FCEB OPERATIONAL CYBERSECURITY ALIGNMENT (FOCAL) PLAN

Version: Public Version
Publication: July 2024

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

REVISION HISTORY

The version number will be updated for each subsequent publication of the FOCAL Plan.

Version	Summary of revisions	Edited By	Date
1.0	• Publication of version 1.0	FEIT	03/01/2024
Public Version	• Shorter, public version of plan	FEIT	07/22/2024

Contents

1. INTRODUCTION

The Federal Civilian Executive Branch (FCEB) is comprised of agencies driven by unique missions. All have independently established networks and system architectures to advance their critical work on behalf of the American people. This independence has led to several outcomes that serve as a backdrop to the development of the FCEB Operational Cybersecurity Alignment (FOCAL) Plan. Agencies vary widely in how effective they are at managing cyber risk, which means there is no cohesive or consistent baseline security posture across all FCEB agencies. These diverse approaches were not designed to collectively address the dynamic nature of our current cyber threat environment, the complexity of our digital ecosystem, and the pace of technology modernization. As a result, despite concerted efforts to adapt and protect against cyberattacks, the FCEB remains vulnerable.

Though risk is best managed at the lowest level possible, standardizing the essential components of enterprise operational cybersecurity across agency components and across the interagency is now more critical than ever. Collective operational defense is required to adequately reduce risk posed to more than 100 FCEB agencies and to address dynamic cyber threats to government services and data. CISA's FCEB Operational Cybersecurity Alignment (FOCAL) Plan outlines how agencies can work toward this by adopting proven practices along the spectrum—from prevention to incident detection and response—and identifying collective goals for security across the federal enterprise.

> *As the operational lead for federal cybersecurity, CISA has oriented the actions of this plan toward "operational cybersecurity," referring to the daily activities and processes used by organizations to defend their data and information systems. These activities may include managing assets and vulnerabilities, communicating and sharing cybersecurity information, planning and architecting future capabilities, and investigating and responding to cybersecurity incidents.*

In recent years, the federal government's executive orders, policies, and directives have driven significant cybersecurity improvements at federal agencies in response to this dynamic threat environment. As the Office of Management and Budget (OMB) and Office of the National Cyber Director (ONCD) continue to shape national cybersecurity policy and set strategic expectations for federal cybersecurity, the Cybersecurity and Infrastructure Security Agency (CISA) is the operational lead, ensuring the enterprise has the necessary capabilities to meet those expectations.

1.1 ALIGNING THE FEDERAL ENTERPRISE

The FOCAL Plan is a strategic document that includes broad organizing concepts for federal cybersecurity and a tactical one that provides specific actionable steps agencies can take in the next year to improve their cybersecurity posture. This plan identifies areas in need of standardization and consistency (***priority areas***), enabling the federal enterprise's cyber defense apparatus during steady state operations and facilitating rapid response when urgent situations require interagency action.

The FOCAL Plan is not intended to provide a comprehensive or exhaustive list of everything that an agency or CISA must accomplish. It is designed to focus resources on those actions that substantively advance operational cybersecurity improvements and ***alignment goals.***

Table 1: FOCAL Plan Terminology and Definitions

Focal Plan Term	*Definitions*
Priority Area	An area of cybersecurity performance that CISA considers critical to the *alignment* of capabilities across the federal enterprise based on feedback, research, and experience. Each prioritized area will serve as the foundation of CISA's conversations with FCEB agencies in FY 2024. These conversations will help CISA better understand the agencies' needs and develop the products, services, and guidance to meet those needs.
Alignment Goal	A subset of each priority area, alignment goals have been created on the operational level with an eye toward standardization and, ultimately, alignment of effort and capabilities across the federal enterprise.

Increased alignment between CISA and FCEB agencies will have real world impact and will shape the actions taken in response to the dynamic threat environment. The ultimate destination on this shared journey is more synchronized and robust cyber defenses, greater communication, and increased agility and resilience across the federal enterprise, resulting in a more cohesive government enterprise capable of defending itself against evolving cyber threats.

1.1.1 FOCAL Plan Overview

This plan is organized into five priority areas that CISA considers essential for positioning efforts across the federal cybersecurity landscape and that align with agencies' Federal Information Security Modernization Act metrics and reporting requirements.

