incidents that involve confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out.

For example:

☐ Incidents involving lateral movement, credential access, exfiltration of data
☐ Network intrusions involving more than one user or system
☐ Compromised administrator accounts

This playbook does not apply to activity that does not appear to have such major incident potential, such as:

☐ "Spills" of classified information or other incidents that are believed to result from unintentional behavior only
☐ Users clicking on phishing emails when no compromise results
☐ Commodity malware on a single machine or lost hardware that, in either case, is not likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

Incident Response Process

The incident response process starts with the declaration of the incident, as shown in Figure 1. In this context, "declaration" refers to the identification of an incident and communication to CISA and agency network defenders rather than formal declaration of a major incident as defined in applicable law and policy. Succeeding sections, which are organized by phases of the IR lifecycle, describe each step in more detail. Many activities are iterative and may continuously occur and evolve until the incident is closed out. Figure 1 illustrates incident response activities in terms of these phases, and Appendix B provides a companion checklist to track activities to completion.

---

[5] [NIST Special Publication (SP) 800-61 Rev. 2: Computer Security Incident Handling Guide](#)
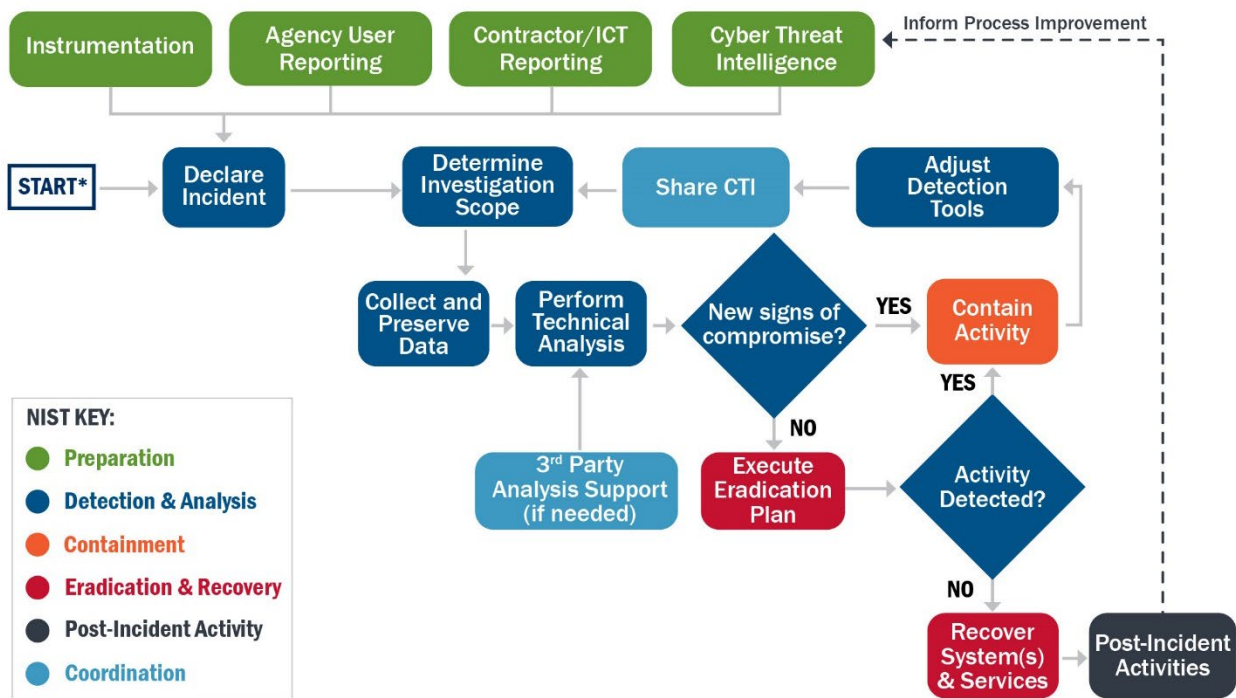
Figure 1: Incident Response Process

Preparation Phase

Prepare for major incidents *before they occur* to mitigate any impact on the organization. Preparation activities include:

- Documenting and understanding policies and procedures for incident response
- Instrumenting the environment to detect suspicious and malicious activity
- Establishing staffing plans
- Educating users on cyber threats and notification procedures
- Leveraging cyber threat intelligence (CTI) to proactively identify potential malicious activity

Define baseline systems and networks before an incident occurs to understand the basics of "normal" activity. Establishing baselines enables defenders to identify deviations. Preparation also includes

- 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

The goal of these items is to ensure resilient architectures and systems to maintain critical operations in a compromised state. Active defense measures that employ methods such as redirection and monitoring of adversary activities may also play a role in developing a robust incident response. [6]

---

[6] For example, "Deception: Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary," as defined in NIST SP 800-160 Vol. 2: Developing Cyber Resilient Systems: A Systems Security Engineering Approach

Preparation Activities

Policies and Procedures

Document incident response plans, including processes and procedures for designating a coordination lead (incident manager). Put policies and procedures in place to escalate and report major incidents and those with impact on the agency's mission. Document contingency plans for additional resourcing and "surge support" with assigned roles and responsibilities. Policies and plans should address notification, interaction, and evidence sharing with law enforcement.

Instrumentation

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 such as antivirus (AV) software; endpoint detection and response (EDR) solutions;[7] data loss prevention (DLP) capabilities; intrusion detection and prevention systems (IDPS); authorization, host, application and cloud logs;[8] network flows, packet capture (PCAP); and security information and event management (SIEM) systems. Monitor for alerts generated by CISA's EINSTEIN intrusion detection system and Continuous Diagnostics and Mitigation (CDM) program to detect changes in cyber posture. Implement additional requirements for logging, log retention, and log management based on Executive Order 14028, Sec. 8. *Improving the Federal Government's Investigative and Remediation Capabilities*,[9] and ensure those logs are collected centrally.

Trained Response Personnel

Ensure personnel are trained, exercised, and ready to respond to cybersecurity incidents. Train all staffing resources that may draw from in-house capabilities, available capabilities at a parent agency/department, third-party organization, or a combination thereof. Conduct regular recovery exercises to test full organizational continuity of operations plan (COOP) and failover/backup/ recovery systems to be sure these work as planned.

Cyber Threat Intelligence

Actively monitor intelligence feeds for threat or vulnerability advisories from government, trusted partners, open sources, and commercial entities. Cyber threat intelligence can include threat landscape reporting, threat actor profiles and intents, organizational targets and campaigns, as well as more specific threat indicators and courses of action. Ingest cyber threat indicators and integrated threat feeds into a SIEM, and use other defensive capabilities to identify and block known malicious behavior. Threat indicators can include:

- Atomic indicators, such as domains and IP addresses, that can detect adversary infrastructure and tools
- Computed indicators, such as Yara rules and regular expressions, that detect known malicious artifacts or signs of activity
- Patterns and behaviors, such as analytics that detect adversary tactics, techniques, and procedures (TTPs)

Atomic indicators can initially be valuable to detect signs of a known campaign. However, because adversaries often change their infrastructure (e.g., watering holes, botnets, C2 servers) between campaigns, the "shelf-life" of atomic indicators to detect new adversary activity is limited. In addition, advanced threat actors

---

[7] EO 14028, Sec. 7. *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks*

[8] NIST SP 800-92: Guide to Computer Security Log Management

[9] E0 14028, Sec. 8. *Improving the Federal Government's Investigative and Remediation Capabilities*

might leverage different infrastructure against different targets or switch to new infrastructure during a campaign when their activities are detected. Finally, adversaries often hide in their targeted environments, using native operating system utilities and other resources to achieve their goals. For these reasons, agencies should use patterns and behaviors, or adversary TTPs, to identify malicious activity when possible. Although more difficult to apply detection methods and verify application, TTPs provide more useful and sustainable context about threat actors, their intentions, and their methods than atomic indicators alone. The MITRE ATT&CK® framework documents and explains adversary TTPs in detail making it a valuable resource for network defenders.[10]

Sharing cyber threat intelligence is a critical element of preparation. FCEB agencies are strongly encouraged to continuously share cyber threat intelligence—including adversary indicators, TTPs, and associated defensive measures (also known as "countermeasures")—with CISA and other partners. The primary method for sharing cyber threat information, indicators, and associated defensive measures with CISA is via the Automated Indicator Sharing (AIS) program.[11] FCEB agencies should be enrolled in AIS. If the agency is not enrolled in AIS, contact CISA for more information.[12] Agencies should use the *Cyber Threat Indicator and Defensive Measures Submission System*—a secure, web-enabled method—to share with CISA cyber threat indicators and defensive measures that are not applicable or appropriate to share via AIS.[13]

Active Defense

FCEB agencies with advanced defensive capabilities and staff might establish active defense capabilities—such as the ability to redirect an adversary to a sandbox or honeynet system for additional study, or "dark nets"—to delay the ability of an adversary to discover the agency's legitimate infrastructure. Network defenders can implement honeytokens (fictitious data objects) and fake accounts to act as canaries for malicious activity. These capabilities enable defenders to study the adversary's behavior and TTPs and thereby build a full picture of adversary capabilities.

Communications and Logistics

Establish local and cross-agency communication procedures and mechanisms for coordinating major incidents with CISA and other sharing partners and determine the information sharing protocols to use (i.e., agreed-upon standards). Define methods for handling classified information and data, if required. Establish communication channels (chat rooms, phone bridges) and method for out-of-band coordination.[14]

Operational Security (OPSEC)

Take steps to ensure that IR and defensive systems and processes will be operational during an attack, particularly in the event of pervasive compromises—such as a ransomware attack or one involving an aggressive attacker that may attempt to undermine defensive measures and distract or mislead defenders. These measures include:

- ☐ Segmenting and managing SOC systems separately from the broader enterprise IT systems,

---

[10] See Best Practices for MITRE ATT&CK® Mapping Framework for guidance on using ATT&CK to analyze and report on cybersecurity threats.

