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