Booz | Allen | Hamilton®

TRANSFORMING FEDERAL CYBERSECURITY

BLUEPRINT FOR ACHIEVING A
SECURE AND RESILIENT .GOV

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

FEDERAL MISSIONS UNDER SIEGE

Today, the federal government's core missions are in perpetual danger. Across the digital battlefields of cyberspace, threat actors have the upper hand and are pummeling not only .gov departments and agencies, but also the national infrastructure, industry, and the American public.

Adversaries are becoming more creative and audacious with attacks that are increasingly frequent and severe. The SolarWinds and Microsoft Exchange breaches magnified and publicized long-enduring vulnerabilities and deficiencies in .gov networks and systems—security gaps that are only widening as technology advances and digitization accelerates on the back of breakthroughs in 5G, the internet-of-things (IoT), and artificial intelligence.

Meanwhile, these civilian departments and agencies remain shackled by myriad legacy network and infrastructure challenges. Aging information technology (IT) systems are borderline impossible to secure. Commendable, but insufficient, efforts to remediate security gaps have often created patchwork quilts of cybersecurity controls—an explosion of bolted-on point solutions with limited efficacy. Ad hoc coordination and misalignment among federal agencies, including those with cross-government missions and mandates, have returned siloed risk management approaches and cybersecurity controls deployments, difficulty accessing valuable data, and reactive cybersecurity operations.

Compounding this is the rapid and exciting .gov digital modernization agenda. However, security is only sometimes, or partially, top of mind as these initiatives launch and accelerate. All too often, cybersecurity is an afterthought or introduced late in the game.

Faced with such obstacles, federal chief information officers (CIO) and chief information security officers (CISO) are perpetually playing catch-up in a game they cannot win.

Rising Risks

Threat Actor Sophistication

Proliferation and dissemination of increasingly sophisticated **attack mechanisms and vectors**

Technological Advances

Advances in 5G and IoT **exponentially expand the attack surface** to include more networks and devices

Legacy IT Infrastructure

Legacy infrastructure often employs **poor security controls and unpatched systems,** creating vulnerabilities

COVID-19 Changes

Increased digitization due to **COVID-19 pushed more work to online platforms**, opening new doors for exploitation

Ransomware

Growth in volume and severity of attacks in addition to increased **targeting of critical infrastructure**

Data Exfiltration

Successful data exfiltration by attackers potentially fuels **damage, destruction, or further attacks on additional targets**

Disinformation

Growing AI capabilities increases disinformation threats as deep fakes and similar tools gain widespread use

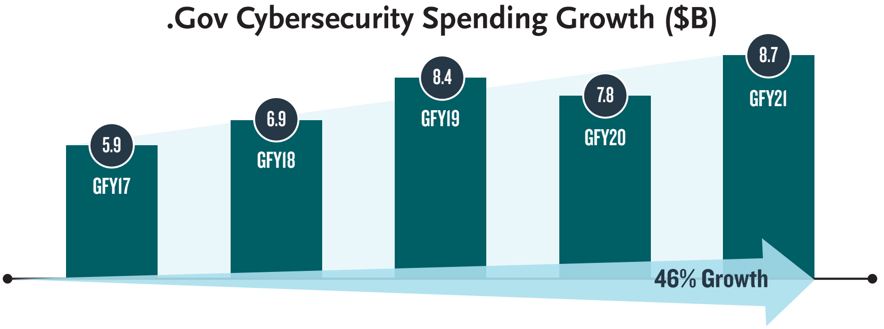
Unauthorized Access

Access by advanced persistent threats (APT) poses **risks from malware deployment to system destruction**

Escalating Attacks

DESPITE SPENDING GROWTH, CHALLENGES REMAIN UNRESOLVED

In search of solutions, the government continues to spend. Federal cybersecurity spending has raced higher year-over-year; indeed, cybersecurity spending across .gov increased 46 percent since 2017.[1]



While this spending growth is necessary and has improved relative cybersecurity maturity across .gov, the gains are a finger in the wall of a bursting dam. In many cases, persistent major gaps in the government's digital defenses remain unresolved. Notably, a March 2021 Government Accountability Office report flagged hundreds of recommendations (dating back to 2010) that remained unaddressed,[2] while an August 2021 Senate Committee on Homeland Security and Governmental Affairs report assigned near-failing cybersecurity grades to seven of eight evaluated federal agencies.[3]

[1] Spending identified from Presidential Budget Requests per the requirement in Section 630 of the Consolidated Appropriations Act, 2017 (P.L. 115–31), which amended 31 U.S.C. § 1105 (a)(35). Spending reflects figures collected by OMB from .gov agencies' CFOs, CIOs, and CISOs. It includes funding for agency protection of information systems as well as broader cybersecurity missions and spending related to standards, research, and the investigation of cybercrimes. All figures reflect actual budgetary resources available except for GFY21, which reflects estimated budgetary resources available.