[11] CISA Automated Indicator Sharing

[12] CISA Automated Indicator Sharing

[13] DHS CISA Cyber Threat Indicator and Defensive Measure Submission System

[14] NIST SP 800-47 Rev. 1: Managing the Security of Information Exchanges

- Managing sensors and security devices via out-of-band means,
- Notifying users of compromised systems via phone rather than email,
- Using hardened workstations to conduct monitoring and response activities, and
- Ensuring that defensive systems have robust backup and recovery processes.

Avoid "tipping off" an attacker by having processes and systems to reduce the likelihood of detection of IR activities (e.g., do not submit malware samples to a public analysis service or notify users of potentially comprised machines via email).

Technical Infrastructure

Implement capabilities to contain, replicate, analyze, reconstitute, and document compromised hosts; implement the capability to collect digital forensics and other data. Establish secure storage (i.e., only accessible by incident responders) for incident data and reporting. Provide means for collecting forensic evidence, such as disk and active memory imaging, and means for safely handling malware. Obtain

analysis tools and sandbox software for analyzing malware. Implement a ticketing or case management system that captures pertinent details of:

- Anomalous or suspicious activity, such as affected systems, applications, and users;
- Activity type;
- Specific threat group(s);
- Adversary tactics, techniques, and procedures (TTPs) employed; and
- Impact.

Detect Activity

Leverage threat intelligence to create rules and signatures to identify the activity associated with the incident and to scope its reach. Configure tools and analyze logs and alerts. Look for signs of incident activity and potentially related information to determine the type of incident, e.g., malware attack, system compromise, session hijack, data corruption, data exfiltration, etc.

See Appendix C for a checklist for preparation activities.

Detection & Analysis

The most challenging aspect of the incident response process is often accurately detecting and assessing cybersecurity incidents: determining 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. To detect and analyze events, 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). As the U.S. government's lead for asset response, CISA will partner with affected agencies in all aspects of the detection and analysis process.

Detection & Analysis Activities

Declare Incident

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. CISA can assist in determining the severity of the incident and whether it should be declared a major incident. **Note:** FCEB agencies must promptly report all cybersecurity incidents, regardless of severity, to CISA

Determine Investigation Scope

Use available data to 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. Discover associated malicious activity by following the trail of network data; discover associated host-based artifacts by examining host, firewall, and proxy logs along with other network data, such as router traffic. Initial scoping of an incident to determine adversarial activity may include analyzing results from:

- An automated detection system or sensor;
- A report from a user, contractor, or third-party information and communication technologies (ICT) service provider; or
- An incident report or situational awareness update from other internal or external organizational components.

Collect and Preserve Data

Collect and preserve data for incident verification, categorization, prioritization, mitigation, reporting, and attribution. When necessary and possible, such information should be preserved and safeguarded as best evidence for use in any potential law enforcement investigation. Collect data from the perimeter, the internal network, and the endpoint (server and host). Collect audit, transaction, intrusion, connection, system performance, and user activity logs. When an endpoint requires forensic analysis, capture a memory and disk image for evidence preservation. Collect evidence, including forensic data, according to procedures that meet all applicable policies and standards and account for it in a detailed log that is kept for all evidence. For more information, see NIST Computer Security Incident Handling Guide, SP 800-61 r2.[15] Extract all relevant threat information (atomic, computed, and behavioral indicators and countermeasures) to share with IR teams and with CISA.

Perform Technical Analysis

Develop a technical and contextual understanding of the incident. Correlate information, assess anomalous activity against a known baseline to determine root cause, and document adversary TTPs to enable prioritization of the subsequent

---

[15] NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide

response activities. The goal of this analysis is to examine the breadth of data sources throughout the environment to discover at least some part of an attack chain, if not all of it. As information evolves and the investigation progresses, update the scope to incorporate new information.

Correlate Events and Document Timeline

Acquire, store, and analyze logs to correlate adversarial activity. Table 1 presents an example of logs and event data that are commonly employed to detect and analyze attacker activities.[16,17] A simple knowledge base should be established for reference during response to the incident. Thoroughly document every step taken during this and subsequent phases. Create a timeline of all relevant findings. The timeline will allow the team to account for all adversary activity on the network and will assist in creating the findings report at the conclusion of the response.

Identify Anomalous Activity

Assess and profile affected systems and networks for subtle activity that might be adversary behavior. Adversaries will often use legitimate, native operating system utilities and scripting languages once they gain a foothold in an environment to avoid detection. This process will enable the team to identify deviations from the established baseline activity and can be particularly important in identifying activities such as attempts to leverage legitimate credentials and native capabilities in the environment.

Identify Root Cause and Enabling Conditions

Attempt to identify the root cause of the incident and collect threat information that can be used in further searches and to inform subsequent response efforts. Identify the conditions that enabled the adversary to access and operate

within the environment. These conditions will inform triage and post-incident activity. Assess networks and systems for changes that may have been made to either evade defenses or facilitate persistent access.

Gather Incident Indicators

Identify and document indicators that can be used for correlative analysis on the network. Indicators can provide insight into the adversary's capabilities and infrastructure. Indicators as standalone artifacts are valuable in the early stages of incident response.

Analyze for Common Adversary TTPs

Compare TTPs to adversary TTPs documented in ATT&CK and analyze how the TTPs fit into the attack lifecycle. TTPs describe "why," "what," and "how." Tactics describe the technical objective an adversary is trying to achieve ("why"), techniques are different mechanisms they use to achieve it ("what"), and procedures are exactly how the adversary achieves a specific result ("how"). Responding to TTPs enables defenders to hypothesize the adversary's most likely course of action. Table 1 provides some common adversary techniques that should be investigated.[18]

Validate and Refine Investigation Scope

Using available data and results of ongoing response activities, identify any additional potentially impacted systems, devices, and associated accounts. From this information, new indicator of compromise (IOCs) and TTPs might be identified that can provide further feedback into detection tools. In this way, an incident is scoped over time. As information evolves, update and communicate the scope to all stakeholders to ensure a common operating picture. **Note:** see *Key Questions to Answer* for guidance.

---

[16] Derived from the MITRE ATT&CK® Framework. **Note:** this table is a representative sampling of common tactics, techniques, and related logs, and is not intended to be complete.

[17] EO 14028, Sec. 8. *Improving the Federal Government's Investigative and Remediation Capabilities*

[18] See Best Practices for MITRE ATT&CK® Mapping Framework for guidance on mapping TTPs to ATT&CK to analyze and report on cybersecurity threats.

Key Questions to Answer

☐ What was the initial attack vector? (i.e., How did the adversary gain initial access to the network?)

☐ How is the adversary accessing the environment?

☐ Is the adversary exploiting vulnerabilities to achieve access or privilege?

☐ How is the adversary maintaining command and control?

☐ Does the actor have persistence on the network or device?

☐ What is the method of persistence (e.g., malware backdoor, webshell, legitimate credentials, remote tools, etc.)?

☐ What accounts have been compromised and what privilege level (e.g., domain admin, local admin, user account, etc.)?

☐ What method is being used for reconnaissance? (Discovering the reconnaissance method may provide an opportunity for detection and to determine possible intent.)

☐ Is lateral movement suspected or known? How is lateral movement conducted (e.g., RDP, network shares, malware, etc.)?

☐ Has data been exfiltrated and, if so, what kind and via what mechanism?

Table 1: Example Adversary Tactics, Techniques, and Relevant Log and Event Data

Tactic	Common Techniques	Log and Event Sources	Indicators
Initial Access	Phishing [T1566], Drive-by Compromise [T1189], Exploit Public Facing Application [T1190], External Remote Services [T1133]	Email, web proxy, server application logs, IDS/IPS	Phishing, redirect, and payload servers (domains and IP addresses), delivery mechanisms (lures, macros, downloaders, droppers, etc.), compromised credentials, web shells
Execution	Command and Script Interpreters [T1059], Exploitation for Client Execution [T1203]	Host event logs, Windows event logs, Sysmon, anti-malware, EDR, PowerShell logs	Invocation of command or scripting interpreter, exploitation, API calls, tools, malware, payloads
Persistence	Account Manipulation [T1098], Scheduled Task/Job [T1053], Valid Accounts [T1078]	Host event logs, Authentication logs, Registry	Scheduled Tasks, registry keys, autoruns, etc.
Lateral Movement	Exploitation of Remote Services [T1210], Remote Session Hijacking [T1563], Software Deployment Tools [T1072]	Internal network logs, host event logs, Application Logs	Mismatch of users and applications/credentials, workstation to workstation communication, beaconing from hosts not intended to be internet accessible, etc.
Credential Access	Brute Force [T1110], Modify Authentication Process [T1556], Man-in-the-Middle [T1557]	Authentication Logs, Domain Controller Logs, network traffic monitoring	LSASS reads, command or scripting interpreters accessing LSASS, etc.
C2	Application Layer Protocol [T1071], Protocol Tunneling [T1572]	Firewall, Web Proxy, DNS, Network Traffic, Cloud activity logs, IDS/IPS	C2 domains, IP addresses
Exfiltration	Exfiltration Over C2 Channel [T1041], Exfiltration Over Alternative Protocol [T1048]	Firewall, Web Proxy, DNS, Network Traffic, Cloud activity logs, IDS/IPS	Domains, URLs, IP addresses, IDS/IPS signatures

Third-Party Analysis Support (if needed):

For potentially major incidents, agencies needing assistance can reach out to CISA. Each FCEB agency has a Federal Network Authorization (FNA) on file with CISA to enable incident response and hunt assistance. When seeking outside assistance, the default first action by the impacted agency should be to activate their standing FNA and request CISA assistance. Based on availability, CISA may provide a threat hunting team to assist.[19] CISA may collaborate with other agencies—such as the National Security Agency (NSA) or U.S. Cyber Command—to provide expertise or supplement CISA's capabilities.

