THE FEDERAL CYBER ENTERPRISE

The Redwood Project's Plan for a Unified Federal Cyber Defense

Authors

Alex Green
Cristin Goodwin

Contributors

Joshua Brown
John Underwood
Bob Kingery
George Maropakis

The Redwood Project

www.redwoodproject.us

Executive Summary

As cyber threats become increasingly sophisticated and impactful breaches more pervasive, the U.S. Federal Government's current approach for securing its own systems remains fragmented, reactive, and insufficiently agile. Adversaries leverage asymmetrical tactics, without being constrained to the restrictions of time, resources, or regulations that defenders must adhere to, as they exploit legacy systems and target disjointed information architectures. The situation is made even worse for the defenders due to outdated organizational structures, erratic funding cycles, and policy frameworks rooted in assumptions that were never true. This environment hinders the government's ability to protect its own essential information and makes it impossible to take a leadership position in cybersecurity with critical infrastructure owners and operators.

Amid these challenges, The Redwood Project has emerged as a nonprofit initiative to strengthen national cybersecurity by fostering real-time intelligence sharing between the private sector and federal agencies. This collaboration aims to close information gaps, enhance situational awareness, and improve collective defenses against escalating cyber threats. In doing so, it underscores the importance of treating U.S. civilian Federal cybersecurity as a core national priority rather than an afterthought.

Central to The Redwood Project's approach is a call for unified governance of federal cybersecurity, along with stable funding, clear strategies for addressing technical debt, modernized information sharing, and updated legal frameworks. Implemented thoughtfully, these measures can give the US Federal government a realistic chance to fight against major nation-state and criminal actors that are able to repeatedly access government networks and data.

This paper recommends a major change in how the Federal Civilian Executive Branch (FCEB) agencies address cybersecurity. First, the government needs to treat the FCEB space as a single "Federal Enterprise" so that policy, technology, threat hunting and remediation, and incident response are applied consistently across all agencies. The disparities and unique approaches cost taxpayers billions and allow attackers to gain the upper hand. Second, the Federal Enterprise needs a CTO, CIO, and CISO positioned at the highest levels of the organization, while agency-specific roles such as agency technology officers focus on execution rather than strategy. In the business world, these agency roles are often comparable to BTOs, BIOs, or BISOs. Third, the Administration should encourage Congress to modernize IT authorities and budget cycles in longer terms so that planning for threats and needs reflects long-term needs, rather than short term priorities.

Introduction

In 2023, the Federal government allocated $11 billion for cybersecurity to support the Federal Civilian Executive Branch (FCEB) needs.[1] That included increases for the Cybersecurity and Infrastructure Security Agency (CISA), $215 million was allocated to the Department of Treasury – the same agency that was compromised by Chinese threat actors through a supply-chain attack targeting remote security and support company BeyondTrust.[2]

To understand the Federal government's cybersecurity priorities, we have to look historically at the era of desktop computing and when cell phones were large devices used for making phone calls.

Security at the federal level is governed by the Federal Information Security Management Act (FISMA), which came into force in 2002 and updated in 2014 in the Federal Information Security Modernization Act. Companies seeking to provide cloud services to the Federal government need to meet the requirements of the Federal Risk and Authorization Management Program (FedRAMP), released in 2011, and Federal agencies may only procure cloud services from FedRAMP certified providers.

Today, Information Technology (IT) policy and approach is largely driven by the Chief Information Officer (CIO) Council of the Federal government – a body of CIOs from the major agencies from the Federal Civilian and Executive Branch (FCEB) agencies. The CIO Council approach came about in 2014 under the Federal Information Technology Acquisition Reform Act (FITARA), which was the first major overhaul of the Federal government's approach to IT leadership in twenty years.[3]

The CIO Council has tackled many issues since its founding, providing guidance for agencies to implement and a requirement that Federal agencies provide annual reports that provide details on data center use and optimization, performance metrics and a timeline for agency action, and yearly calculations on cost savings and investment that arise out of FITARA implementation.[4] Today, the CIO Council focuses on cybersecurity, technology business management, driving agency adoption of cloud services, recruiting and fostering Federal IT talent, and using data to deliver the Federal CIO mission.[5]

In the decade since the creation of the CIO Council and the release of FITARA and FedRAMP, the world has seen the rise of cloud computing, waves of nation state cyberattacks, criminal actors and ransomware attacks, the growth of the Internet of Things (IOT), and of course, the dawn of Artificial Intelligence (AI) and Machine Learning (ML).

The Federal government is under constant attack from nation state actors. Russian threat actors were successful in attacks against nine agencies during the Solar Winds attack in 2020 – 2021, not including the likely involvement of Chinese, Iranian, and North Korean attackers in attacks that have not been made public.