[2] United States Government Accountability Office (2021), Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges. https://www.gao.gov/assets/gao-21-288.pdf

[3] United States Senate, Committee on Homeland Security and Governmental Affairs (2021), Federal Cybersecurity: America's Data Still At Risk. https://www.hsgac.senate.gov/imo/media/doc/Federal%20Cybersecurity%20-%20America's%20Data%20Still%20at%20Risk%20(FINAL).pdf

GAO Report (Mar. 2021): *Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*

Report Overview	**750 recommendations** aligned to four cybersecurity challenges identified by the GAO since 2010 were not implemented as of December 2020, including **67 of 103 priority recommendations**

	CHALLENGE	STATUS	
1	**Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight**	**59%** of recommendations implemented	**22%** of priority recommendations implemented
2	**Securing Federal Systems and Information**	**75%** of recommendations implemented	**34%** of priority recommendations implemented
3	**Protecting Cyber Critical Infrastructure**	**38%** of recommendations implemented	**18%** of priority recommendations implemented
4	**Protecting Privacy and Sensitive Data**	**54%** of recommendations implemented	**75%** of priority recommendations implemented

Senate Committee Report (Aug. 2021): *Federal Cybersecurity: America's Data Still at Risk*

Report Overview	Two years after a previous report analyzed systemic failures in eight key federal agencies' compliance with federal cybersecurity standards, a follow-up report found the **same issues remained**, and **seven agencies had not met basic cybersecurity standards**

SELECT REPORT FINDINGS

- ✗ Seven of eight agencies used legacy systems and/or **applications no longer supported** by the vendor with security updates
- ✗ Seven of eight agencies **failed to maintain** accurate and comprehensive IT asset inventories
- ✗ Seven of eight agencies **failed to adequately protect PII**
- ✗ Six of eight agencies operated systems **without current authorizations** to operate
- ✗ Six of eight agencies **failed to install security patches** and other vulnerability remediations quickly

Several agencies made only **minimal improvements** in one or more key areas, with multiple failures **persisting for the past 10 years**

More spending for more incremental gains is not the answer. Instead, a wholesale revolution in how .gov agencies approach and execute cybersecurity is needed.

OVERHAULING FEDERAL CYBER: SETTING A NEW "NORTH STAR"

Sweeping statements on the need to modernize cybersecurity are all too common. More elusive, however, is a way to fundamentally rethink and reboot federal cybersecurity around a concrete, structured vision for greater security and resilience at the national level. In addition, to achieve improvements at scale, .gov cyber leaders at agencies ranging from the Cybersecurity and Infrastructure Security Agency (CISA) to small civilian agencies must be empowered to track and demonstrate progress on the path to cybersecurity transformation.

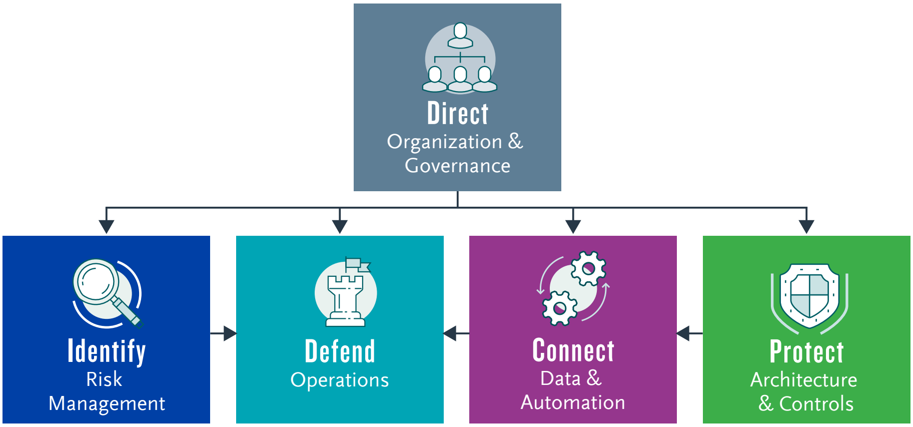
This journey starts with a unified, singular framework encapsulating comprehensive, good federal cybersecurity. Leveraging commercial, government, and international best practices (alongside lessons learned from today's federal cybersecurity shortcomings), this framework provides a guiding "North Star" and a tangible roadmap for navigating challenges and achieving a *secure and resilient .gov*.