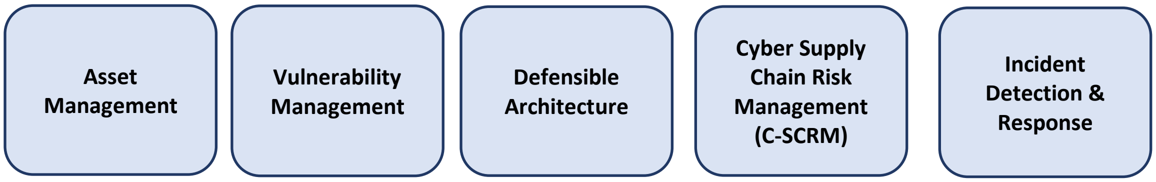
Asset Management
Vulnerability Management
Defensible Architecture
Cyber Supply Chain Risk Management (C-SCRM)
Incident Detection & Response

Figure 1: Five FOCAL Priority Areas

2. PRIORITY AREA 1: ASSET MANAGEMENT

Full understanding of the cyber environment, including both operational terrain and interconnected assets, is foundational for the federal enterprise. Agencies must properly account for and manage each individual asset to defend against sophisticated attacks from adversaries or determine localized risk posed by an insecure software product. This level of operational visibility is essential in our current threat environment.

Achieving comprehensive asset visibility and enabling continuous, automatic updates to an asset catalog can be challenging for large organizations, but managing cybersecurity risk necessitates this critical step in gaining full awareness of an enterprise's digital footprint. Enterprise-wide asset management directly enables targeted vulnerability and incident response, facilitates rapid identification and collective action, and supports on-demand coordination between CISA, the agency, and peer agencies or other key stakeholders.

Recent advances in continuous diagnostics and mitigation (CDM) capabilities and agency programs have dramatically improved the collective federal cybersecurity posture. As we expand our focus from the cyber risk governance enablement to interactive cyber operations—using CDM to gain and maintain host-level visibility and leveraging this information to drive strategic and tactical discussions—all agencies must focus their efforts and align their work to meet these objectives.

In October 2022, CISA issued Binding Operational Directive (BOD) 23-01 to standardize the federal government's approach to enhancing continuous visibility into agency assets and associated vulnerabilities. This BOD amplified the importance of asset management and defined expectations of how agencies should fully participate in a CDM program. While CISA's CDM Program has been a key enabler for federal agencies in asset management, the requirements outlined in the BOD were created to serve as a blueprint for any organization. Priority Area 1: Asset Management builds on the successes that have come from agencies' work following the issuance of BOD 23-01 and response to several zero-day vulnerabilities.

2.1 ALIGNMENT GOAL: INCREASE OPERATIONAL VISIBILITY

CISA is committed to gaining greater cyber operational visibility and driving timely risk reduction. Increased visibility into assets and vulnerabilities will improve the capabilities of CISA and individual agencies to detect, prevent, and respond to cybersecurity incidents. These are critical steps in managing cybersecurity risk.

To accomplish alignment goal 2.1, agencies should have completed these foundational activities:

- Established a centralized hardware and software inventory database that uses automated updates.
- Established automated asset discovery, conducting asset discovery scans at least every seven days.
- Documented asset coverage and capability gaps and strategies to address them.

3. PRIORITY AREA 2: VULNERABILITY MANAGEMENT

What constitutes an agency's enterprise has evolved over the years, particularly as the attack surface has expanded and grown more complicated. One key to vulnerability management is to acquire and maintain the initiative within one's environment. This is done by embracing sustainable and forward-leaning approaches to preemptively mitigate risks rather than defaulting to a reactive posture reliant on a constant flow of alerts and advisories.

Vulnerability response must be a strategic imperative, both across the FCEB and at the individual agency level. Enabling timely, coordinated, and collective cyber response is critical to cybersecurity and can only be achieved through standard vulnerability management procedures and clear expectations.

The federal government has steadily matured its cyber vulnerability management capabilities. These include specific requirements for securing high-value assets (BOD 18-02), remediating vulnerabilities in internet-accessible systems (BOD 19-02), establishing vulnerability disclosure programs (BOD 20-01), managing the heightened risk of known exploited vulnerabilities (BOD 22-01), and investing in regular asset and vulnerability scanning (BOD 23-01).

CISA recognizes that there is work to be done to align vulnerability management activities across the federal enterprise. Improving vulnerability management across the FCEB will provide more timely and efficient mitigation of vulnerabilities and give CISA a better understanding of the federal-wide attack surface, enabling a more agile and coordinated response when vulnerabilities are detected.

3.1 ALIGNMENT GOAL: MANAGE THE ATTACK SURFACE OF INTERNET-ACCESSIBLE ASSETS

By understanding the total number of entry points, vulnerabilities, and weaknesses an adversary might exploit to gain unauthorized access to their system or network, agencies can reduce risks on their attack surface. Internet-accessible assets are of particular focus, due to the increased exposure.

