

Booz | Allen | Hamilton®

VISION FOR A SECURE AND RESILIENT .GOV

[CLICK TO ENTER](#)

FOREWORD

Booz Allen’s core mission is focused on supporting and facilitating successful outcomes for the United States government. As a trusted partner to agencies across the civil, defense, and intelligence domains, Booz Allen works shoulder-to-shoulder with clients to secure, protect, and enable their most critical missions. Central to this work, the firm—as the nation’s largest cybersecurity services provider—is defending against the toughest cyber adversaries and anticipating over-the-horizon threats.

Today, there is an urgent need to rethink federal cybersecurity to support critical missions, U.S. national security, and the country’s economic prosperity.

Given this imperative and the central role of the U.S. government in shepherding the nation’s cybersecurity, this report puts forward a detailed vision for how the federal government can comprehensively transform its cybersecurity ecosystem. This vision is encapsulated in a broad framework and detailed roadmap that facilitates a wholesale rethinking of federal cybersecurity today to ensure its networks, information, infrastructure, and people are safe tomorrow.

The following pages provide a detailed analysis of the federal cybersecurity ecosystem today and its associated challenges. Working from this current state, this report constructs a comprehensive blueprint—leveraging an overarching Federal Cybersecurity Framework—that creates a foundation for a transformed federal cybersecurity ecosystem. This blueprint includes tangible, implementable actions for federal agencies—led by the Cybersecurity and Infrastructure Security Agency (CISA)—to execute on the road to realizing a *secure and resilient .gov*.

The vision articulated in the subsequent pages can help the federal government make immediate, effective progress in modernizing and protecting the federal cybersecurity ecosystem, while simultaneously enabling the conversations, planning, and long-term actions needed to secure the future.

INTRODUCTION

1 UNDERSTANDING THE JOURNEY

Historical federal government policies, actions, and spending—plus developments under the Biden administration

2 IDENTIFYING THE CHALLENGES

Key, persistent obstacles—from cyber attacks to human capital—threatening and obstructing federal cybersecurity progress

3 CREATING A NEW BLUEPRINT

Methodology and framework design process to understand the current state and establish a defensible foundation for transformation

4 SECURING .GOV

New federal cybersecurity architecture and solutions roadmap—based on the framework—to create a *secure and resilient .gov*

A SECURE .GOV AND BEYOND

FEDERAL MISSIONS ARE UNDER SIEGE

Today, the government's core missions are in perpetual danger.

Sophisticated cyber threat actors have gained 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 while cyber attacks grow more frequent and increasingly severe.

In parallel, long-enduring vulnerabilities and deficiencies present in .gov networks often remain unresolved, compounding gaps and attack damages—highlighting the uphill battle required to remediate problems and advance the federal cybersecurity posture.

While improvement efforts across the .gov environment are commendable, they have often created patchwork quilts of cybersecurity standards and controls in addition to promulgating an explosion of bolted-on security tools, with mixed results at best.

Faced with legacy, aging infrastructure and these environmental obstacles, federal chief information officers (CIO) and chief information security officers (CISO) are perpetually playing catch-up in a game they cannot possibly 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

Escalating Attacks

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**

A SINGULAR FRAMEWORK, ENCAPSULATING “GOOD” FEDERAL CYBERSECURITY, CAN GUIDE THE .GOV CYBERSECURITY REBOOT



There is an urgent need for a complete reboot of federal cybersecurity centered around a concrete, structured picture for security and resilience at the national level.

The starting point for this journey is 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—the Federal Cybersecurity Framework provides a guiding “North Star” by which .gov can navigate in addition to serving as an anchor point for the development of a tangible roadmap for achieving a secure and resilient .gov.

Good federal cybersecurity for the .gov ecosystem addresses the framework’s five core 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.

Integrated, these elements are greater than the sum of their parts; however, each helps federal cyber leaders break down and tackle cyber transformation without losing sight of the complete picture.

CISA IS THE LYNCHPIN FOR FEDERAL CYBERSECURITY TRANSFORMATION AND ULTIMATE ENABLER OF ITS SUCCESS

The framework, across its elements and attributes, provides a blueprint for federal cybersecurity—oriented around the Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