Agencies may also bring on a third-party IR service provider to assist. Such providers supplement rather than replace the assistance provided by CISA. The NSA National Cyber Assistance Program (NSCAP)[20] provides a list of accredited IR providers. An FCEB agency using

third-party assistance is responsible for coordinating with CISA and facilitating access during the incident response, including access to externally hosted systems.

Adjust Tools:

The IR team should 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. The focus should be on preventing and detecting tactics—such as execution, persistence, credential access, lateral movement, and command and control—to minimize the likelihood of exfiltration and/or operational or informational impact. IOC signatures can be incorporated into prevention and detection tools to impose temporary operational cost upon the adversary and assist with scoping the incident. However, the adversary can introduce new tools to the network and/or modify existing tools to subvert IOC-centric response mechanisms.

[19] Level of CISA analysis support will be determined by resources available and priority of incident.

[20] National Security Agency (NSA) National Security Cyber Assistance Program

Containment

Containment is a high priority for incident response, especially for major incidents. The objective is to prevent further damage and reduce the immediate impact of the incident by removing the adversary's access. The particular scenario will drive the type of containment strategy used. For example, the containment approach to an active sophisticated adversary using fileless malware will be different than the containment approach for ransomware.

Considerations

When evaluating containment courses of action, 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), and
- Any impact on the collection, preservation, securing, and documentation of evidence.

Some adversaries may actively monitor defensive response measures and shift their methods to evade detection and containment. Defenders should therefore develop as complete a picture as possible of the attacker's capabilities and potential reactions to avoid "tipping off" the adversary. Containment is challenging because defenders must be as complete as possible in identifying adversary activity, while considering the risk of allowing the adversary to persist until the full scope of the compromise can be determined. Containment activities for major incidents should be closely coordinated with CISA.

Containment Activities

Implement short-term mitigations to isolate threat actor activity and prevent additional damage from the activity or pivoting into other systems.

Key containment activities include:

- Isolating impacted systems and network segments from each other and/or from non-impacted systems and networks. If this is needed, consider the mission or business needs and how to provide services so missions can continue during this phase to the extent possible.
- 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. Note: this containment activity is limited to advanced SOCs with mature capabilities.

Ensure that the containment scope encompasses all related incidents and activity—especially all adversary activity. If new signs of compromise are found, return to the technical analysis step to re-scope the incident. Upon successful containment (i.e., no new signs of compromise), preserve evidence for reference or law enforcement investigation, adjust detection tools, and move to eradication and recovery.

Eradication & Recovery

The objective of this phase is to 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. Before moving to eradication, 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. This is often an iterative process. It may also involve hardening or modifying the environment to protect targeted systems if the root cause of the intrusion and/or initial access vector is known. It is possible that eradication and recovery actions can be executed simultaneously. **Note:** coordinate with ICT service providers, commercial vendors, and law enforcement prior to the initiation of eradication efforts.

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. Threat actors often have multiple persistent backdoor accesses into systems and networks and can hop back into 'clean' areas if eradication is not well orchestrated and/or not stringent enough. Therefore, eradication plans should be well formulated and coordinated before execution. If the adversary exploited a specific vulnerability, initiate the Vulnerability Response Playbook below to address the vulnerability during eradication activities.

Eradication Activities

- Remediating all infected IT environments (e.g., cloud, OT, hybrid, host, and network systems).
- Reimaging affected systems (often from 'gold' sources), rebuilding systems from scratch.
- Rebuilding hardware (required when the incident involves rootkits).
- Replacing compromised files with clean versions.
- Installing patches.
- Resetting passwords on compromised accounts.
- Monitoring for any signs of adversary response to containment activities.

- Developing response scenarios for threat actor use of alternative attack vectors.
- Allowing adequate time to ensure all systems are clear of all possible threat actor persistence mechanisms (backdoors, etc.) as adversaries often use more than one mechanism.

After executing the eradication plan, continue with detection and analysis activities to monitor for any signs of adversary re-entry or use of new access methods. If adversary activity is discovered after completion of eradication efforts, contain the activity, and return to technical analysis until the true scope of the compromise and initial infection vectors are identified. If no new adversary activity is detected, enter the recovery phase.

Recover System(s) and Services

Restore systems to normal operations and confirm that they are functioning normally. The main challenges of this phase are confirming that remediation has been successful, rebuilding systems, reconnecting networks, and recreating or correcting information.

Recovery Actions[21]

- Reconnecting rebuilt/new systems to networks.
- Tightening perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.

---

[21] See [NIST SP 800-184: Guide for Cybersecurity Event Recovery](#) for additional guidance.

- Testing systems thoroughly, including security controls.
- Monitoring operations for abnormal behaviors.

A key aspect to the recovery is to 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. To validate that normal operations have resumed, consider performing an independent test or review of compromise/response-related activity. To help detect related attacks, review cyber threat intelligence (including network situational awareness), and closely monitor the environment for evidence of threat actor activity.

Post-Incident Activities

The goal of this phase is to document the incident, inform agency leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.

Adjust Sensors, Alerts, and Log Collection

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. Advanced SOCs should consider emulating adversary TTPs to ensure recently implemented countermeasures are effective in detecting or mitigating the observed activity. This testing should be closely coordinated with a blue team to ensure that they are not mistaken for true adversary activity.

Finalize Reports

Provide post-incident updates as required by law and policy.[22] Work with CISA to provide required artifacts, close the ticket, and/or take additional response action.

Perform Hotwash

Conduct a lessons-learned analysis to review the effectiveness and efficiency of incident handling. Capture lessons learned, initial root cause, problems executing courses of action, and any missing policies and procedures.

The primary objectives for the analysis include:

- Ensuring root-cause has been eliminated or mitigated.
- Identifying infrastructure problems to address.
- Identifying organizational policy and procedural problems to address.
- Reviewing and updating roles, responsibilities, interfaces, and authority to ensure clarity.
- Identifying technical or operational training needs.
- Improving tools required to perform protection, detection, analysis, or response actions.

---

[22] CISA Federal Incident Notification Guidelines

Coordination

Coordination is foundational to effective incident response. It is critical that the FCEB agency experiencing the incident and CISA coordinate early and often throughout the response process. It is also important to understand that some agencies have special authorities, expertise, and information that are extremely beneficial during an incident. This section highlights these aspects of coordination.

Coordination with CISA

Cyber defense capabilities vary widely. For this reason, coordinating involves different degrees of engagement between the affected agency and CISA. As a baseline, every cybersecurity incident affecting an FCEB agency must be reported to CISA. For organizations with mature security operations efforts, reporting and information sharing are key to assisting others.

Agencies also leverage CISA's cyber defense services to supplement their own IR capabilities. CISA provides a variety of services, such as threat hunting, analytics, malware analysis, and

CTI, that can help agencies throughout the IR lifecycle. The full list of cybersecurity services available to the FCEB are listed in the CISA Services Catalog, page 18.[23]

Reporting requirements for FCEB agencies are defined by FISMA and actioned by CISA. See the numbered circles in Figure 2 for reporting and coordination activities that should be a part of the IR process. See Appendix B, #11, for a companion checklist to track coordination activities to completion.
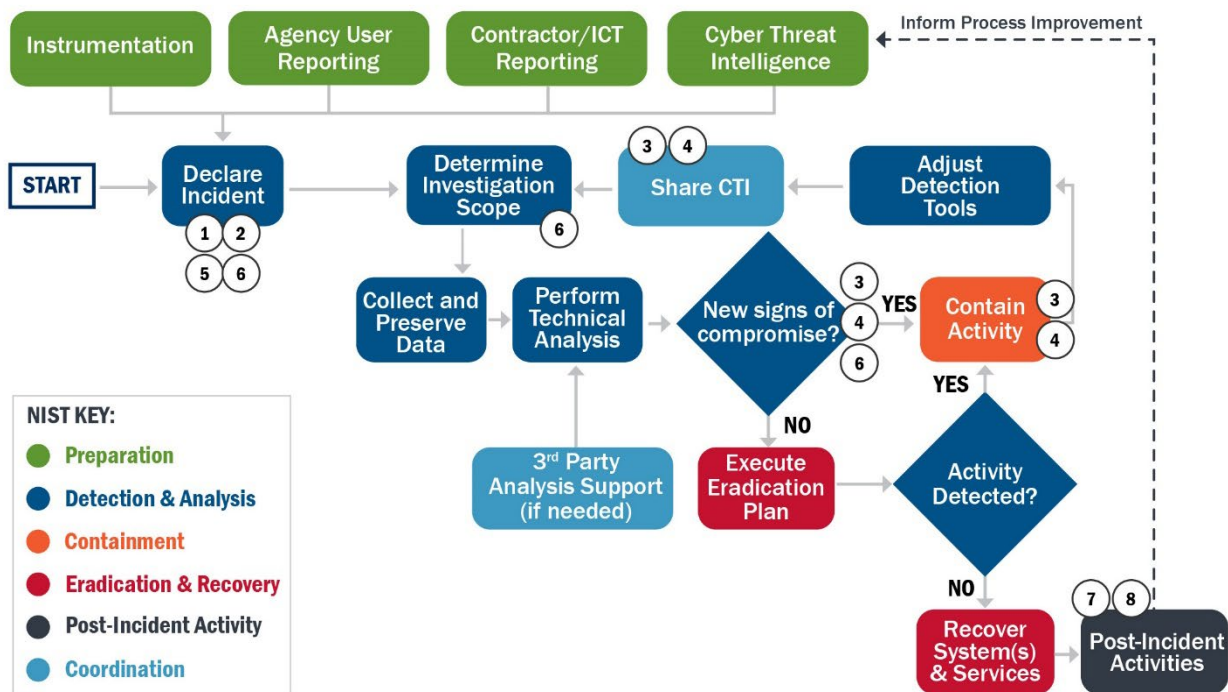