To accomplish alignment goal 3.1, agencies should have completed these foundational activities:

- Regularly performed full-credentialed vulnerability scanning across all assets.
- Leveraged internal capabilities, directive requirements, and CISA cybersecurity advisories to enable vulnerability prioritization and more timely mitigation of critical vulnerabilities.
- Established processes and procedures to identify and prioritize vulnerabilities for remediation within mandated timeframes.

4. PRIORITY AREA 3: DEFENSIBLE ARCHITECTURE

As federal agencies modernize their technology, the importance of keeping every new component working seamlessly with the existing systems can create new cybersecurity challenges. This is why agencies must intentionally build a *defensible architecture.*

The goal of a defensible architecture is resilience. A defensible architecture is designed with an understanding that security incidents are inevitable and, therefore, does not rely solely on detecting an incident to minimize its harm. Instead, the network and systems are designed with the appropriate controls to limit an adversary’s ability to access sensitive data or disrupt operations even after successful compromise of part of the infrastructure. Zero Trust (ZT) is a critical part of building more defensible architecture.

From CISA’s perspective, for an architecture to be defensible, it must:

- Have a mature, enterprise-wide identity management solution that enables cybersecurity professionals to understand who the users are and what resources they should be accessing.
- Isolate different resources from one another through host-based or network-based segmentation, limiting an adversary’s ability to move laterally after a single point of compromise.
- Harden systems controlled or hosted by third parties such as those relying on platform-as-a-service and software-as-a-service offerings.
- Take precautions against “upstream” vulnerabilities that occur outside of the organization’s immediate control, such as Domain Name System-based attacks.

4.1 ALIGNMENT GOAL 1: SECURE CLOUD BUSINESS APPLICATIONS

Transitioning to cloud computing environments provides clear benefits in managing resources and the agility to leverage technology advancements including security services. CISA offers federal agencies a set of security configurations, like those used for on-premises applications and systems, to help protect information stored within these environments. By implementing these best practices, cloud environments and business applications are better protected from cybersecurity vulnerabilities and are more capable of detecting, responding, and recovering from cyber incidents.

4.1.1 Alignment Goal 2: Share Cybersecurity Telemetry Data With CISA

As agencies continue to modernize their services and underlying architectures, network traffic may no longer be available to CISA through traditional Trusted Internet Connection (TIC) access-points. OMB Memorandum 19-26: Update to the Trusted Internet Connections (TIC) Initiative (TIC 3.0) allows agencies to leverage modern and distributed architectures to connect to the internet more efficiently and securely. The various TIC 3.0 use cases (Cloud, Remote User and Branch Office) demonstrate how agencies can share telemetry with CISA.

4.1.1.1 Alignment Goal 3: Enhance ZT Capabilities Across the Federal Enterprise

Adopting the ZT "never trust, always verify" principle is central to mitigating the likelihood and impact of future cyber incidents and maintaining operational resilience in the face of cyberattacks. While implementing a Zero Trust Architecture (ZTA) enterprise-wide is a long-term investment, it can be integrated incrementally and is already in progress through efforts such as phishing-resistant Multi-Factor Authentication (MFA), improved inventories of devices, and increased Endpoint Detection and Response (EDR) coverage.

To accomplish alignment goal 4.1.1.1, agencies should have completed these foundational activities:

- Identify challenges to meeting agency ZT implementation plans and develop potential solutions.
- Identify internet-exposed management interfaces and removed the interface from the internet or deployed capabilities that enforce access controls through a Policy Enforcement Point (PEP).
- Identified, justified and addressed technical, business and process gaps in meeting the phishing-resistant MFA implementation requirement in a plan, documenting tasks and resources required to bridge gaps.

5. PRIORITY AREA 4: CYBER SUPPLY CHAIN RISK MANAGEMENT

The U.S. government has taken meaningful steps to improve how it manages significant risk to the cyber supply chain. With the Federal Acquisition Supply Chain Security Act of 2018, Congress established the Federal Acquisition Security Council (FASC) as a standing body to review, investigate, and act on cyber supply chain-related concerns; similarly, the federal interagency created numerous cross-functional leadership working groups to address cybersecurity supply chain risks.

In its role as the operational cybersecurity lead, CISA has produced cybersecurity supply chain guides, training content, and communities of practice to build interagency capacity. These resources range from guides such as Defending Against Software Supply Chain Attacks and a C-SCRM-related publications library to the establishment of the Federal C-SCRM Roundtable. The focus in FY 2024 and beyond is ensuring that when there is a risk to software or hardware—whether it leads to an actual supply chain compromise or not—the federal enterprise is able to quickly identify where the problematic software exists in federal IT environments and act to mitigate that risk.

