

Know It. Control It. Contain It.

**A Binding Operational Directive for
OT Cybersecurity**

October 6, 2026



**Operational Technology
Cybersecurity Coalition**

Table of Contents

-  **Executive Summary**
-  **Introduction**
-  **Why do we need an OT BOD?**
-  **Recommendations**

Executive Summary

The convergence of AI-accelerated threats, blatant adversary pre-positioning in our critical networks, and a renewed federal focus on resilience has opened a rare, urgent window of opportunity. Policymakers are finally paying attention. We at the Operational Technology Cybersecurity Coalition (OTCC) are optimistic that we can channel this momentum into mandatory, enforceable baseline requirements to finally protect federal civilian operational technology (OT).

This proposal lays out the path forward through a dedicated Cybersecurity & Infrastructure Security Agency (CISA) Binding Operational Directive (BOD). A BOD is not about adding compliance red tape to plant operations; it is about establishing the non-negotiable, pre-incident baseline that prevents attacks from cascading into physical catastrophes. Emergency resilience frameworks like CI Fortify are vital for surviving the storm, and we strongly support CISA's efforts on this project, but they cannot be our only line of defense. By pairing post-compromise resilience with a targeted OT BOD focused on defined Continuous Diagnostics and Mitigation (CDM) visibility, pragmatic microsegmentation, enforceable remote access, documented incident preparedness processes, established configuration baselines, and verified backup and recovery capabilities, CISA can finally give operational technology the mandatory security posture it has needed for years.

The following memo outlines actionable steps to strengthen enterprise cybersecurity oversight, governance, and compliance across Federal Civil Executive Branch (FCEB) agencies. Aligning operational directives with CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) and mandating clear administrative ownership is essential for a unified, risk-based defense of federal infrastructure. We urge CISA to review these recommendations for fundamental baseline actions and work with the OT industry to take reasonable, actionable, implementable steps to secure OT environments.

OTCC recommendations for CISA to release as a BOD for OT environments within the FCEB that:

1. Establishes Clear OT Governance and Accountability
2. Incorporates OT More Broadly across Existing Guidance
3. Aligns CPGs to OT Needs and Prioritizes Implementation

Introduction

The spate of cyberattacks this past summer on U.S. water systems in at least 12 states was a painful reminder of how vulnerable our critical infrastructure is to malicious actors' ill intent. Worse, it could have been prevented, or at least its impact limited. The OT systems impacted were due to devices that shouldn't have been connected online, default or non-existent passwords, and lack of network segmentation. Thankfully, utility workers across the states quickly switched to manual operations, highlighting the importance of OT resilience. Yet this should serve as a call to action to take immediate steps to shore up the United States' OT security, especially for systems that serve or connect to the federal government.

CISA can improve the cybersecurity of OT systems within the federal government while also sending a powerful message to private, state, and local critical infrastructure. Since its establishment in 2018, CISA has consistently used BODs when it determined that voluntary guidance alone proved insufficient to address systemic cybersecurity risk across the FCEB. Unlike guidance or recommendations, a BOD establishes mandatory cybersecurity requirements for FCEB agencies, enabling CISA to drive consistent implementation and measure compliance across the government. The value of a BOD is to establish a uniform, government-wide baseline so that CISA can understand, measure, and manage cyber risk consistently across the FCEB. While private or local entities are not required to implement BODs, they still provide a strong demand signal of what the government views as a cybersecurity best practice.

Why do we need an OT BOD?

Despite years of guidance, increasing convergence between IT and OT, and repeated warnings that Chinese actors have pre-positioned themselves inside critical infrastructure, establishing strict requirements and controls for OT environments has historically been difficult due to their unique operational demands. To be fair, CISA has incorporated OT security requirements into prior directives (such as BODs 23-01, 23-02, and 26-04) alongside a host of technical guidance. But as AI reduces the technical barriers to sophisticated cyber operations, enabling adversaries to identify weaknesses, accelerate reconnaissance, and move laterally through poorly segmented operational environments with greater speed and scale, it is time for an encompassing BOD solely focused on OT security.

An OT BOD is necessary to address three core systemic challenges across government:

1. **Widespread Risk:** The FCEB relies on more than 8,000 General Services Administration (GSA)-managed owned and leased facilities, such as laboratories, hospitals, research campuses, warehouses, ports of entry, and other specialized facilities. The OT that supports these environments, including HVAC, power management, access control, water systems, and building automation, is essential to maintaining safety and federal mission continuity during cyber incidents. Yet, CISA does not currently have a holistic view of the assets managed by the FCEB and the potential risks, such as connected programmable logic controllers, to which the government may be exposed.

2. **Inconsistent Implementation:** Federal agencies retain broad discretion over how operational technology is secured. While guidance exists, no BOD establishes consistent minimum cyber practices or requirements for agencies to demonstrate implementation. Because agencies govern OT independently, CISA lacks consistent visibility into the security posture of federal OT. The Government Accountability Office (GAO) recently found that most federal agencies have not implemented the Office of Management and Budget (OMB's) 2023 security requirements for network devices for OT systems. As a result, GAO found “agencies that have not yet fully met the requirements may continue to struggle to apply appropriate security controls to their devices, make informed risk-based decisions about mitigating security threats, and respond appropriately in the event of a cybersecurity incident.”
3. **Unacceptable Consequences:** Cyber incidents affecting OT can directly affect safety, disrupt the federal government's ability to deliver essential services, protect personnel, and sustain continuity of operations. As the cyber incidents on US water and wastewater systems show, the consequences of cyberattacks impacting OT systems can be severe. The National Security Agency determined the risk to be unacceptable and, in 2024, as the National Manager for National Security Systems, issued BOD 2024-001 establishing OT security implementation, reporting, inventory, and minimum-control requirements for OT systems. Ultimately, an OT focused BOD would enable CISA to advance President Trump's National Resilience Strategy by “reduc[ing] risk [and] improv[ing] reliability of infrastructure and continuity of key services.”