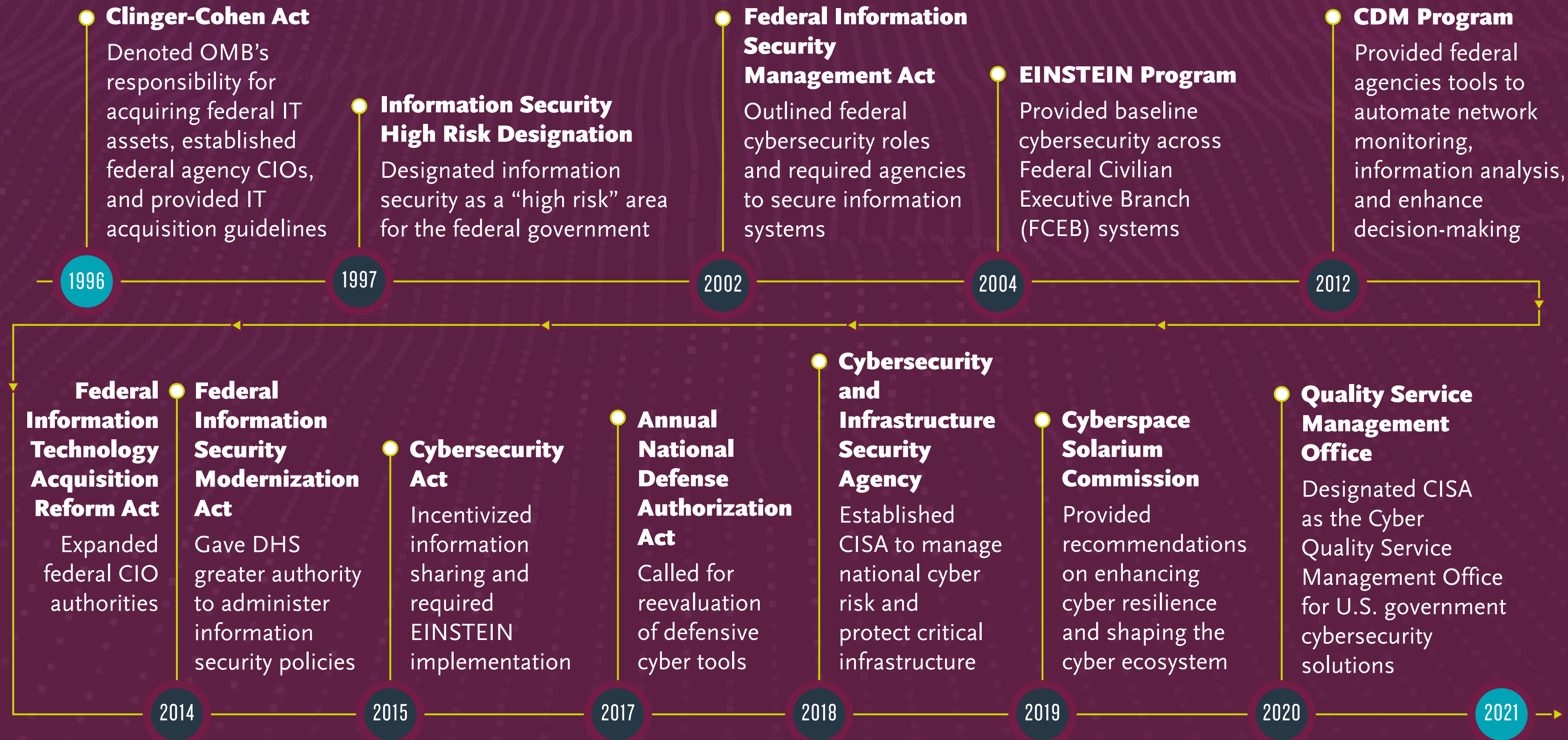
Adoption and implementation of the framework requires codifying—and empowering CISA’s centralized authorities as the director and orchestrator of .gov cybersecurity, enabling CISA to create standards and policies to prioritize and manage cyber risk, coordinating federal-wide cyber defense operations through CISA or via centralized SOC-as-a-Service, allowing CISA to operationalize data and intelligence from agency-deployed sensors, and designing and deploying architectures and security controls for the federal environment through CISA.

ULTIMATELY, CISA IS THE KEY TO SUCCESSFUL FEDERAL CYBERSECURITY TRANSFORMATION AND THE AGENCY LIES AT THE HEART OF THE VISION STATE ARCHITECTURE FOR A SECURE AND RESILIENT .GOV.

Although the framework and recommendations contained in the following pages will not singularly complete the federal cybersecurity transformation, they represent an actionable and achievable roadmap that will fundamentally improve .gov cybersecurity.