---

[1] Biden administration's FY 2023 budget includes 11% increase for cyber | Cybersecurity Dive
[2] Five Things To Know On The 'Major' US Treasury Department Hack; letter-to-chairman-brown-and-ranking-member-scott.pdf
[3] Inside the federal law that promotes CIO authority | CIO Dive
[4] 2.1 Federal Information Technology Acquisition Reform Act (2014) | CIO.GOV
[5] Home | CIO.GOV

Key Focuses

Establishing the Federal Enterprise

Today, the Office of Management and Budget (OMB), through the authorities established in the federal laws outlined above and additional government directives, continues to have oversight over the IT approach for the US government. However, agencies have the ability to implement policies and programs for their departments and report findings back to the various OMB channels and processes (CIO Council, Congressionally mandated reporting, etc.) so that there is agency autonomy in implementation.

That Department and Agency autonomy is historical. It arises in part out of the Information Technology Management Reform Act of 1996, which was passed as a part of the National Defense Authorization Act for Fiscal Year 1996, together with the Federal Acquisition Reform Act of 1996. Colloquially, it is known as the Clinger–Cohen Act.[6] It also has roots in FISMA, from 2002. That makes sense. Back then, computing was distributed, the cloud was not yet invented, data centers were operated by governments and companies for their own purposes, and technology couldn't yet support "whole of enterprise" management at the level available today.

Today's computing ecosystem and attack environment requires that the Federal government optimize to meet today's challenges and tomorrow's AI revolution.

The Federal Enterprise

Research from institutions such as Harvard's Belfer Center emphasizes the importance of integrating cybersecurity leadership into core strategic decision-making.[7] The government needs to treat the FCEB space as a single "Federal Enterprise" so that policy, technology, threat hunting and remediation, and incident response are treated consistently across all agencies and departments. The disparities and unique approaches cost taxpayers billions and allow attackers to gain the upper hand.

This new approach is similar to how citizens see their government – when a citizen thinks about the US government, it assumes that it is a government "of the people" and thus that "whole" is the default mindset. We have the technical capabilities today to establish policies and technologies that can be used across the entirety of the Federal enterprise. Those technologies and approaches would have to align with the approach set by the Federal IT Leadership, or they could not be procured and implemented.

Procurement Must Reflect the "Federal Enterprise" Approach

Anyone that has done business with the Federal Government will acknowledge the complexity of the process, the time it takes to complete a deal, and the challenges of working through a massively bureaucratic process. That cannot continue if Federal agencies want to be

[6] 2.2 Clinger Cohen Act (1996) | CIO.GOV
[7] National Cyber Power Index 2020 | Belfer Center

able to implement new technologies or decommission outdated technologies in a meaningful and timely way.

The General Services Administration adds to the complexity of this space, with challenging procurement requirements and processes that are time-consuming and expensive.[8] Fixing the Federal Enterprise will also require streamlining federal procurement into a simple process. Simply put, the process needs to align with how technology products and services are developed, sold, and implemented in the private sector, making them more accessible to the public sector.

Security Across the Federal Enterprise

One of the greatest benefits from the Federal Enterprise approach is the move toward uniform security standards. For instance, consistent identity management solutions ensure robust user authentication across all agencies, while standardized security information and event management (SIEM) tools help consolidate threat intelligence into a single view. Adopting just-in-time access controls further minimizes risk by granting privileges only when needed. These measures allow IT leaders to detect threats and anomalies early, averting major incidents. Executive Order 14028, Improving the Nation's Cybersecurity, set forth terms that would allow CISA to hunt for threats across the Federal enterprise.[9] That right should be preserved and expanded, and any impediments should be removed, so that the Federal government has a skilled team that can hunt across any Department or agency in the FCEB space, regardless of platform, and create reports and share data about the threats, exploits, and attackers that it sees.

116 agencies and hundreds of thousands of devices will provide a treasure trove of data that will give more telemetry to the Federal government than it has ever possessed before and allow it to be less dependent on the private sector for early warning on threats and attacks. In addition, it will allow CISA and the Federal CISO to have data to exchange with critical infrastructure providers with similar data, allowing for a richer "public private partnership" experience and resulting in more effective and actionable guidance to protect the Federal government and the American computing ecosystem.

Misaligned Organizational Structures

The Immediate Need – Whole of Government Leadership

The Office of Management and Budget (OMB) has been at the center of federal information technology since 1996, when Clinger-Cohen required OMB to analyze IT procurement projects and risks and now is a part of the IT budget process.[10] OMB has also had jurisdiction over the CIO function since the enactment of FISMA in 2002. No company in the world still organizes technology under structures from 1996 or 2002.