Figure 2: Numbered IR Coordination Activities

---

[23] CISA Services Catalog, First Edition: Autumn 2020

It is essential for the affected department or agency to closely collaborate and coordinate with CISA on each step in the IR flow chart. Some of the essential coordination and communication activities are defined by the numbered circles. Each number corresponds to a description below:

1) *Inform and Update CISA*

The FCEB agency provides situational awareness reports to CISA, including:

- Notifying CISA within 1 hour of incident determination as directed by OMB M-20-04. **Note:** FCEB ICT Service providers should provide notification of cyber incidents in accordance with FCEB Agency Contracting Officer (CO) requirements, which include National Security System (NSS) reporting requirements.[24]
- Where applicable, notifying their appropriate Congressional Committees, their Office of Inspector General (OIG), and OMB Office of the Federal Chief Information Officer (OFCIO) as directed by OMB M-20-04.
- Providing incident updates to CISA as appropriate until all eradication activities are complete or until CISA agrees with the FCEB agency that the incident is closed.
- Complying with additional reporting requirements for major incidents as mandated by OMB and other federal policy.[25]

2) *CISA Provides Incident Tracking and NCISS Rating*

Within one hour of receiving the initial report, CISA provides the agency with (1) a tracking number for the incident and (2) a risk rating based on the CISA National Cyber Incident Scoring System (NCISS) score.[26, 27]

3) *Share IOCs, TTPs, data*

The affected FCEB agency share relevant log data, cyber threat indicators with associated context (including associated TTPs, if available), and recommended defensive measures with CISA and sharing partners. Sharing additional threat information is a concurrent process throughout the containment phase. Incident updates include the following:

- Updated scope
- Updated timeline (findings, response efforts, etc.)
- New indicators of adversary activity
- Updated understanding of impact
- Updated status of outstanding efforts
- Estimation of time until containment, eradication, etc.

4) *CISA Shares Coordinated Cyber Intelligence*

CISA—in coordination with the intelligence community and law enforcement—shares related cyber intelligence to involved organizations.

5) *Report to Federal Law Enforcement*

The FCEB agency reports incidents to federal law enforcement as appropriate.

6) *CISA Determines Escalation*

CISA or the Federal Bureau of Investigation (FBI) determines if the incident warrants Cyber Unified Coordination Group (C-UCG) escalation, and, if so, recommends establishment of a C-UCG in accordance with the provisions of PPD-41 § V.B.b. C-UCG is the primary mechanism for

---

[24] EO 14028, Sec. 2. *Removing Barriers to Sharing Threat Information*

[25] Per OMB M-20-04, appropriate analysis of whether the incident is a major incident will include the agency CIO, CISO, mission or system owners, and, if it is a breach, the Senior Agency Official for Privacy (SAOP). Regardless of the

internal reporting chain of the organization, CISA must receive the major incident report within 1 hour of major incident declaration.

[26] CISA Federal Incident Notification Guidelines

[27] OMB M-20-04

coordination between and among federal agencies in response to a significant cyber incident as well as for integration of private sector partners into incident response efforts.

7) Provide Final Incident Report

The FCEB agency provides CISA post-incident updates as required.

8) CISA Conducts Verification and Validation

To ensure completion of recovery, CISA will validate agency incident and vulnerability response results and processes. Validation assures agencies that they are meeting baseline standards, implementing all important steps, and have fully eradicated an incident or vulnerability. For all incidents that require the use of the playbook, agencies must proactively provide completed incident response checklists and a completed incident report to close the ticket. If an agency is unable to complete the checklist, the

agency will confer with CISA to ensure all appropriate actions have been taken. CISA will evaluate these materials and:

- ☐ Determine that the incident is adequately addressed, and close the CISA ticket.
- ☐ Determine if additional response actions must be completed and request the agency complete them prior to closing the ticket.
- ☐ Request more information, including log data and technical artifacts.
- ☐ Recommend the use of CISA or other third-party incident response services.

Affected FCEB entities must take CISA-required actions prior to closing the incident. Working with affected FCEB entities, CISA determines the actions, which vary depending on the nature of the incident and eradication.

Intergovernmental Coordination

In a broader context, FCEB cyber defensive operations are not alone in tackling major incidents. Several government departments and agencies have defined roles and responsibilities and are coordinating across the government even before incidents occur. These roles and responsibilities can be described in terms of concurrent lines of effort (LOEs): asset response, threat response, intelligence support, and affected agency response; together these LOEs ensure a comprehensive response. Table 2 summarizes the LOEs for agencies in responding to cyber security incidents.

Table 2: Federal Government Leads for Lines of Effort per the NCIRP[28]

Line of Effort	Role	Lead Federal Agency
Threat Response	Conduct investigative activity and execute courses of action intended to mitigate the immediate threat; facilitate information sharing and operational coordination with asset response.	Department of Justice through the FBI and National Cyber Investigative Joint Task Force (NCIJTF)
Asset Response	Conduct response activities with FCEB agencies to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents. Coordinate with threat response and provide guidance on how to best utilize federal resources.	Department of Homeland Security (DHS) through the CISA
Intelligence Support	Facilitate building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary capabilities.	Office of the Director of National Intelligence (ODNI) through Cyber Threat Intelligence Integration Center (CTIIC)

---

[28] [National Cyber Incident Response Plan](#)

For major incidents or incidents that may become major, CISA is the "front door" for agencies for asset response. CISA will work with affected FCEB agencies to determine their needs, provide recommendations for services, and coordinate with other agencies (e.g., NSA) to provide a whole-of-government response. By serving as a single coordination point, CISA can ease the burden on FCEB agencies by facilitating the assistance available across the government.

Depending on the nature of events and involved organizations, FCEB agencies may also work directly with other LOE lead agencies in support of those LOEs. Figure 3 identifies the organizations providing the types of data and information that inform incident detection, analysis, and response.

The whole-of-government roles and responsibilities are outlined in Appendix G.
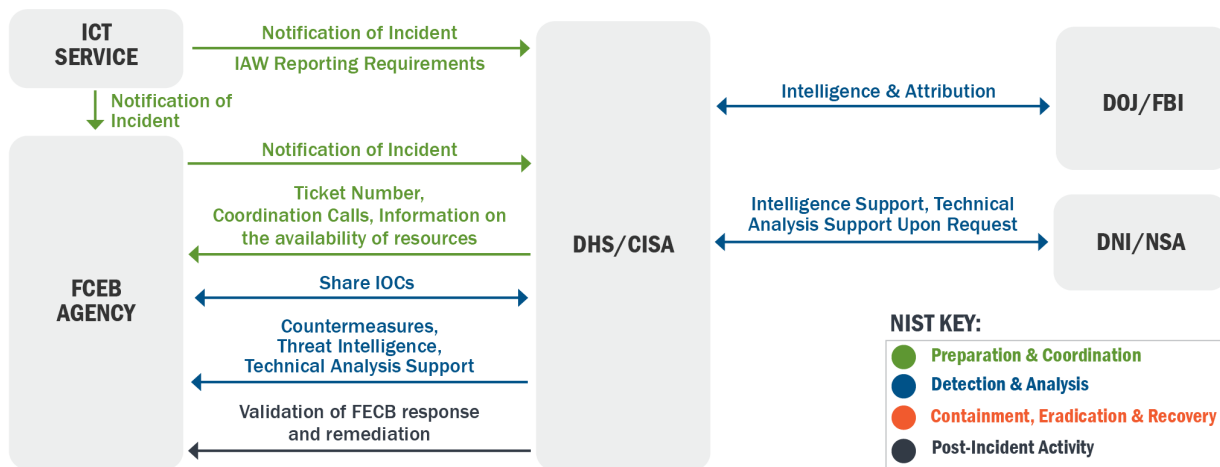

Figure 3: Whole of Government Asset Response

VULNERABILITY RESPONSE PLAYBOOK

One of the most straightforward and effective means for an organization to prioritize vulnerability response and protect themselves from being compromised is by focusing on vulnerabilities that are already being actively exploited in the wild. This playbook standardizes the high-level process that agencies should follow when responding to these urgent and high-priority vulnerabilities. It is not a replacement for existing vulnerability management programs in place at an agency but instead builds on existing vulnerability management practices. A standardized response process ensures that agencies, including CISA, can understand the impact of these critical and dangerous vulnerabilities across the federal government.

> **When to use this playbook**
>
> Vulnerabilities in scope for this playbook are those actively exploited "in the wild," namely, any vulnerability that is observed to be used by adversaries to gain unauthorized entry into computing resources.