UNDERSTANDING THE JOURNEY 1

THE U.S. GOVERNMENT HAS BEEN ON A 25+ YEAR JOURNEY TO IMPROVE FEDERAL CYBERSECURITY



.GOV CYBERSECURITY SPENDING IS ON THE RISE

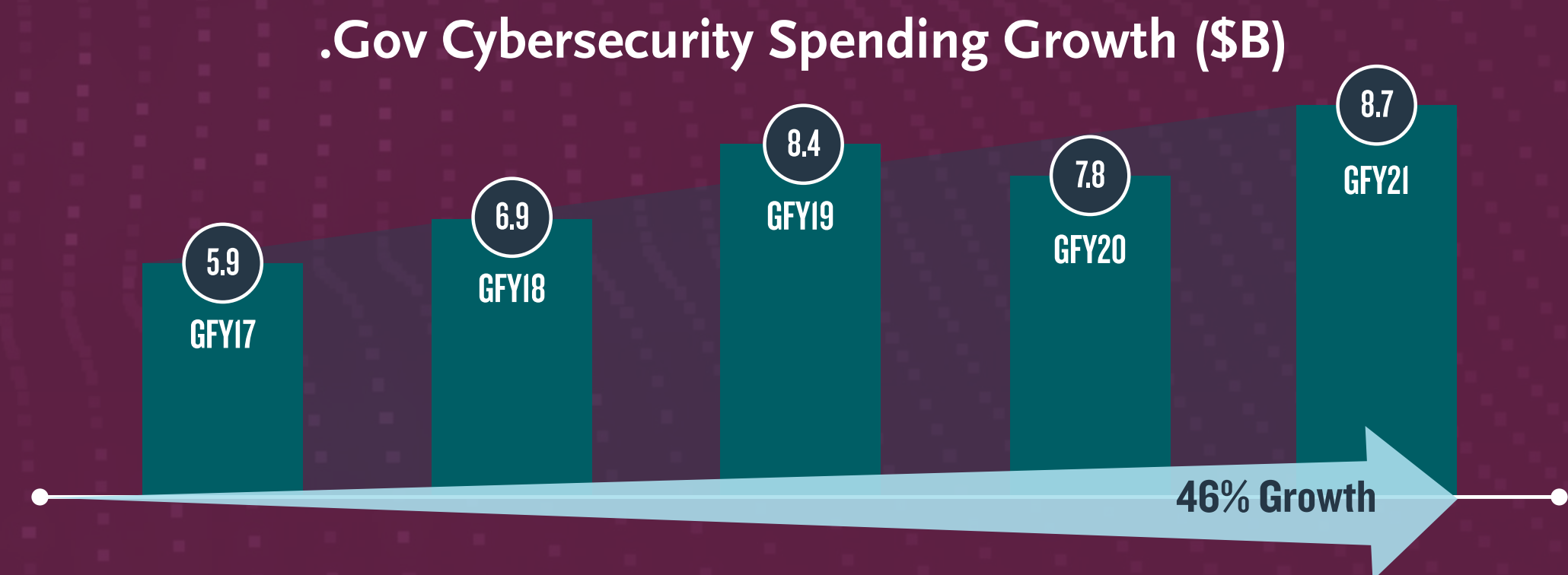
Over the last five years, .gov has received a nearly 50% increase in cybersecurity budget. These increases have come as part of efforts to close the gap between Department of Defense (DoD) and civilian agency cybersecurity maturity, respond to major gaps in federal cybersecurity, and strengthen the resilience of .gov systems and networks in the face of ever-more capable cyber attackers.

GFY'22 PBR REQUESTED \$9.8B | 14% INCREASE
IN DEDICATED CYBER SPENDING | FROM GFY'21¹



The 2022 Presidential Budget Request supports critical cybersecurity goals across the .gov ecosystem including providing funding for federal agencies as they modernize, strengthen, and secure antiquated information systems; enhancing federal cybersecurity by securing federal networks; protecting critical infrastructure; sharing best practices with public and private partners, and cultivating a sustainable pipeline of employees to build, maintain, and secure federal information systems.

FEDERAL CYBERSECURITY SPENDING HAS INCREASED YEAR-OVER-YEAR RISING 46% IN THE LAST FIVE YEARS ALONE



* (per Sec. 630 of the Consolidated Appropriations Act, 2017). Figures collected by OMB from .gov agencies. Includes funding for agency protection of information systems; cybersecurity missions; and spending related to standards, research, and investigation of cybercrimes.

THE BIDEN ADMINISTRATION IS ACCELERATING FEDERAL—AND BROADER NATIONAL—CYBERSECURITY EFFORTS

The appointment of the first National Cyber Director, a critical Solarium Commission recommendation enacted in the 2021 NDAA, facilitates the promotion of centralization and oversight for siloed cyber policies, organizations, and resources across the national cybersecurity ecosystem.²

Additionally, the May 2021 Executive Order on Improving the Nation’s Cybersecurity and July 2021 National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems enables improvement in the standardization of cybersecurity practices across .gov and industry, as well as supports information sharing efforts.³ Zero Trust, supply chain security, and proactive, preventative cyber defense operations are top-of-mind priorities.

These statements of policy and guidance underscore the Biden Administration’s focus on shoring up federal cybersecurity—and fostering long-term resilience across the nation’s critical infrastructure, whether operated by the public or private sector.

The Biden Administration has followed through with its promise to elevate the status of cyber issues through executive and legislative action enhancing, centralizing, and standardizing cybersecurity controls and practices for .gov agencies.

“WE’VE ELEVATED THE STATUS OF CYBER ISSUES WITHIN OUR GOVERNMENT” – PRESIDENT BIDEN

2 IDENTIFYING THE CHALLENGES

FEDERAL DEPARTMENTS AND AGENCIES FACE FOUR PERSISTENT, GROWING CYBER CHALLENGES



1. More Capable Cyber Threat Actors + Growing Cyber Attack Severity

- Vast expansion in adversary capabilities—from hostile nation-states to state-sponsored hacker organizations to global cybercrime syndicates, increasing the severity of cyber attacks
- Sophisticated tactics, techniques, and procedures; malware and ransomware-as-a-service; and the rise of mis- and dis-information mean bad actors constantly outpace defenders
- Many adversaries do not fear the consequences of reprisals; deterrence appears limited



2. Proliferation of Emerging Technologies and Connected Devices

- Emerging technologies (e.g., IoT, 5G) are exponentially increasing connected devices and—by extension—the volume of data
- Pandemic-driven digitization and remote work have created hard-to-map attack surfaces with vulnerable entry points



3. Scarcity of Cyber Talent

- The federal government faces a near-unwinnable battle for cyber talent—it is extremely hard to compete with the private sector's compensation packages and flexibility
- Burdensome, intrusive hiring processes can deter mission-motivated cyber professionals from pursuing government jobs