Federal Cybersecurity Framework: *Overview*

ELEMENT	DEFINITION
Direct Organization & Governance	Operational authorities, decision-making, and personnel for the ecosystem
Identify Risk Management	Identification and management of risk across the ecosystem
Defend Operations	Cyber defense operations to combat cyber threats across the ecosystem
Connect Data & Automation	Data and information to see a holistic view of the ecosystem
Protect Architecture & Controls	Controls and tools to harden the ecosystem

Good federal cybersecurity for the .gov ecosystem must address the framework's five central elements: Direct, Identify, Defend, Connect, and Protect. Although the elements are discrete definitionally, they are relationally intertwined, driven by the Direct element with all elements ultimately working to facilitate Defend—the framework's heart and core of good cybersecurity.

Federal Cybersecurity Framework: *Element Relationships*



Integrated, these elements are greater than the sum of their parts, but each helps federal cyber leaders break down and tackle cyber transformation without losing sight of the complete picture. Importantly, good cybersecurity requires a balance of effort and effectiveness across the elements. Like the proverbial weak link in a chain, deficiencies in any one element can cause the entire ecosystem to underperform (or worse, break).

This framework provides key features and benefits, including:

- **Multi-Level Applicability:** The framework and its elements are equally relevant at the federal level (i.e., cybersecurity across .gov) and at the agency level (i.e., each entity's cybersecurity program).
- **Additive to Common Frameworks:** The framework includes the functions and families present in NIST's cybersecurity framework (and others). However, it introduces vital additions encompassing the management of cybersecurity and the importance of data and analytics—the connective tissue of cutting-edge cybersecurity programs.
- **Cyber Transformation Aid:** The framework provides CIOs, CISOs, and other cyber-focused leaders with a uniform way to plan, execute, manage, and measure specific cybersecurity transformation efforts at departments and agencies and in aggregate across .gov.

A BLUEPRINT FOR FEDERAL CYBERSECURITY

As transformation-minded federal cyber leaders orient around the framework, it is vital to understand the strategic paradigm shifts needed in each element at each layer of the framework. These shifts crystalize what good .gov cybersecurity looks like and provide an actionable path forward for a federal cyber reboot. They include:

Direct

Accelerating the positioning of the Department of Homeland Security (DHS) CISA as the director and orchestrator of federal cybersecurity. Fundamentally, CISA's job must focus on eliminating complexity: simplifying and clarifying federal cyber policies, establishing single standards and reporting requirements for .gov agencies, and working with the Office of Management and Budget to centralize cybersecurity budgeting, planning, and program execution across .gov.

Identify

Embracing threat-centric risk management across the entirety of ever-morphing digital ecosystems. In today's software-everything, cloud-centric, and remote-work world, the classic enterprise boundary is gone. The focus cannot be compliance-based checklists, but rather threat-centric risk management with modeling, emulation, and testing to understand how real adversaries might attack via weak links in supply chains.

Defend

Moving from reactive threat detection and incident response to proactive cyber defense operations, especially persistent threat hunt. This is aggressive defense: seeking to identify and disrupt threats before they cause damage, raising the costs of conducting attacks, and automating threat and vulnerability management to identify adversary behaviors and eliminate weak points in time.

Connect

Recognizing that data (and the ability to operationalize it faster than adversaries) is imperative for effective cybersecurity. Federal-wide cyber programs and agencies must vastly improve how they harness, normalize, analyze, and exploit data to inform cyber defense operations. Speed, precision, and accuracy matter. Data fuels it all.

Protect

Breaking free of tools and realizing that cutting-edge technology is no panacea. The security tool era has peaked, and layering ever-more-protective products is increasingly ineffective and redundant. The emphasis must shift to architecting more defensible, resilient networks (rooted in .gov-wide baselines and best practices) via zero trust principles.