Vulnerabilities that this playbook addresses could be observed by the impacted agency, CISA, industry partners, or others in the related mission space. Most vulnerabilities will have common vulnerabilities and exposures (CVE) descriptors. In other cases, agencies might encounter new vulnerabilities that do not yet have a CVE (e.g., zero -days) or vulnerabilities resulting from misconfigurations. Appendix D provides a companion checklist to track response activities to completion.

Preparation

Effective vulnerability response builds on strong vulnerability management. Ensure that effective vulnerability management practices are being followed.[29] Such practices include building and maintaining robust asset management that includes inventorying:

- ☐ Agency-operated systems and networks,
- ☐ Systems and networks that involve partnerships with other organizations, and
- ☐ Systems and networks operated by others, including cloud, contractor, and service provider systems.

Have a process in place to understand the relevance of vulnerabilities to the environment by tracking operating systems and other applications for all systems. Understand all systems might have vulnerabilities and the implication of potential vulnerabilities on operations.

---

[29] NIST SP 800-40 Rev. 3: Guide to Enterprise Patch Management Technologies

Vulnerability Response Process

Standard vulnerability management programs include phases for identifying, analyzing, remediating, and reporting vulnerabilities. Figure 4 describes the vulnerability response process in terms of standard vulnerability management program phases.
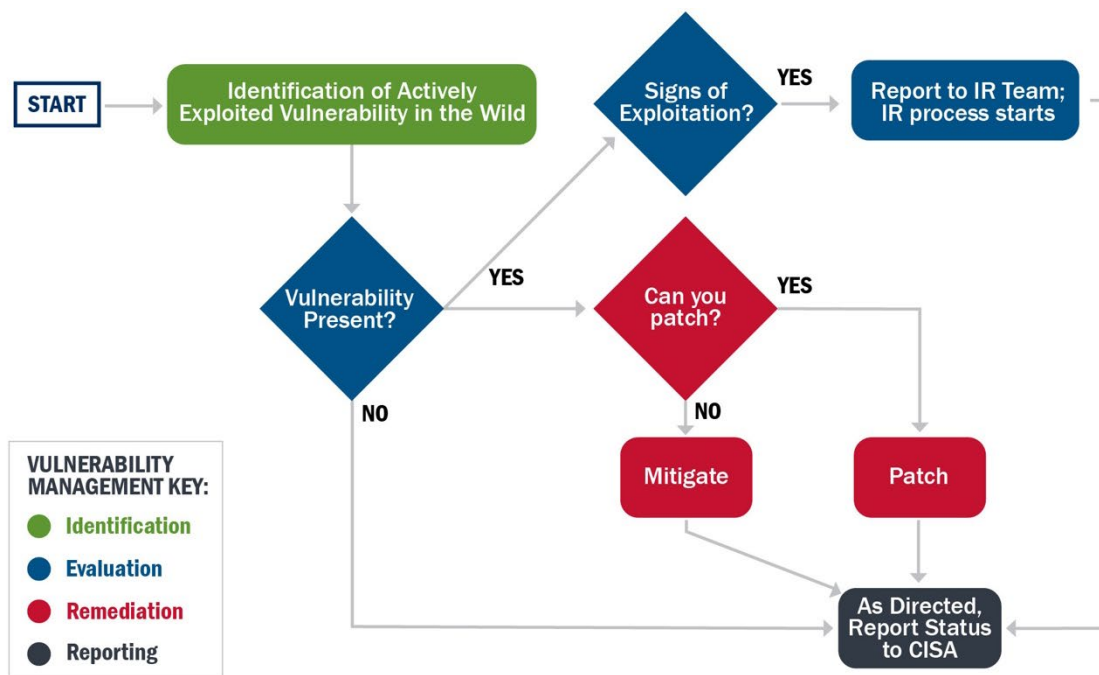

Figure 4: Vulnerability Response Phases

Identification

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 resources; for example:
  - CISA/US-CERT National Cyber Awareness System (NCAS) products, which include the weekly bulletins containing vulnerability summaries, and
    - **Note:** all agencies should subscribe to NCAS products.[30]
  - CISA Binding Operational Directive (BOD) 22-01, Managing Unacceptable Risk of Known Vulnerabilities, which is continually updated with vulnerabilities being exploited in the wild.
    - **Note:** subscribe to NCAS products for all BOD 22-01 vulnerability updates, which are announced via Current Activities.
- External threat or vulnerability feeds, such as NIST's National Vulnerability Database,[31] that can also show vulnerabilities being exploited in the wild outside FCEB agencies.

---

[30] CISA National Cyber Awareness System

[31] NIST National Vulnerability Database

☐ Internal SOC monitoring and incident response, which can detect vulnerabilities being exploited at an agency.

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 IOCs or other investigation steps that can be used to determine if it was exploited.

Evaluation

First, determine whether the vulnerability exists in the environment and how critical the underlying software or hardware is, using methodologies such as Stakeholder-Specific Vulnerability Categorization (SSVC).[32] Existing patch and asset management tools are critical and can be used to automate the detection process for most vulnerabilities. For actively exploited vulnerabilities, use the "rapid response" processes in these tools (e.g., CDM). In rare cases, such as one-off misconfigurations and zero-days, additional manual scans may need to be performed. Binding Operational Directives (BODs) or Emergency Directives (EDs) issued by CISA may also list specific technical steps to evaluate whether a vulnerability exists.

If the vulnerability exists in the environment, address the vulnerability itself—as described in the Remediation section below—and determine whether it has been exploited in the agency's environment. Use existing best practices to find signs of exploitation, including:

☐ A sweep for known IOCs associated with exploitation of the vulnerability.
☐ Investigation of any abnormal activity associated with vulnerable systems or services, including anomalous access attempts and behavior.
☐ Completion of any detection processes in CISA directives.
☐ If needed, collaboration with a third-party incident responder.

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.

---

[32] [Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization](#)

Remediation

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; or
- Making permanent configuration changes.

Existing patch management tools and processes can be used to regularly patch all vulnerabilities. Use "rapid response" processes—as described in the Evaluation section above—in those tools for vulnerabilities that are being actively exploited in the wild.

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, or
- Increasing monitoring to detect exploitation.

Once patches are available and can be safely applied, mitigations can be removed, and patches applied.

As systems are remediated, keep track of their status for reporting purposes. Each system should be able to be described as one of these categories:

- **Remediated.** The patch or configuration change has been applied, and the system is no longer vulnerable.
- **Mitigated.** Other compensating controls—such as detection or access restriction—are in place and the risk of the vulnerability is reduced.
- **Susceptible/Compromised.** No action has been taken, and the system is still susceptible or compromised.

Reporting and Notification
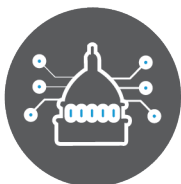
Sharing information about how vulnerabilities are being exploited by adversaries can help defenders across the federal government understand which vulnerabilities are most critical to patch. CISA, in partnership with other federal agencies, is responsible for the overall security posture of the FCEB. As such, CISA needs to maintain awareness of the status of vulnerability response for actively exploited vulnerabilities. This awareness enables CISA to help other agencies understand the impact of vulnerabilities and to narrow the time between disclosure and vulnerability exploitation. Agencies must report to CISA in accordance with Federal Incident Notification Guidelines, Binding Operational Directives, or as directed by CISA in an Emergency Directive.

APPENDIX A: KEY TERMS

Term	Definition	Source
Binding Operational Directive (BOD)	A compulsory direction to federal executive branch, civilian departments, and agencies ("agencies") for purposes of safeguarding federal information and information systems. DHS develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014 (FISMA). Federal agencies are required to comply with these DHS-developed directives.	Section 3553 of title 44, U.S. Code
Emergency Directive (ED)	In response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary of Homeland Security may issue an ED to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency for the purpose of protecting the information system from, or mitigating, an information security threat. This authority has been delegated to and may be issued with the signature of the Director of CISA.	Section 3553 of title 44, U.S. Code
FCEB Agencies	Federal Civilian Executive Branch Agencies (FCEB Agencies) include all agencies except for the Department of Defense and agencies in the Intelligence Community.	EO 14028, Sec.10
FCEB Information Systems	Those information systems operated by Federal Civilian Executive Branch Agencies but excludes National Security Systems (NSS).	EO 14028, Sec.10
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.	EO 14028, Sec. 10 44 U.S.C. 3552(b)(2)
ICT Service Providers	Information and communications technology (ICT) service providers- includes IT, OT, and cloud service providers (CSPs).	EO 14028, Sec.2
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.[33] 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 publichealth and safety of the American people.[34]	OMB Memorandum M-20-04: Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements.

---

[33] Using the CISA Cyber Incident Scoring System, this includes Level 3 events (orange), defined as those that are "likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence"; Level 4 events (red), defined as those that are "likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties"; and Level 5 events (black), defined as those that "pose an imminent threat to the provision of widescale critical infrastructure services, national government stability, or the lives of US persons."

[34] The analysis for reporting a major breach to Congress is distinct and separate from the assessment of the potential risk of harm to individuals resulting from a suspected or confirmed breach. When assessing the potential risk of harm to individuals, agencies should refer to 0MB M-17-12.

Term	Definition	Source
National Security Systems (NSS)	National Security Systems (NSS) are information systems as defined in 44 U.S.C.3552(b)(6). (A)The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i)the function, operation, or use of which— (I)involves intelligence activities; (II)involves cryptologic activities related to national security; (III)involves command and control of military forces; (IV)involves equipment that is an integral part of a weapon or weapons system; or (V)subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii)is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (B)Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).	44 U.S.C.3552(b)(6)
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.	Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, § 102

APPENDIX B: INCIDENT RESPONSE CHECKLIST

Note: the incident response playbook for incidents that involve confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out.