It is time to revisit whether OMB remains the right authority to oversee the nuances and technology interests of the vast needs of the United States government, and particularly the 116 FCEB agencies outside the military and national security realm.

---

[8] Information technology policy | GSA
[9] Executive Order on Improving the Nation's Cybersecurity | CISA
[10] Clinger-Cohen, at 5.

The Office of the National Cyber Director (ONCD) could serve some of this function, but it has not been as technically oriented as what is being proposed here. Currently, the Office of Management and Budget (OMB) is attempting to manage both the financial oversight and the strategic implementation of federal cybersecurity, creating inefficiencies and misaligned priorities. A more effective approach would be to realign responsibilities: OMB should focus on budgeting and spending oversight, while ONCD should take the lead on cybersecurity strategy, policy, and implementation. Additionally, an independent watchdog entity should be established to audit programs, eliminate waste and fraud, and ensure agencies adhere to cybersecurity directives effectively. To unify this approach, there must be a clear authority within the Executive Office of the President (EOP) that functions as the Technology Office for the federal government, setting policy across the entire Federal enterprise. This structure will provide mission clarity to all agencies and, during times of cybersecurity 'incidents of national significance' as defined in the Cyber Incident Reporting for Critical Infrastructure Act of 2022, will enable the Cybersecurity and Infrastructure Security Agency (CISA) to operate with focused Executive Branch leadership.

Once in place within the EOP, the Federal Enterprise needs a single Office of the CTO, Office of the CIO, and Office of the CISO that set a single policy for the FCEB agencies. Agency leadership roles would be "agency technology officers" etc., (considered "Business Technology Officers or BTOs" in the business world, for example) with the obligation to execute, rather than originate approaches. These agency officers would then work towards a unified technology and security plan, and a unified set of metrics that allow leaders to understand risks and mitigations, deduplicating significant time, effort, and spending compared to the current model.

Preparing for the AI Revolution

One of the things that the Federal government has done better than the private sector has been to create positions of "Chief Data Officers" as mandated by The Foundations for Evidence-Based Policymaking Act of 2018.[11] The Chief Data Officer (CDO) role is present in many agencies and offices across the Federal government, and a Chief Data Officer Council has been in place for several years.[12] This group should be put on steroids to start preparing the USG to take advantage of AI wherever and whenever possible to provide assistance to Federal employees in their job functions, and to be focused on data taxonomies that are consistent across the US federal government.

This last point is particularly important – if left to the agencies, there will be unique taxonomies or approaches that will cost billions, if not trillions, of dollars to unwind over time. The US government needs a single approach to indexing and organizing its unclassified data that is applied across the FCEB domain, and that cannot be done exclusively by those working on AI issues. This is ultimately an issue of organizing the people's data, and it should be done with the Chief Data Officers involved.

This will be an extremely difficult challenge. The amount of data that the Federal government holds is difficult to compute, and so this will be a problem that should also involve

[11] Federal CDO Council - About Chief Data Officers
[12] Federal CDO Council - About Us

private sector partners and working groups to think about, and the National Institute of Standards and Technology (NIST) should be engaged for a leadership role in large data taxonomy standards for the US government. Once standards are in place, the CDOs can execute.

Long-term Planning and Budgeting

The Internal Revenue Service (IRS) is testing a new system to replace its Individual Master File and its Business Master File mainframes from IBM that have been in place for 64 years. The Department of Veterans Affairs Personnel and Accounting Integrated Data (PAID) system, similarly, has relied on the same architectural components for 61 years.[13] These are examples of how systems can get so embedded that short-term budget and planning cycles make it impossible for real work to move forward, when resources are shifted to keep antique cars running on modern highways those systems have no business being on.

As a result, the United States government has a technical debt problem. There are countless egregious examples across the Federal government where employees are forced to use outdated technology and legacy hardware because the budget and planning resources do not exist to allow Departments and agencies to plan for the future – only to plan for the immediate needs of yesterday. That must stop. CIOs, CTOs, and CISOs are expected to stop tomorrow's threats with today's resources, and so they need budget and resource authority that is longer-term than the Federal government's current budget allocation cycle. The lack of budget consistency also leads to a lack of a clear inventory of assets or metrics to gauge technical debt. This makes it harder for technical leaders to prioritize upgrades, measure progress, or justify cybersecurity investments.