To address these vulnerabilities effectively across the FCEB, federal policy must cover both operational continuity during an attack and proactive defense before an intrusion occurs. In recent months, policy discussions have increasingly focused on resilience initiatives designed to ensure critical functions persist under fire. While preparing for worst-case operational disruption is essential, resilience planning represents only half of a complete cybersecurity architecture. That is why we embrace CI Fortify's approach: prepare for compromise and have adequate response measures in place. CI Fortify plans for assumed compromise, telecommunications disruption, isolation, continued operations, and recovery. Where emergency planning frameworks address keeping operations running during and after an incident, a dedicated OT BOD establishes the preventive and containment baseline: **Know it. Control it. Contain it.**

PREVENTION AND CONTAINMENT BASELINE

Know it.
Control it.
Contain it.

Recommendation

Recommendation: CISA should establish an OT BOD that requires FCEB entities with OT systems and assets to achieve specific cybersecurity goals. Specifically, CISA should:

1

Establish clear organizational ownership and accountability for OT environments.

Because operational technology frequently falls into a governance gray zone between Chief Information Officers and physical facilities managers, CISA must mandate clear administrative ownership. Specifically, the directive should require agencies to:

- Formally designate a senior official or unified office responsible for the cybersecurity governance, asset inventory validation, configuration baselines, backup and recovery, incident preparedness, and risk reporting of all agency-managed and CSA-leased OT systems.
- Integrate OT risk registers into the agency's overarching enterprise risk management framework to ensure critical infrastructure dependencies are no longer siloed from traditional IT security oversight.
- Ensure coordination between CIOs and those responsible for OT security and resilience.

2

Review existing federal requirements for inclusion in the BOD.

First, CISA should review the requirements in the National Security Agency's BOD 2024-001 to determine what applies to the FCEB. Second, CISA should enforce compliance with previously issued BODs that would apply to OT environments. Third, CISA should require implementation of OMB Memo 24-04 Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements. A 2026 GAO report found that due to poor implementation of OMB's memo and a lack of further guidance, "agencies are left without a clear imperative to prioritize implementation of the requirements or a timeline for doing so." Further, OMB did not oversee implementation of the memo. CISA, through the BOD, could ensure FCEB agencies comply with the OMB memo and oversee its implementation.

3

Align requirements within the BOD to the Cybersecurity Performance Goals (CPGs) and help agencies prioritize implementation of CPGs.

CISA could take a page from BOD 26-04, Prioritizing Security Updates Based on Risk, and develop a process for entities to prioritize CPG implementation. CISA could also create OT specific CPGs, similar to sector-specific CPGs. Though, in lieu of OT specific CPGs, CISA should review previous OT cyber incidents and the causes of disruption and recommend that the FCEB prioritize the following CPGs:

- Manage risks from managed service providers (1.E)
- Manage organizational assets (2.A)
- Obtain independent validation of cybersecurity controls (2.C)
- CPGs focused on Identity Access Management such as Changing Default Passwords (3.A), Establish Minimum Password Strength (3.B), Create Unique Credentials (3.C), Implement MFA (3.F), Monitor unsuccessful (automated) login attempts (3.E), Implement the Principles of Least Privilege (3.H)
- CPGs that would implement CI Fortify principles such as Manage Incident Response Plans (1.C), Implement logical/physical network segmentation (3.I), Maintain System Backups and Restoration Ability (3.O), and Formalize incident planning and preparedness (6.a)

Separate from the BOD, CISA should engage with the national labs and industry advocates on Cyber Informed Engineering (CIE) and incorporate these principles into FCEB OT work. CIE reduces the possibility of catastrophic outcomes by ensuring that no cyber pathway, regardless of access level, can produce physical destruction beyond what the engineered safety envelope permits. This includes engineered safety barriers, mechanical interlocks, analog trip systems, and hardwired limits that software cannot override. CIE ensures that a cyber event stays a cyber event and doesn't become an explosion, a chemical release, or a loss of life. While implementing CIE across the federal civilian OT space is outside the scope and capability of a BOD, it is still critically important to mention in this conversation.

Together, an OT BOD, CI Fortify, and CIE form a defense-in-depth model appropriate for systems that predate and will outlive any single generation of cybersecurity technology.

Acknowledgments: *The OTCC would like to thank Tatyana Bolton, Michael Garcia, Katy Blake Burch-Hudson, and Faith Grant in the development of this report.*



Operational Technology Cybersecurity Coalition

About the OT Cyber Coalition

The Operational Technology Cybersecurity Coalition (OTCC) is dedicated to advancing cohesive, risk-based, and globally interoperable cybersecurity policy for industrial and operational technology environments. OTCC brings together leading experts to advocate for consensus-based standards that reduce regulatory fragmentation and strengthen critical infrastructure resilience worldwide.

www.otcybercoalition.org