Step	Incident Response Procedure	Action Taken	Date Completed
	Detection & Analysis		
1. Declare Incident			
1a.	Perform initial categorization of incident.[35]		
1b.	Designate agency incident coordination lead.		
1c.	Notify CISA and, if applicable, law enforcement.		
2. Determine Investigation Scope			
2a.	Identify the type and extent of the incident.		
2b.	Assess operational or informational impact on organization's mission.		
3. Collect and Preserve Data			
3a.	Collect and preserve the data necessary for incident verification, categorization, prioritization, mitigation, reporting, attribution, and as potential evidence in accordance with NIST 800-61r2.		
3b.	Log all evidence and note how the evidence was acquired, when it was acquired, and who acquired the evidence.		
4. Perform Technical Analysis			
4a.	Develop a technical and contextual understanding of the incident.		
4b.	Based on analysis thus far and available CTI, form a hypothesis of what the adversary was attempting to access/accomplish.		
4c.	Update scope as investigation progresses and information evolves. Report most recent findings and incident status to CISA.		
4d.	**Terminating condition:** Technical analysis is complete when the incident has been verified, the scope has been determined, the method(s) of persistent access to the network has/have been identified, the impact has been assessed, a hypothesis for the narrative of exploitation has been cultivated (TTPs and IOCs), and all stakeholders are proceeding with a common operating picture.		

---

[35] OMB M-20-04

Step	Incident Response Procedure	Action Taken	Date Completed
Correlate Events and Document Timeline			
4e.	Analyze logs to correlate events and adversary activity		
4f.	Establish an incident timeline that records events, description of events, date-time group (UTC) of occurrences, impacts, and data sources. Keep updated with all relevant findings.		
Identify Anomalous Activity			
4g.	Assess affected systems and networks for subtleties of adversary behavior which often may look legitimate.		
4h.	Identify deviations from established baseline activity - particularly important to identify attempts to leverage legitimate credentials and native capabilities and tools (i.e., living off the land techniques).		
Identify Root Cause and Enabling Conditions			
4i.	Attempt to identify the root cause of the incident and collect threat information that can be used in further searches and inform subsequent response efforts.		
4j.	Identify and document the conditions that enabled the adversary to access and operate within the environment.		
4k.	Assess networks and systems for changes that may have been made to either evade defenses or facilitate persistent access.		
4l.	Identify attack vector. This includes how the adversary accessing the environment (e.g., malware, RDP, VPN).		
4m.	Assess access (depth and breadth). This includes All compromised systems, users, services, and networks.		
Gather Incident Indicators			
4n.	Review available CTI for precedent of similar activity.		
4o.	Analyze adversary tools. Assess tools to extract IOCs for short-term containment.		
4p.	Identify and document indicators that can be used for correlative analysis on the network.		
4q.	Share extracted threat information (atomic, computed, and behavioral indicators, context, and countermeasures) with internal response teams and CISA.		
Analyze for Common Adversary TTPs			
4r.	Identify initial access [TA0001] techniques (e.g., spearphishing, supply chain compromise).		

Step	Incident Response Procedure	Action Taken	Date Completed
4s.	If access is facilitated by malware, identify associated command and control [TA0011] (e.g., identify port, protocol, profile, domain, IP address).		
4t.	Identify the techniques used by the adversary to achieve code execution [TA0002].		
4u.	Assess compromised hosts to identify persistence [TA0003] mechanisms.		
4v.	Identify lateral movement [TA0008] techniques. Determine the techniques used by the adversary to access remote hosts.		
4w.	Identify the adversary's level of credential access [TA0006] and/or privilege escalation.		
4x.	Identify the method of remote access, credentials used to authenticate, and level of privilege. If access is by legitimate but compromised application (e.g., RDP, VPN), identifies the method.		
4y.	Identify mechanism used for data exfiltration [TA0010].		

Validate and Refine Investigation Scope

Step	Incident Response Procedure	Action Taken	Date Completed
4z.	Identify new potentially impacted systems, devices, and associated accounts.		
4aa.	Feed new IOCs and TTPs into detection tools.		
4bb.	Continue to update the scope and communicate updated scope to all stakeholders to ensure a common operating picture.		

5. Third-Party Analysis Support (if needed)

Step	Incident Response Procedure	Action Taken	Date Completed
5a.	Identify if third-party analysis support is needed for incident investigation or response. CISA may recommend use of another agency or a third-party for intrusion detection and incident response support services.		
5b.	Invoke Federal Network Authorization (FNA) to enable CISA incident response and hunt assistance. [36]		
5c.	Coordinate and facilitate access if incorporating third-party analysis support into response efforts.		
5d.	Coordinate response activities with agency service providers for systems hosted outside of the agency.		

6. Adjust Tools

Step	Incident Response Procedure	Action Taken	Date Completed
6a.	Tune tools to slow the pace of advance and decrease dwell time by incorporating IOCs to protect/detect specific activity.		

---

[36] CISA Services Catalog, First Edition: Autumn 2020

Step	Incident Response Procedure	Action Taken	Date Completed
6b.	Introduce higher-fidelity modifications to tools. Tune tools to focus on tactics that must be used by the adversary to obtain operational objectives (e.g., execution, credential access, and lateral movement).		

Containment

7. Contain Activity (Short-term Mitigations)

Step	Incident Response Procedure	Action Taken	Date Completed
7a.	Determine appropriate containment strategy, including: ☐ Requirement to preserve evidence ☐ Availability of services (e.g., network connectivity, services continuity) ☐ Resource constraints ☐ Duration of containment steps		
7b.	System backup(s) to preserve evidence and continued investigation.		
7c.	Coordinate with law enforcement to collect and preserve evidence (as required by (Step 3a) prior to eradication, if applicable.		
7d.	Isolate affected systems and networks including: ☐ Perimeter containment ☐ Internal network containment ☐ Host-based/Endpoint containment ☐ Temporarily disconnect public-facing systems from the Internet, etc.		
7e.	Close specific ports and mail servers. Update firewall filtering.		
7f.	Change system admin passwords, rotate private keys and service/application account secrets where compromise is suspected revoke privileged access.		
7g.	Perform blocking (and logging) of unauthorized accesses, malware sources, and egress traffic to known attacker Internet Protocol (IP) addresses.		
7h.	Prevent Domain Name Server (DNS) resolution of known attacker domain names.		
7i.	Prevent compromised system(s) from connecting to other systems on the network.		
7j.	Advanced SOCs may direct adversary to sandbox to monitor activity, gather additional evidence, and identify TTPs.		
7k.	Monitor for signs of threat actor response to containment activities.		
7l.	Report updated timeline and findings (including new atomic and behavioral indicators) to CISA.		
7m.	If new signs of compromise are found, return to technical analysis (Step 4) to re-scope the incident.		

Step	Incident Response Procedure	Action Taken	Date Completed
7n.	**Terminating condition:** Upon successful containment (i.e., no new signs of compromise), preserve evidence for reference and law enforcement investigation (if applicable), adjust detection tools, and move to eradication.		

Eradication & Recovery

8. Execute Eradication Plan

Step	Incident Response Procedure	Action Taken	Date Completed
8a.	Develop a well-coordinated eradication plan that considers scenarios for threat actor use of alternative attack vectors and multiple persistence mechanisms.		
8b.	Provide incident status to CISA until all eradication activities are complete.		
8c.	Remove artifacts of the incident from affected systems, networks, etc.		
8d.	Reimage affected systems from clean backups (i.e., 'gold' sources).		
8e.	Rebuild hardware (if rootkits involved).		
8f.	Scan for malware to ensure removal of malicious code.		
8g.	Monitor closely for signs of threat actor response to eradication activities.		
8h.	Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism.		
8i.	Update the timeline to incorporate all pertinent events from this step.		
8j.	Complete all actions for eradication.		
8k.	Continue with detection and analysis activities after executing the eradication plan to monitor for any signs of adversary re-entry or use of new access methods.		
8l.	If new adversary activity is discovered at the completion of the eradication step, contain the new activity and return to Technical Analysis (Step 4) until the true scope of the compromise and infection vectors are identified.		
8m.	If eradication is successful, move to Recovery.		

9. Execute Eradication Plan

Step	Incident Response Procedure	Action Taken	Date Completed
9a.	Restore agency systems to operational use: recovering mission/business data.		
9b.	Revert all changes made during incident.		

CISA | Cybersecurity and Infrastructure Security Agency

Step	Incident Response Procedure	Action Taken	Date Completed
9c.	Reset passwords on compromised accounts.		
9d.	Implement multi-factor authentication for all access methods.		
9e.	Install updates and patches.		
9f.	Tighten perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.		
9g.	Test systems thoroughly (including security controls assessment) to validate systems are operating normally before bringing back online in production networks.		
9h.	Consider emulating adversarial TTPs to verify countermeasures are effective.		
9i.	Review all relevant CTI to ensure situational awareness of the threat actor activity.		
9j.	Update incident timeline to incorporate all pertinent events from Recovery step.		
9k.	Complete all actions for recovery.		

 Post-Incident Activities

10. Post-Incident Activities

Step	Incident Response Procedure	Action Taken	Date Completed
10a.	Document the incident, inform agency leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.		

Adjust Sensors, Alerts, and Log Collection

Step	Incident Response Procedure	Action Taken	Date Completed
10b.	Add enterprise-wide detections to mitigate against adversary TTPs that were successfully executed.		
10c.	Identify and address operational "blind spots" to adequate coverage moving forward.		
10d.	Continue to monitor the agency environment for evidence of persistent presence.		