A critical gap in Federal IT modernization lies in the lack of a standardized methodology for quantifying technical debt—the accumulated costs and risks of outdated systems. While agencies are aware that legacy infrastructure hinders service delivery and security, many cannot reliably estimate the scope or cost of their obsolescence. For instance, the IRS's Individual Master File has been in place for over six decades, but the true expense of patching versus replacing this mainframe remains elusive. This absence of clear metrics complicates long-term planning and budgeting, undermines cybersecurity justifications, and frustrates efforts to prioritize modernization projects.

A unified framework for calculating technical debt would give agency leaders and policymakers the data they need to make effective investment decisions. It would also enable consistent reporting to oversight bodies like the GAO and OMB, helping to identify the most urgent modernization needs across government. By compelling agencies to quantify legacy system risk and track progress year over year, Federal leadership would be better positioned to fund and implement modernization initiatives that meaningfully reduce technical debt.

Approaches for Strategic Improvement

[13] Here Are 10 of the Oldest IT Systems in the Federal Government | Nextgov/FCW

1. Embrace an Enterprise-Wide View of the Federal Government

NIST's Cybersecurity Framework (https://www.nist.gov/cyberframework) and MITRE's enterprise-level threat hunting strategies emphasize standardization and collaboration. Viewing the government as a single enterprise rather than a collection of isolated agencies can foster consistent baseline security, reduce duplication, and enable system-wide threat analysis.

Recommendations:

- Standardize common architectures, authentication, endpoint protection, and monitoring tools across agencies.
- Deploy centralized threat intelligence platforms to correlate information, reduce detection times, and scale best practices efficiently.

---

2. Realign Authority and Oversight with Strategic Importance

NIST's Cybersecurity Framework and CISA's Zero Trust Maturity Model underscore the necessity of treating cybersecurity as a strategic governance priority rather than an isolated exercise.[14][15] Viewing cybersecurity in this broader context allows agencies to maintain consistent baselines, reduce duplication, and conduct system-wide threat analysis that treat cybersecurity as a fundamental governance principle rather than a compliance checkbox.

Recommendations:

- Rather than categorizing cybersecurity strictly as an isolated budget line, federal agencies should be encouraged to coordinate strategies and align programs across the Federal enterprise for FCEB entities, ensuring it informs and is informed by broader policy strategies.
- Shift cybersecurity decision-making and oversight to a centralized federal authority while placing implementation responsibility within agencies at an operational level. This approach ensures consistency in strategy, policy enforcement, and risk management while allowing agencies to focus on execution without redundant oversight structures.

---

3. Establish Sustainable, Flexible Funding Models

Insights from the Brookings Institution and GAO underscore the importance of stable, predictable funding. Multi-year appropriations or ongoing funding commitments enable continuous modernization, proactive defense measures, and systematic technical debt reduction.

Recommendations:

- Introduce budget models that support multi-year planning and avoid reactive spending surges.
- Use performance-based incentives to encourage agencies to meet benchmarks in modernization and security improvements.

---

[14] NIST Cybersecurity Framework | NIST
[15] Zero Trust Maturity Model | CISA

4. Measure and Prioritize Technical Debt Reduction

Carnegie Mellon's Software Engineering Institute and CISA's SBOM guidance (https://www.cisa.gov/sbom) stress the importance of transparency, metrics, and standardized frameworks in addressing technical debt.

Recommendations:

- Create comprehensive asset inventories and track system health using standardized metrics.
- Prioritize technical debt reduction based on risk scores, ensuring that investments lead to measurable improvements in security posture.

5. Modernize Threat Intelligence Sharing and Control

The Center for Internet Security and various cybersecurity consortia highlight the need for trust and control in information sharing. Ensuring private partners can maintain ORCON status and leveraging AI/ML analysis from efforts like DARPA's advanced R&D (https://www.darpa.mil/) will improve the quality, timeliness, and depth of shared threat intelligence.

Recommendations:

- Allow private entities to set terms for intelligence dissemination, encouraging fuller participation.
- Integrate AI-driven analytics for advanced correlation, anomaly detection, and actionable insights.

- Private entities reporting active nation-state threats should have clearer pathways for engagement with federal agencies. Strengthening two-way communication will help organizations validate threats, assess potential data exposure, and enhance collective defense.

6. Update Legal, Policy, and Regulatory Foundations

The Atlantic Council and World Economic Forum recommend adjusting legal frameworks to handle the asynchronous, global nature of cyber threats. Legal updates should account for emerging technologies (quantum computing, AI-driven attacks) and evolving threat patterns that blend espionage, crime, and sabotage.

Recommendations:

- Craft flexible legal authorities that enable swift responses to complex, rapidly changing threat landscapes.
- Apply tiered approaches to critical infrastructure protection, focusing resources on the most vital systems first.