4. Burden of Legacy Networks and Infrastructure

- Patchwork cloud environment and legacy IT infrastructure means copious vulnerabilities in agency-level systems and networks
- Security is too often an afterthought in federal digital modernization efforts

KEY UNDERLYING DRIVERS ARE FACILITATING CONTINUED WORSENING OF THE CYBER THREAT ENVIRONMENT



Adversaries

More Nation-State Cyber Incidents

Nation state-backed cyber incidents doubled from 2017-2020, leveraging hardware backdoors, targeted malware, and remote access trojans, to target .gov agencies. Russia and China are expected to increase cyber spending dramatically in the coming years, with a 25% increase in China and an up to 200% increase in Russia by 2023.⁴

More Capable Cyber Criminals

Cyber criminals often recycle nation-state exploits to access systems and data. The lines between nation-state and non-state cyber criminals are often blurred, as nation-states leverage proxies to conduct criminal activities that ultimately meets that nation state's goals.⁵

Severity

New, Novel Adversary Capabilities

Threat actors are continuously evolving their tactics, techniques, and procedures to stay ahead of defenders. And like defenders, the bad guys share information and insights, too. Compounding this, the availability of Ransomware as a Service, or COTS-style ransomware, and malware gives threat actors multiple ways to target defenders.⁶ Ransomware attacks, in particular, continue to grow, with a 62% increase in ransomware attacks globally since 2019 and a 158 percent spike in North America alone.⁷

Growing Cyber Attack Severity

The severity of cyber attacks has grown in recent years, with attacks leading to major data, record, and financial losses across government and commercial entities. Attacks such as the SolarWinds attack and the Microsoft Exchange breach exploited vulnerabilities to hack several .gov and private sector entities.

Records Lost to Breaches (millions)⁸



THE EXPANSION OF EMERGING TECHNOLOGIES EXACERBATES THE IMPACT OF THESE THREATS



Rollout of 5G Connectivity

With up to 20-times the capacity of 4G, 5G can support many more simultaneous connections at faster speeds. However, the transition to 5G also leaves infrastructure more vulnerable. For example, an overlay of 4G legacy and 5G architecture can allow hackers to leverage 5G infrastructure to exploit 4G vulnerabilities.⁹

Increasing IoT Device Usage

Between 67 and 75 billion IoT devices are expected to be online by 2025.¹⁰ Many IoT devices ship with default, rarely-changed passwords, leading to more insecure devices on a network, growing the attack surface, and increasing the types of devices necessary to manage and protect.

Pandemic-Driven Attack Surface Expansion

More information, business functions, and connected devices shifted to virtualized environments, some with questionable security and resiliency. Accordingly, adversaries also shifted their tactics as COVID-related spear-phishing attacks rose more than 677% in 2020.¹¹

SCARCE HUMAN CAPITAL HAS HINDERED FEDERAL CYBER DEFENSE CAPABILITIES



Insufficient Pipeline of New Cyber Talent

The federal cyber work force has grown by around 8% since 2016—including nearly 300 cyber hires by DHS between May and July 2021. There is a shortage of nearly 36,000 cyber jobs across federal, state, and local governments.

Shrinking Federal Cyber Workforce

There are 16 times more federal IT workers older than 50 than there are younger than 30, part of a larger trend of the federal government's age imbalance as the workforce continues to shrink while needs increase.¹²

Hard to Compete with the Private Sector

1. Private sector compensation can be two to five times higher than government
2. Private sector typically offers greater flexibility and mobility for employees
3. Burdensome and intrusive hiring practices may deter qualified cyber candidates—even those motivated to serve the nation

OUTDATED FEDERAL NETWORKS AND INFRASTRUCTURE—AND RAPID DIGITAL MODERNIZATION—IS EXACERBATING CYBER GAPS



Hard-to Secure Legacy Systems

The .gov IT backbone is a complex patchwork of systems—many of which are aging—created well before cybersecurity was at the fore. This legacy technology is hard to secure, if not outright insecurable. Compounding this, the rise of cloud and hybrid cloud environments creates new seams and gaps that attackers can exploit and pivot from.

Modernization Outpacing Security

Federal agencies have embarked on ambitious digital and IT modernization efforts. These are badly-needed, but often do not “bake in” cybersecurity from the beginning. This can result in a rush to bolt-on security solutions late in the modernization game or, worse, provide new avenues of attack for adversaries.

THE TAKEAWAY? IT IS TIME TO TRANSFORM FEDERAL CYBERSECURITY

Against this backdrop, several things are clear:

- Federal CIOs and CISOs are trapped in an unwinnable arms race—spending more but never quite getting ahead of ever-more capable cyber adversaries
- Piecemeal, point solutions to .gov cyber gaps will not cut it. Cybersecurity is a systems problem that requires systems-level solutions
- It is time to fundamentally re-think what the federal ecosystem cybersecurity should look like

The starting point for this journey begins 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—a framework that provides a guiding “North Star” by which .gov can navigate in addition to a tangible roadmap for achieving a *secure and resilient .gov*

3 CREATING A NEW BLUEPRINT

A CLEAR FRAMEWORK AND “TO-BE” SCENARIOS ANCHOR THE NEW FEDERAL CYBERSECURITY BLUEPRINT

Design Federal Cybersecurity Framework— providing a “North Star” for .gov cybersecurity