Step	Incident Response Procedure	Action Taken	Date Completed
Finalize Reports			
10e.	Provide post-incident updates as required by law and policy.		
10f.	Publish post-incident report. Provide a step-by-step review of the entire incident and answer the Who, What, Where, Why, and How questions.		
10g.	Provide CISA with post-incident update with seven (7) days of resolution or as directed by CISA in the **Federal Incident Notification Guidelines.**		
10h.	Work with CISA to provide required artifacts, close the ticket, and/or take additional response action.		
Perform Hotwash			
10i.	Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.		
10j.	Identify if agency IR processes were followed and if they were sufficient.		
10k.	Identify any policies and procedures in need of modification to prevent similar incidents from occurring.		
10l.	Identify how information sharing with CISA and other stakeholders can be improved during IR.		
10m.	Identify any gaps in incident responder training.		
10n.	Identify any unclear or undefined roles, responsibilities, interfaces, and authorities.		
10o.	Identify precursors or indicators that should be monitored to detect similar incidents.		
10p.	Identify if agency infrastructure for defense was sufficient. If not, identify the gaps.		
10q.	Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.		
10r.	Identify any deficiencies in the agency incident response planning process. If no deficiencies identified, identify how the agency intends to implement more rigor in its IR planning.		

Step	Incident Response Procedure	Action Taken	Date Completed
	Coordination with CISA		
11. Coordination with CISA			
11a.	Notify CISA with initial incident report within 1 hour after incident determination.[37]		
11b.	Receive incident tracking number and CISA National Cyber Incident Scoring System (NCISS) priority level from CISA.		
11c.	Comply with additional reporting requirements for Major incidents as mandated by OMB and other federal policy. [38,39]		
11d.	Provide incident updates until all eradication activities are complete.		
11e.	Report incident updates to include: ☐ Updated scope ☐ Updated timeline (findings, response efforts, etc.) ☐ New indicators of adversary activity ☐ Updated understanding of impact ☐ Updated status of outstanding efforts ☐ Estimation of time until containment, eradication, and recovery are completed		
11f.	Share relevant atomic and behavioral indicators and countermeasures with CISA throughout the IR process.		
11g.	Provide post-incident updates as directed by CISA.		
11h.	ICT service providers and contractors who operate systems on behalf of FCEB agencies must promptly report incidents to such agencies and directly report to CISA whenever they do so.		

---

[37] CISA Federal Incident Notification Guidelines

[38] Per OMB M-20-04, appropriate analysis of whether the incident is a major incident will include the agency CIO, CISO, mission or system owners, and, if it is a breach, the Senior Agency Official for Privacy (SAOP). Regardless of the internal reporting chain of the organization, CISA must receive the major incident report within 1 hour of major incident declaration.

[39] OMB M-20-04

APPENDIX C: INCIDENT RESPONSE PREPARATION CHECKLIST

Step	Incident Response Preparation	Action Taken	Date Completed
1. Policies and Procedures			
1a.	Document agency Incident Response plan with procedures for escalating and reporting major incidents and those with impact on agency mission.		
1b.	Document procedure for designating agency incident coordination lead.		
1c.	Identify key incident response personnel and responsibilities. Provide POC names, phone numbers, and email addresses.		
1d.	Identify system owners and Information System Security Officers (ISSOs).		
1e.	Identify system IPs, system security plan, system/enclave boundaries, mission essential status, etc.		
1f.	Document contingency plan for additional resourcing or "surge support" with assigned roles and responsibilities.		
2. Instrumentation			
2a.	Implement detection and monitoring capabilities to include AV, EDR, DLP, IDPS, logs, net flows, PCAP, and SIEM to provide accurate picture of agency infrastructure (systems, networks, cloud platforms, and contractor-hosted networks).		
2b.	Establish a baseline for systems and networks to understand what "normal" activity is to enable defenders to identify any deviations.		
2c.	Implement EINSTEIN capabilities.		
2d.	Implement CDM capabilities.		
2e.	Ensure logging, log retention, and log management comply with EO 14028, Sec 8.		
3. Train Response Personnel			
3a.	Train and exercise agency and staffing personnel to prepare for major incidents.		
3b.	Conduct recovery exercises to test full organizational COOP (failover/backup/recovery systems).		

Step	Incident Response Preparation	Action Taken	Date Completed
4. Cyber Threat Intelligence			
4a.	Monitor intelligence feeds for threat or vulnerability advisories from a variety of sources: government, trusted partners, open source, and commercial entities.		
4b.	Integrate threat feeds into SIEM and other defensive capabilities to identify and block known malicious behavior.		
4c.	Analyze suspicious activity reports from users, contractors/ICT service providers; or incident reports from other internal or external organizational components.		
4d.	Collect incident data (indicators, TTPs, countermeasures) and share with CISA and other partners (law enforcement, etc.).		
4e.	Set up CISA Automated Indicator Sharing (AIS) or share via *Cyber Threat Indicator and Defensive Measures Submission System*		
5. Active Defense			
5a.	For those with advanced capabilities and staff, establish active defense mechanisms (i.e., honeypots, honeynets, honeytokens, fake accounts, etc.,) to create tripwires to detect adversary intrusions and to study the adversary behavior to understand more about their TTPs.		
6. Communications and Logistics			
6a.	Establish a communications strategy. This includes: ☐ Defining an out-of-band email communication protocol ☐ Designating a war room ☐ Establishing a comm channel (phone bridge or chat room)		
6b.	Establish procedures mechanisms for coordinating major incidents with CISA.		
6c.	Designate CISA reporting POC. Provide POC name, phone number and email address. Implement info sharing format and platform to CISA.		
6d.	Define methods for handing classified information and data, if required.		
7. OPSEC			
7a.	Segment/manage SOC systems separately from broader enterprise IT systems. Manage sensors and security devices via out-of-band means (network, etc.).		
7b.	Develop method to notify users of compromised systems via phone rather than email.		

Step	Incident Response Preparation	Action Taken	Date Completed
7c.	Use hardened workstations to conduct monitoring and response activities.		
7d.	Ensure defensive systems have robust backup and recovery processes.		
7e.	Implement processes to avoid "tipping off" an attacker to reduce likelihood of detection of IR-sensitive information (e.g., do not submit malware samples to a public analysis service or notify users of compromised systems via email)		

8. Technical Infrastructure

Step	Incident Response Preparation	Action Taken	Date Completed
8a.	Establish secure storage (i.e., only accessible by incident responders) for incident data and reporting.		
8b.	Implement capabilities to contain, replicate, analyze, and reconstitute compromised hosts.		
8c.	Deploy tools to collect forensic evidence such as disk and active memory imaging.		
8d.	Implement capability to handle/detonate malware, sandbox software, and other analysis tools.		
8e.	Implement a ticketing or case management system.		

9. Detect Activity

Step	Incident Response Preparation	Action Taken	Date Completed
9a.	Implement SIEM and sensor rules and signatures to search for IOCs.		
9b.	Analyze logs and alerts for signs of suspicious or malicious activity.		

APPENDIX E: VULNERABILITY AND INCIDENT CATEGORIES

CISA has adopted the following common set of terms to improve clarity for Federal Civilian Executive Branch (FCEB) agencies for reporting to and updating CISA. [40]

Incident – Per the Federal Information Security Modernization Act of 2014 (FISMA), as codified at 44 U.S.C. § 3552(b)(2): 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 – Per the Office of Management and Budget (OMB) Memorandum M-20-04 or subsequent memo, a major incident is either:

1. 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. [41] Agencies should determine the level of impact of the incident by using the existing incident management process established in the National Institute of Standards and Technology (NIST) Special Publication (SP) 900-61 Revision 2, Computer Security Incident Handling Guide.

or,

2. 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. Major incident determination is required for breaches involving PII of 100,000 or more people. [42]

Breach – Per OMB Memorandum M-17-12 or subsequent memo: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for other than authorized purpose.

Event – Per NIST SP 900-61 Revision 2: An event is any observable occurrence in a system or network.

Vulnerabilities:

☐ Internal discovery of potential compromise leveraging a vulnerability

☐ Known exploitation of vulnerability (NVD tagged entries; wide-spread public reporting; viable proof-of-concept exploit released, etc.)

---

[40] CISA Federal Incident Reporting Requirements (draft)

[41] Using the CISA Cyber Incident Scoring System, this includes Level 3 events (orange), defined as those that are "likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence"; Level 4 events (red), defined as those that are "likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties"; and Level 5 events (black), defined as those that "pose an imminent threat to the provision of wide scale critical infrastructure services, national government stability, or the lives of US persons."

[42] The analysis for reporting a major breach to Congress is distinct and separate from the assessment of the potential risk of harm to individuals resulting from a suspected or confirmed breach. When assessing the potential risk of harm to individuals, agencies should refer to 0MB M-17-12.

APPENDIX F: SOURCE TEXT

This is a list of sources used in FCEB incident and vulnerability response.