Third-party risk continues to increase as agencies rely on more external providers and technology. As a result, agencies are accountable for their own security posture and must also be aware of the security posture of the numerous third parties with whom they do business. This priority area aligns the work CISA has done to improve cyber supply chain with the agencies' efforts to better understand the risk posed by third parties, including "acquirers, suppliers, developers, system integrators, external system services providers, and other [Information and Communication Technology (ICT)/Operational Technology (OT)]-related service providers."[1] To address risk across the wider supply chain ecosystem, agencies must establish an enterprise-level view and engage upper-level leadership on cyber supply chain risks.

[1] Boyens, Jon, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, and Matthew Fallon. "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." CSRC, May 5, 2022. https://csrc.nist.gov/pubs/sp/800/161/r1/final.

5.1 ALIGNMENT GOAL 1: PREPARE FOR RAPID REMOVAL OF HIGH-RISK SOFTWARE AND HARDWARE

A software or hardware product may be identified through various authoritative sources (e.g., federal government, industry) as too risky to be present on enterprise networks. Organizations should ensure that processes are in place to: rapidly identify those products on their networks, evaluate the impact of removing the products, develop a plan for removing the identified products, and establish a process to ensure that removed products are not reintroduced.

To accomplish alignment goal 5.1, agencies should have undertaken these foundational activities:

- Established supply chain processes and structures that integrate C-SCRM requirements and information sharing into enterprise governance.
- Coordinated across the agency and developed an agency-wide C-SCRM strategy to make informed risk-based decisions.
- Included appropriate C-SCRM requirements and guidance into procurement/contractual agreements with suppliers.
- Developed organizational supplier requirements to ensure that suppliers address product and service risks.
- Identified and removed information and communications technologies or services as directed by federal, state and local laws, policies and directives.

6. PRIORITY AREA 5: INCIDENT DETECTION AND RESPONSE

The maturity of incident detection and response capabilities varies between organizations, yet even the most effective Security Operations Centers (SOCs) are unable to detect all intrusions. Adversaries' tactics, techniques, and procedures increasingly use built-in administration tools, a technique known as "living off the land" (LOTL) to blend in and make detection more difficult. The movement of IT services to external providers creates additional visibility challenges to manage. In this environment, SOCs are faced with the daunting challenge of detecting these more subtle attacks on constantly changing, hybrid IT environments. Incident detection and response is a critical component of an effective cybersecurity program, as no protective measures are likely to fully prevent adversaries' access to federal IT assets.

Aligning the enterprise's incident detection and response capabilities requires improving the ability of agency SOCs to see and protect assets across the enterprise, as well as the data residing on those assets. Implementing proper logging on those devices, beginning with agencies' High Value Assets and internet-facing systems that are most likely to be targeted will be key to detecting stealthy techniques such as LOTL and preventing the threat actor from establishing persistence. Early detection enables SOCs to respond quickly, limit the impact of intrusions, and capture and share relevant threat information. This requires a defined, measured, and enforced set of enterprise-wide standards and metrics.

As part of this strategy, agency SOCs rely on best-in-class security technologies, such as EDR, which are being "architected" to accomplish "whole-of-government" threat hunting and incident response.

6.1 ALIGNMENT GOAL 1: ENABLE CISA'S PERSISTENT ACCESS CAPABILITY

Cyber criminals and nation-state actors have demonstrated the ability to gain and maintain access to FCEB assets for extended periods. By ensuring EDR coverage across the agency and enabling CISA's persistent access capability, agencies facilitate situational awareness and information sharing across the federal enterprise. This positions agency and CISA cybersecurity operations to detect, analyze, respond, and mitigate incidents, improving defense and continuous detection and rapid response actions.

6.1.1 Alignment Goal 2: Advance SOC Governance

Given the rise in adversarial activity, a focus on enterprise-level operational visibility provides agency SOCs with the agility necessary to detect and respond using a common operating picture. This allows SOCs to facilitate actions that reduce the scope and severity of an initial intrusion. The feedback loop from security operations into the broader cybersecurity program supports risk management decisions and decreases the likelihood and severity of future incidents.

To accomplish alignment goals 6.1 and 6.1.1, agencies should have completed these foundational activities:

- Engaged in cross-agency technical exchanges to share information and feedback about operational challenges, best practices, standards, and acquisitions to improve data quality and relevance.
- Integrated Cyber Threat Intelligence (CTI) tools, data, and services, including commercial CTI, to improve agencies' CTI generation, consumption, utilization and sharing.
- Assessed and compared the agency's "As-Is" status against applicable governance and mandates to identify compliance challenges and issues and communicate them to CISA.