- A** Define the core components of good federal cybersecurity
- B** Identify the integral features and capabilities within each framework element
- C** Assess the major strategic and operational weaknesses of today, based on the framework

Develop vision state scenarios and features—formulating a blueprint for a *secure and resilient .gov*

- A** Develop a spectrum of options for the future of .gov cybersecurity at each layer of the Federal Cybersecurity Framework
- B** Identify the key characteristics for good federal cybersecurity based on preferred options
- C** Create vision state for .gov cybersecurity—the destination at the end of the transformation roadmap

THE FEDERAL CYBERSECURITY FRAMEWORK DEPICTS THE CORE ELEMENTS AND ATTRIBUTES OF GOOD .GOV CYBERSECURITY

A

Develop Core Framework Elements

Define the core components of good federal cybersecurity

- Covers key pieces of cybersecurity programs
- Provides the basis for reviewing and improving the current federal cybersecurity ecosystem

B

Identify Supporting Framework Features and Capabilities

Identify the integral features and capabilities within each framework element

- Illuminates the organizational, technological, and resource needs for federal cybersecurity
- Further details the federal cybersecurity environment

C

Review the Current Federal Cybersecurity Situation

Assess the major strategic and operational weaknesses of today, based on the framework

- Maps identified gaps against the framework's attributes
- Offers a clear picture of today's challenges and shortcomings to begin conceptualizing improvements





















THE FEDERAL CYBERSECURITY FRAMEWORK DEFINES AND ORGANIZES THE FIVE MAJOR ELEMENTS OF FEDERAL CYBERSECURITY



The Framework's elements are driven by the Direct element, with each working towards the Defend Element—the framework's heart



EACH FRAMEWORK ELEMENT DECOMPOSES INTO CORE FEATURES OR CAPABILITIES COVERING THE ELEMENT'S ACTIONS AND ACTIVITIES

		FEATURES AND CAPABILITIES					
	Direct Organization & Governance	 Budget <i>Funding needs and allocation mechanisms</i>	 Authority <i>Decision-making and oversight functions</i>	 Talent <i>Personnel, staffing, and hiring needs</i>			
	Identify Risk Management	 Identify Risks <i>Policies and strategies for standards and configurations</i>	 Prioritize Actions <i>Threat-driven actions to mitigate vulnerabilities</i>	 Direct Mitigations <i>Guidance and mandated compliance to mitigate vulnerabilities</i>			
	Defend Operations	 Prepare <i>Threat intelligence and vulnerability monitoring</i>	 Detect <i>Proactive threat hunting</i>	 Respond/Recover <i>Incident response (IR), forensics, and recovery activities</i>			
	Connect Data & Automation	 Extract <i>Data collection and ingest</i>	 Normalize <i>Data standardization for proactive threat hunting across networks</i>	 Distribute <i>Data enrichment activities</i>			
	Protect Architecture & Controls	 Design <i>Development of specific security controls, architectures, and tools</i>	 Deploy <i>Dissemination of controls, architecture, and tools—including guidance</i>	 Manage <i>Continuous update of controls, architecture designs, and security tools</i>			

TODAY, THE FEDERAL CYBERSECURITY ECOSYSTEM FACES A RANGE OF GAPS AND SHORTCOMINGS




		GAPS AND CHALLENGES					
	Direct Organization & Governance	 Ad Hoc Budget <i>Ad hoc agency budgets that are siloed across the ecosystem</i>	 Limited Authority <i>Decentralized, inconsistent operational authorities</i>	 Talent Mismatch <i>Mismatch of talent by agencies not connected to a larger .gov ecosystem strategy</i>			
	Identify Risk Management	 Isolated Identification <i>Segregated vulnerability identification activities across ecosystem</i>	 Insufficient Prioritization <i>No threat-based prioritization to mitigate vulnerabilities</i>	 Unclear Direction <i>Risk management strategies, standards, and policies lack a unified direction</i>			
	Defend Operations	 Perimeter-Focused <i>Perimeter-focused and defensive rather than threat-driven with proactive hunt</i>	 Siloed <i>Siloed cybersecurity operations across agencies in ecosystem</i>	 Reactive <i>Reactive cyber defense operations geared toward recovery</i>			
	Connect Data & Automation	 Slow Extraction <i>Slow data extraction process from agencies to federal level</i>	 Disparate <i>Lack of normalized data sets creates disparate intelligence</i>	 Unstructured <i>Unstructured data and analysis leads to gaps in intelligence</i>			
	Protect Architecture & Controls	 Compliance-Focused <i>Architecture, tools, and controls designed for compliance, not threats</i>	 Legacy Architectures <i>Antiquated security control, tool deployments, and architectures</i>	 Unmanaged <i>No centralized management, oversight, and monitoring</i>			

CHALLENGES IN THE DIRECT ELEMENT ENCOMPASS THE LACK OF CENTRALIZED, CONSISTENT AUTHORITIES TO GOVERN THE .GOV ECOSYSTEM



CHALLENGES IN THE IDENTIFY ELEMENT FOCUS ON THE ABSENCE OF THREAT-DRIVEN STANDARDS AND PRACTICES TO MANAGE FEDERAL CYBER RISK