Responsible Organization	Source Title	Category
DHS	**U.S. Department of Homeland Security Cybersecurity Strategy**	Authorities
DHS/CISA	**National Cyber Incident Scoring System (NCISS)**	Standards
DHS/CISA	**US-CERT Federal Incident Notification Guidelines (FING)**	Standards
DOJ	**Best Practices for Victim Response and Reporting of Cyber Incidents**	Best Practices
DOJ	**Sharing Cyber Threat Information Under 19 USC § 2702(a)(3)**	Law/Statute
Executive Branch	**National Cyber Strategy of the USA**	Authorities and Standards
Executive Branch	**EO 13691: Promoting Private Sector Cybersecurity Information Sharing**	Executive Order
Executive Branch	**PPD-41: United States Cyber Incident Coordination**	Authorities
Executive Branch	**Nation Cyber Incident Response Plan (NCIRP)**	
Executive Branch	**EO 13636: Improving Critical Infrastructure Cybersecurity**	Authorities
Executive Branch	**EO 13900: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**	Authorities
Executive Branch/OMB	**M-20-04, Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements**	Authorities
DOJ; FTC	**Antitrust Policy Statement on Sharing of Cybersecurity Information**	Authorities and Standards
Executive Branch	**NSPD-54/HSPD-23: Cybersecurity Policy**	Authorities
Executive Branch	**EO 13719: Commission on Enhancing National Cybersecurity**	Authorities
Executive Branch	**EO 12333: United States Intelligence Activities, as amended**	Authorities and Standards
Executive Branch	**EO 14029: Improving the Nation's Cybersecurity**	Authorities and Standards

Responsible Organization	Source Title	Category
Health SCC	**Health Industry Cybersecurity Information Sharing Best Practices**	Authorities and Standards
Executive Branch	**Cybersecurity Information Sharing Act of 2015**	Law/Statute
Executive Branch	**USA Freedom Act**	Law/Statute
Executive Branch	**PL 114-113 [6 USC § 651-674]: Cybersecurity and Infrastructure Security Agency Act of 2019**	Law/Statute
Executive Branch	**32 CFR § 236.4**	Law/Statute
Executive Branch	**US Patriot Act**	Law/Statute
Executive Branch	**PL 113-292 [codified in 6 U.S.C.]: The National Cybersecurity Protection Act of 2014**	Law/Statute
Executive Branch	**PL 107-296 [codified in 6 U.S.C.]: Homeland Security Act of 2002**	Law/Statute
Executive Branch	**44 U.S.C. § 3551: Federal Information Security Modernization Act of 2014**	Law/Statute
Executive Branch	**National Strategy for Trusted Identities in Cyberspace**	Authorities and Standards
NIST	**SP 900-53 rev4/5: Security and Privacy Controls for Information Systems and Organizations**	Authorities and Standards
NIST	**SP 900-30 rev.1: Guide for Conducting Risk Assessments**	Authorities and Standards
NIST	**SP 900-37 rev.2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy**	Authorities and Standards
NIST	**SP 900-39: Managing Information Security Risk: Organization, Mission, and Information System View**	Authorities and Standards
NIST	**NISTIR 9296: Integrating Cybersecurity and Enterprise Risk Management (ERM) (Draft)**	Authorities and Standards
NIST	**SP 900-61 Rev. 2, Computer Security Incident Handling Guide	CSRC (nist.gov)**	Standards

APPENDIX G: WHOLE-OF-GOVERNMENT ROLES AND RESPONSIBILITIES

This is a list of incident response and vulnerability response government roles and responsibilities.

Responsible Organization	Source Title	Category
Cyber Response Group (CRG)	☐ Coordinates the development and implementation of the federal government's policies, strategies, and procedures for responding to significant cyber incidents. ☐ Receives regular updates from the federal cybersecurity centers and agencies on significant cyber incidents and measures being taken to resolve or respond to those incidents. ☐ Collaborates with the Counterterrorism Security Group and Domestic Resilience Group when a cross-disciplinary response to a significant cyber incident is required. ☐ Identifies and considers options for responding to significant cyber incidents, and makes recommendations to the Deputies Committee, where higher-level guidance is required. ☐ Coordinates a communications strategy.	☐ PPD-41 ☐ NCIRP
Cyber Unified Coordination Group (C-UCG)	☐ Primary mechanism for coordination between and among federal agencies in response to a significant cyber incident as well as for the integration of private sector partners into IR efforts. ☐ The CRG may request the formation of a Cyber UCG. ☐ A Cyber UCG may also be formed when two or more federal agencies* that generally participate in the National Security Council (NSC) Cyber Response Group (CRG) request its formation. *These include relevant Sector Risk Management Agencies (SRMAs). ☐ Identifies and recommends to the CRG, if elevation is required, any additional federal government resources or actions necessary to appropriately respond to and recover from the incident.	☐ PPD-41 ☐ NCIRP
DHS/CISA	☐ Lead agency for asset response activities. ☐ Collaborates with industry and government partners to help organizations understand and counter critical infrastructure and cybersecurity risks associated with the malicious activities of nation-state and non-state actors. ☐ Coordinates Government-wide efforts on information security policies and practices; compiles and analyzes agency information security data; develops and conducts targeted operational evaluations, including threat and vulnerability assessments; and hunts for and identifies threats and vulnerabilities within Federal information systems. ☐ Centrally collects and manages FCEB and ICT service provider incident information per EO 14028. ☐ Provides CTI to agencies directly or at scale. When sharing CTI with an agency, or multiple agencies, CISA will communicate with the agency SOC, and depending on the severity, may include the agency CISO along with additional POCs the agency has explicitly designated for the information exchange. ☐ Communicates with the affected FCEB Agencies to understand the nature of the cyber incident or vulnerability. ☐ Disseminates intelligence and information learned during the IR response to other federal agencies for awareness and threat-informed defense. ☐ When sharing at scale, CISA publishes to cisa.gov (such as https://us-cert.cisa.gov/ncas/alerts). Information too sensitive to publish is distributed	☐ PPD-41 ☐ CISA Act of 2018 ☐ FISMA (44 USC 3553(b)) ☐ EO 14028 (Secs. 2,6) ☐ NCIRP

Responsible Organization	Source Title	Category
	via alternative avenues into the FCEB space, such as the weekly agency SOC call, HSDN, or classified networks. ☐ Hosts FCEB agency incident coordination call. Provides recommendations on actions, data to collect/check. ☐ Advises FCEB of available resources to assist in response, including CISA, FBI, NSA, and third-party entities. ☐ Upon request, provide analysis, expertise, and other technical assistance to the affected FCEB agency. Available cybersecurity services can be found on page 18 in the CISA service catalog.[43] ☐ Provides informational webinars to educate FCEB agencies on targeted cyber threats and mitigations. ☐ Reviews and validates FCEB agency's incident response and remediation results upon completion of the incident response.	
DOJ/FBI/NCIJTF	☐ Lead agency for threat response activities. ☐ Law enforcement investigation, forensics, and mitigation activities to support interdiction of the threat actor. ☐ Provide attribution that may lead to information sharing. ☐ Disseminates intelligence and information learned during the response to FCEB Agencies. ☐ Investigation of FCEB agency incidents that may have a criminal nexus. ☐ Share intelligence, including attribution.	☐ PPD41 ☐ NCIRP ☐ Other LE authorities
FCEB Agency	☐ Coordinates with CISA for cyber response as directed by CISA Federal Incident Notification Guidelines and the IR playbook. ☐ Provides additional notification to OMB, OFCIO, Congress, OIG, if applicable. ☐ Reports incident to law enforcement, as appropriate. ☐ Notifies stakeholders of actions they need to take. ☐ Provides cyber threat indicators with available associated context, to include associated TTPs if available, and recommended defensive measures to CISA and sharing partners. ☐ Allows access and assists third-party incident responders when requested by CISA. ☐ Provides network and system log information (including ICT provider logs) to CISA upon request per EO 14028, Sec 8. ☐ Maintain business and operational continuity. ☐ Comply with legal and regulatory requirements. ☐ Engage in communications with employees or other affected individuals. ☐ Conduct incident response within FCEB and its subcomponents, ensuring that the agency-level SOC has operational control of incident response activities.	☐ PPD41 ☐ CISA Act of 2018 ☐ Federal Incident Notification Guidelines (FING) ☐ FISMA (44 USC 3553(b)) ☐ EO 14028 (Secs. 2,6)
ICT Service Providers	☐ Report cyber incidents to FCEB agencies and directly report to CISA when doing so. ☐ Collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of FCEB agencies. ☐ Share data, information, and reporting as set forth under EO 14028, section 2. ☐ Collaborate with federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents on	☐ EO 14028 (Sec. 2)

---

[43] CISA Services Catalog, First Edition: Autumn 2020

Responsible Organization	Source Title	Category
	Federal Information Systems (FIS), including implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed.	
National Security Council (NSC)	☐ Coordinates the Cyber Unified Coordination Group (UCG): the interagency and private sector partner coordination mechanism to take immediate response actions to a cyber incident of specific severity and scale.	☐ PPD41
ODNI/CTIIC	☐ Lead agency for intelligence support and related activity. ☐ Provide classified threat reporting on cyber adversaries and other national security topics. ☐ Coordinates intelligence collection. ☐ Provides attribution. ☐ Provides situational awareness, shares of relevant intelligence information, integrated analysis of threat trends, events, and support to interagency efforts to develop options to degrade or mitigate adversary threat capabilities.	☐ PPD41 ☐ NCIRP
Third-Party Analysis Support	☐ Incident response support may come from CISA, other government entities (such as FBI, NSA), or commercial vendors upon request from the agency or from CISA ☐ Available CISA cybersecurity services can be found on page 18 in the CISA service catalog.[44]	☐ Homeland Security Act (6 USC 659) ☐ Federal Network Authorization (FNA)
National Security Agency (NSA)	☐ Provide intelligence support in response to cyber incidents and vulnerabilities. ☐ Provides attribution information. ☐ Provides technical support upon request. ☐ Provides threat response, asset response and intelligence support to NSS/other systems.	☐ EO 12333 ☐ NSD-42 ☐ PPD41

[44] CISA Services Catalog, First Edition: Autumn 2020