Together, these paradigm shifts help bring to life the vision state for .gov cybersecurity, rooted in the overarching need for CISA to play an expanded, central role in .gov cybersecurity. That vision state is encapsulated below in a series of central questions and answers:

Federal Cybersecurity Framework: *Vision State Overview*

ELEMENT	VISION STATE QUESTION	VISION STATE ANSWER
Direct Organization & Governance	How do you bring together agencies to fully leverage the .gov ecosystem?	Integrated authorities where CISA defines needs based on priorities while agencies execute their budgets and hiring of personnel based on priorities
Identify Risk Management	How do you identify and manage risk across the .gov ecosystem?	CISA issues strategies, policies, and standards for identifying and managing risk based on national and federal priorities
Defend Operations	How do you facilitate dynamic cyber defense across the .gov ecosystem?	CISA coordinates cyber defense operations with larger agencies and SOCs while providing SOC-as-a-Service for smaller agencies
Connect Data & Automation	How do you ensure a comprehensive view of the .gov ecosystem?	CISA fully operationalizes data from agencies and federal sensors to provide intelligence for proactive cyber defense operations
Protect Architecture & Controls	How do you harden the digital .gov ecosystem?	CISA designs and defines architectures, security tools, and security controls based on national and federal priorities for the .gov environment

MOVING TOWARDS A SECURE AND RESILIENT FUTURE

Beyond the paradigm shifts tied to the federal cybersecurity framework, practical steps can accelerate transformation to a *secure and resilient .gov*. Here are several such steps:

Direct

Simplify and streamline policies, standards, and budgeting—and stop fighting the cyber talent war.

- **Simplify the myriad cyber policies, standards, and regulations across .gov**. CISA should be the single driver of federal-wide policy, strategy, and planning—establishing non-negotiable rules of the road and best practices for standardized agency-level cybersecurity.
- **Streamline federal cybersecurity budgeting through CISA** to facilitate review and recommendation for budget priorities and deconfliction of proposed spending across civilian departments and agencies.
- **Embrace shared services, delivered "as-a-service" in a one-to-many business model**. CISA can leverage the government's purchasing power to drive down costs while reaping the benefits of standardized and predictable control and capability deployments across disparate entities.
- **Recognize that the "war for cyber talent" is fundamentally unwinnable**. Use shared services as a release valve for workforce pressures. Shared and managed services should enable cyber professionals to focus on complex and challenging cyber problems.

Identify

Move to ecosystem-wide and threat-driven risk identification and prioritization.

- **Create a common baseline methodology for .gov-wide threat and countermeasure modeling**. CISA should develop and deploy this methodology in addition to providing .gov entities with resources and tools for application across internal agency ecosystems.

- **Establish federal-wide dashboards at CISA that aggregate and prioritize mitigation-specific, real-world threat scenarios facing .gov**. These dashboards should be rooted in the standardized threat and countermeasure modeling conducted at individual departments and agencies.

- **Rewrite standards to drive agency-level risk management programs away from compliance** (implementing controls to specified maturity levels) and toward threats (implementing controls that directly address weaknesses in the kill chain).

- **Extend the role of asset management programs to encompass the ecosystem beyond enterprise IT walls**: software supply chains, cloud and edge, and IoT-enabled products and devices. Through CISA, require software vendors serving .gov to show their software bill of materials to accelerate illumination of opaque supply chains.

Defend

Invest in preventative and proactive cyber operations.

- **Prioritize investments in threat and vulnerability management** that seek to reveal adversary behaviors and patterns, match them to exploitable vulnerabilities, and close those vulnerabilities before adversaries attack.

- **Expand CISA's resources to conduct persistent hunt across .gov and provide threat hunting as a shared (and managed) service**—grounded in adversary insights and tradecraft gleaned from sensitive cyber missions conducted by Intelligence Community and military entities—to federal departments and agencies.

- **Drive adoption of purple teaming platforms and practices at the agency level** that enable integration of attacker and defender insights and tradecraft and continually stress-test defenses against adversary patterns and behaviors.

Connect

Extract, normalize, and operationalize data.

- **Accelerate deployment of standard-configuration endpoint detection and response tools across .gov** to enable federal-wide access to (and visibility over) crucial cyber data. This data is imperative for proactive threat hunting across .gov.
- **Implement a federal-wide data analytics pipeline to increase the speed and quality of data normalization**, which in turn, improves the speed and quality of cyber defense operations.
- **Share agency-level data across .gov entities** (anonymized, if needed). A data analytics pipeline can enable sharing of distributed data and event-based analysis, helping CISA establish a self-updating common operating picture of threats.