 <p>Isolated Identification</p> <p>Segregated risk and vulnerability identification activities across ecosystem</p>	 <p>Insufficient Prioritization</p> <p>No threat-based prioritization to mitigate vulnerabilities</p>	 <p>Unclear Direction</p> <p>Risk management strategies, standards, and policies lack a unified direction</p>
<p>Narrow Scope Lack of visibility into software and technology supply chains creates blind spots for risk identification, assessment, and mitigation</p> <p>Gaps in Coverage Uneven and incomplete asset management across .gov ecosystem means there is no comprehensive view of what is connected to FCEB networks and systems</p> <p>Diverse Methodologies .Gov lacks a standardized methodology for threat-based cyber risk management that can be applied and tailored across the full spectrum of FCEB agencies</p>	<p>Lack of Federal-Wide Visibility and Aggregation Threat and risk assessments often stop at agency boundaries; while some .gov-wide dashboards exist, these do not yet generate a true holistic, “common operating picture”—type view of the broader .gov cyber threat and risk landscape</p> <p>No Risk Prioritization Processes Agencies lack proven and repeatable methodologies for prioritizing risks based on insights into adversaries; .gov does not have a mechanism to aggregate and prioritize identified risks to the ecosystem—these gaps lead to control implementation decisions that are not clearly traceable to threats and risks</p>	<p>Compliance-Driven Mindset Agencies tend to focus on meeting requirements rather than demonstrating reductions in cyber risk from real-world threats through established, repeatable processes</p> <p>Disconnected Risk Management Cyber risk management is often disconnected from mission and business functions, exacerbating challenges of linking risk mitigation activities to real-world consequences of cyber threats and risks</p> <p>Limited Top-Down Direction and Policy Sprawl Risk management policies and standards are a bottom-up sprawl and often created reactively; .gov lacks clear direction and best practices for ecosystem risk management</p>

CHALLENGES IN THE DEFEND ELEMENT CENTER ON REACTIVE, PERIMETER-BASED FEDERAL CYBER DEFENSE OPERATIONS





Perimeter-Focused

Perimeter-focused and defensive rather than threat-driven with proactive hunt

Tactical, Sporadic Cyber Threat Intelligence
Most .gov agencies lack a comprehensive view into the adversaries and adversary tactics, techniques, and procedures targeting their networks. Intelligence is indicator based, ad hoc, and incomplete—and varied among different agencies

Manual Vulnerability Management
Lack of integrated, automated systems for revealing vulnerabilities, matching those to adversary attack patterns and behaviors, and closing vulnerabilities before adversaries can exploit


Siloed

Isolated cybersecurity operations across agencies in ecosystem

Alerts Over Searches
Agency cyber operations focus predominantly on alert-based cyber threat detection and reactive countermeasures that too often result in delayed mitigation while heavy reliance on alerts means more subtle threat actors can penetrate and dwell in networks for longer periods of time—inflicting more damage, exfiltrating more data, and facilitating additional attacks

Sub-Scale Testing and Adversary Emulation
No consistent approaches to red, purple, and blue teaming, resulting in inconsistent stress-testing of cyber defenses and missed opportunities to anticipate adversary actions before breaches occur


Reactive

Reactive cyber defense operations geared towards response and recovery

Response-Focused
Most investments in cyber defense operations are focused on response and recovery—critical functions for all .gov security programs—but have resulted in neglected focus on proactive and preventative operational activities

Non-Uniform Response and Recovery Playbooks
Agencies largely left to their own devices to develop incident response and recovery plans and procedures, versus following or leveraging .gov-wide blueprints, playbooks, and best practices, although CISA's recently released incident and vulnerability response playbooks constitute initial progress on this front

CHALLENGES IN THE CONNECT ELEMENT COVER THE SLOW, DISPARATE PROCESSES FOR DATA COLLECTION AND ANALYSIS



CHALLENGES IN THE PROTECT ELEMENT INCLUDE THE FEDERAL GOVERNMENT'S OUTDATED APPROACH AND ARCHITECTURE FOR SECURING THE ECOSYSTEM



AGAINST THIS BACKDROP, HOW CAN THE ESSENTIAL COMPONENTS OF GOOD FEDERAL CYBERSECURITY BE IDENTIFIED AND STRUCTURED INTO AN ACHIEVABLE VISION STATE THAT ENABLES CISA AND .GOV AGENCIES TO OVERCOME THESE CHALLENGES, DRIVE REAL CYBERSECURITY TRANSFORMATION, AND START OUTPACING CYBER THREATS?

THE FRAMEWORK CAN HELP FEDERAL CYBERSECURITY LEADERS IMAGINE AND ESTABLISH A VISION FOR TRANSFORMED FEDERAL CYBERSECURITY

A Define and Consider Options

Develop a spectrum of options for the future of .gov cybersecurity at each layer of the Federal Cybersecurity Framework

- Facilitates broad thinking about desired federal cybersecurity outcomes, features, and benefits
- Incorporates global best practices and insights from other countries

B Determine Key Characteristics

Identify the key characteristics for good federal cybersecurity based on preferred options

- Cascades characteristics aligned to the design options back into the framework
- Creates a nuanced, defensible target state view for .gov cybersecurity transformation

C Detail “To-Be” Endstate for Federal Cybersecurity

Create vision state for .gov cybersecurity—the destination at the end of the transformation roadmap

- Serves as the basis for an actionable transformation roadmap
- Drives consistent progress and measurable gains in federal cybersecurity

KEY QUESTIONS, ALIGNED TO EACH ELEMENT, SHAPE THE SPECTRUM OF DESIGN OPTIONS ON WHICH TO BUILD THE .GOV VISION STATE



Direct
Organization &
Governance

How do you integrate and align .gov cybersecurity stakeholders?



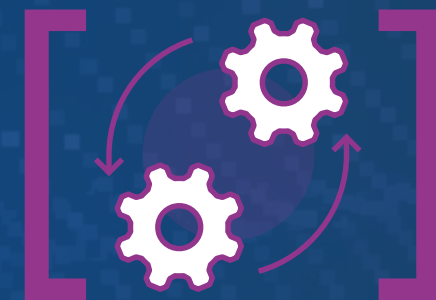
Identify
Risk Management

How do you holistically identify, prioritize, and manage risk across the .gov ecosystem?



Defend
Operations

How do you facilitate proactive cyber defense operations across the .gov ecosystem?



Connect
Data & Automation

How do you harness data and automation to maintain a common operating picture across the .gov ecosystem?



Protect
Architecture &
Controls

How do you apply controls and tools to harden and create resilience in the .gov ecosystem?

EACH DESIGN OPTION IS MEASURED USING THREE CRITERIA: COVERAGE, EFFICIENCY, AND EFFECTIVENESS



Evaluation Criteria **1** Coverage: Breadth of Solution **2** Efficiency: Speed of Implementation **3** Effectiveness: Ability to Mitigate

HOW DO YOU HOLISTICALLY IDENTIFY, PRIORITIZE, AND MANAGE RISK ACROSS THE .GOV ECOSYSTEM?

Identify: Risk Management



Agencies define their own policies, processes, and procedures for identifying and mitigating cyber risks. Risk identification and mitigation occurs at the agency level, with limited and ad hoc sharing across .gov

Risk management focus is driven by a compliance mindset rather than threat-driven standards.

- ✓ Cyber risk management programs tailored and focused on agency-specific threat/risk profiles
- ✗ Missed opportunities to share insights about leading threats, risks, and mitigations; no common operating picture across .gov
- ✗ Compliance focus means risk mitigations may not be effective against real world threats



Agencies develop threat-focused risk management policies, processes, and procedures based on threat scenarios most relevant to the .gov ecosystem.

CISA provides threat intelligence to drive agency policies, strategies, and standards that align to .gov priorities

- ✓ Drives prioritization toward risks that cut across agencies and promotes sharing of best practices
- ✓ Agency risk management approaches are consistent and aligned with one another
- ✗ Interdependency mapping between federal level and agencies is costly and slow



Agencies implement and manage to a uniform .gov cyber risk management approach, issued and overseen by CISA

CISA provides environment-wide, threat-driven dashboards with visualizations to guide and direct agencies in aligning with established .gov priorities.

- ✓ Reveals potential weak spots and gaps across wider .gov environment; provides widespread, comprehensive coverage across .gov
- ✓ Relieves agency-level burdens and responsibilities for policy, processes, and procedures
- ✗ Interdependency mapping between federal level and agencies is costly and slow



Evaluation Criteria **1** Coverage: Breadth of Solution **2** Efficiency: Speed of Implementation **3** Effectiveness: Ability to Mitigate

HOW DO YOU FACILITATE PROACTIVE CYBER DEFENSE OPERATIONS ACROSS THE .GOV ECOSYSTEM?

Defend: Operations



Agencies manage and run their own cyber defense operations either in an agency-level security operations center (SOC), or through agency-level procurement and operations of cyber defense functions

CISA provides operational guidance to agencies, but no operational capability or capacity

- ✓ Flexibility for agencies to tailor and right-size security operations
- ✗ No coordinated cyber defense operations across .gov
- ✗ Potentially costly, with redundant capabilities emerging across .gov
- ✗ Lack of overarching minimum standards for effective security operations across .gov

Coverage	Efficiency	Effectiveness
Low	Low	Low

CISA coordination efforts function in a capacity that facilitates information sharing and shared situational awareness for large agencies

CISA provides SOC-as-a-Service-style capacity smaller agencies that may lack resources and expertise to operate in-house SOCs.

- ✓ Increases situational awareness across .gov
- ✓ Creates efficiencies and consistency; relieves smaller agencies of a significant cyber program burden
- ✗ Requires clear threshold definitions for large vs. small agencies
- ✗ Does not solve challenges around redundancies or lack of consistency in security operations at largest .gov agencies

Coverage	Efficiency	Effectiveness
High	Medium	Medium

CISA provides centralized security operations capacity for the entire .gov—and is largely accountable for operations (versus supporting individual agencies)

CISA serves in centralized execution role, providing SOC-as-a-Service to all agencies, regardless if they have their own individual SOCs or cyber defense capabilities.