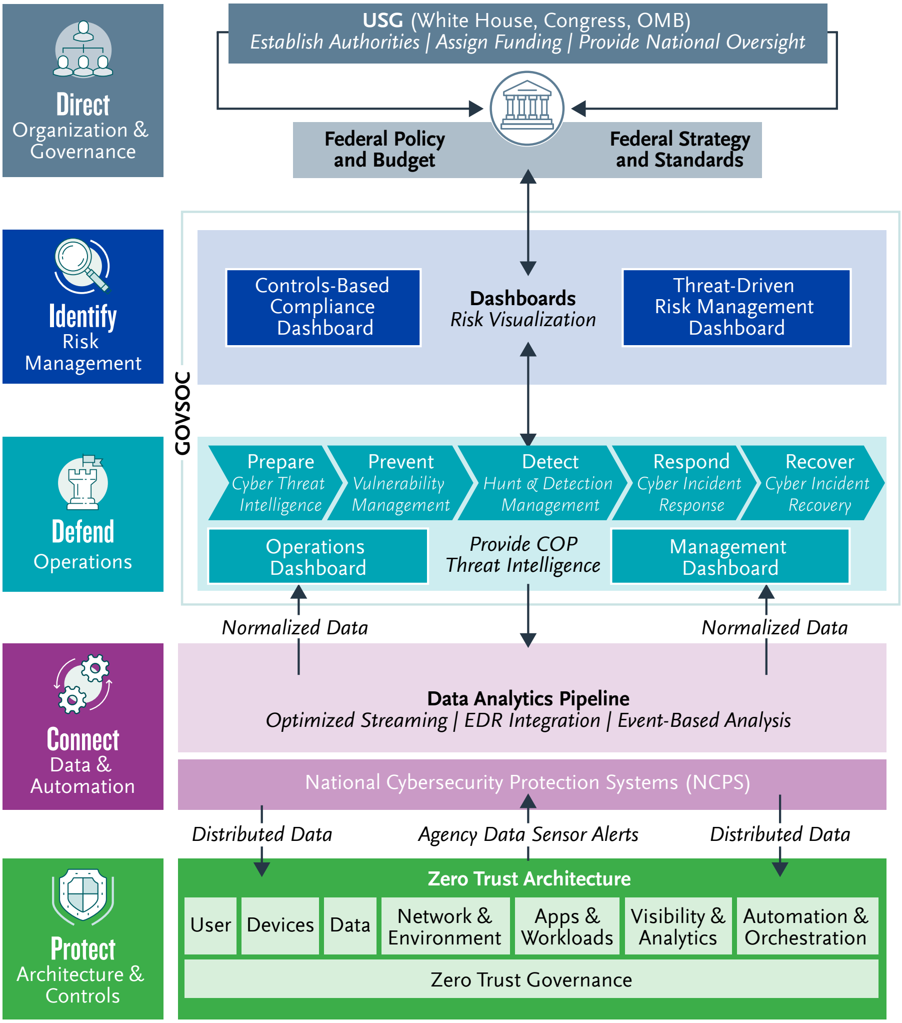
Protect

Adopt zero-trust paradigms and architectures that are brought to life via shared and managed services.

- **Create and distribute zero trust accelerators via CISA to agencies**: diagnostics, templates, blueprints, and architectures that help agencies progress toward a zero trust-based security program. While every environment is different, CISA can provide a core toolkit with broadly applicability across .gov.
- **Design and deploy commoditized, shared services** (especially for core protective controls) across departments and agencies to gain efficiency of scale, consistency of performance, and visibility into results.
- **Shift away from siloed agency tool buying and focus on automating and orchestrating existing controls, technologies, and security products**. Develop a clear security product roadmap specifying how to optimize and integrate existing tools, engage CISA for access to shared services, and procure in a uniform manner.

Together, these actions coalesce into a unified vision state view for federal cybersecurity, with discrete transformations in each framework element integrated into a new picture for federal cybersecurity.

Architecture for a *Secure and Resilient .Gov*



Even at this point, the federal cybersecurity reboot will not end. Ongoing strategic challenges remain, such as moving beyond information sharing to deep collaboration and integration between industry and government or determining how to leverage the cyber adversary insights generated by forward-focused intelligence and military operators. However, the journey toward fundamentally better .gov cybersecurity will be well underway.

About Booz Allen

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by its most sensitive agencies. We work shoulder-to-shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision. With global headquarters in McLean, Virginia, our firm employs nearly 27,700 people globally, and had revenue of $7.9 billion for the 12 months ended March 31, 2021. To learn more, visit BoozAllen.com. (NYSE: BAH)

BoozAllen.com/cyber