- ✓ Significantly increases situational awareness across .gov environment
- ✓ Ensures standardized approaches to all aspects of security operations
- ✗ More difficult to account for specific agency needs or network / infrastructure
- ✗ Requires CISA to build and maintain significant additional technical capacity and resources

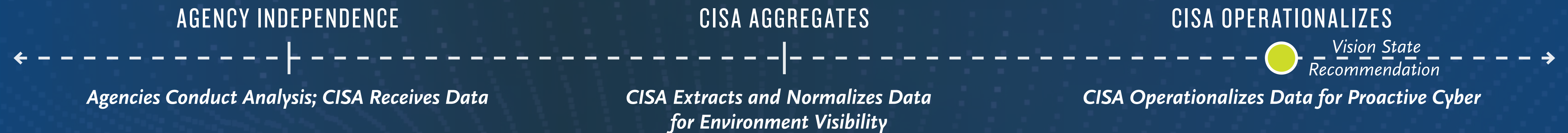
Coverage	Efficiency	Effectiveness
High	Medium	High

Evaluation Criteria **1** Coverage: Breadth of Solution **2** Efficiency: Speed of Implementation **3** Effectiveness: Ability to Mitigate

HOW DO YOU HARNESS DATA AND AUTOMATION TO MAINTAIN A COMMON OPERATING PICTURE ACROSS THE .GOV ECOSYSTEM?



Connect: Data & Automation



CISA pulls agency data sets but does not normalize and enrich data sets or feed them back to individual agencies to facilitate proactive cyber operations.

Agencies, at their discretion, conduct their own analysis on data sets for agency-designated priorities

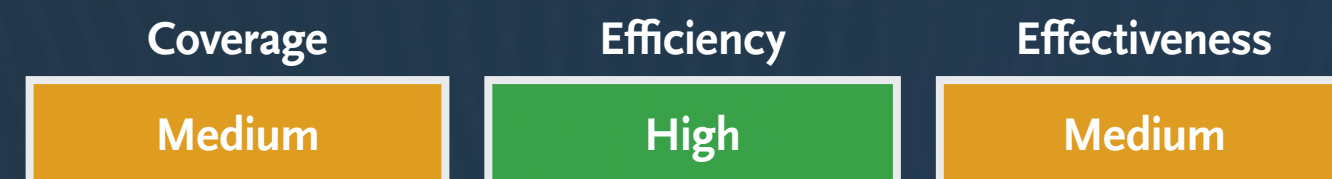
- ✓ Analysis is done internally by agencies and tailored to individual agencies' requirements
- ✗ Data is not normalized, making it difficult to identify cross-government threat activity and vulnerabilities
- ✗ Lack of normalized data at CISA level makes .gov-wide threat hunting impossible



CISA establishes its data set requirements for its centralized environment tools and dashboards, which are utilized by agencies for proactive cyber defense operations.

Agencies share data sets with CISA for normalization and enrichment across the federal environment.

- ✓ Normalized data sets enable CISA to easily identify patterns and gaps
- ✓ Normalization makes it easier to find and remediate vulnerabilities, especially cross-ecosystem, including via Federal threat hunting
- ✗ Development and deployment of federal-wide analytics capabilities may be costly in short term



CISA establishes baseline standards and technology requirements to ensure it can access, normalize, visualize, and operationalize .gov-wide threat and vulnerability data

CISA places data in distributed cloud environment and harnesses it for proactive threat hunt across .gov.

- ✓ Normalized and enriched data provides a comprehensive common operating picture (COP) for the federal environment
- ✓ Enriched data sets enable federal threat hunt operations at scale—entire .gov in scope
- ✗ Potentially costly in short term, and requires agencies to make all relevant data available to CISA



Evaluation Criteria **1** Coverage: Breadth of Solution **2** Efficiency: Speed of Implementation **3** Effectiveness: Ability to Mitigate

HOW DO YOU APPLY CONTROLS AND TOOLS TO HARDEN AND CREATE RESILIENCE IN THE .GOV ECOSYSTEM?



Protect: Architecture & Controls



Agencies architect, procure, and implement distinctive security control and tool regimes based on unique agency needs and preferences

There are no foundational or core security architectures, design patterns, control, or tool requirements established by CISA

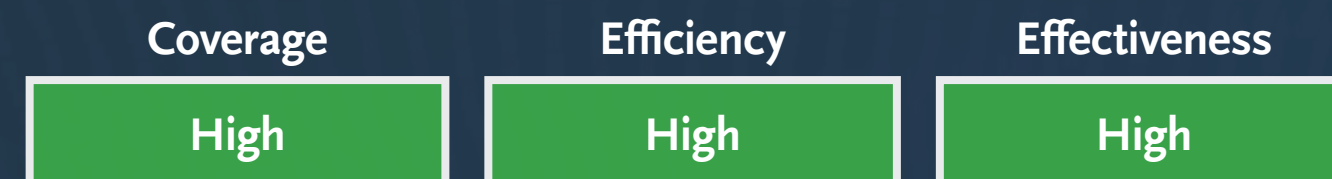
- ✓ Faster to design and implement at the agency level
- ✗ No standardized architecture or security controls blueprints for .gov agencies
- ✗ Lack of standardization and minimum requirements can create weak links across .gov; government unable to harness purchasing power



CISA determines security controls, which are pushed out through CISA-coordinated platforms and tools while agencies separately manage their own security controls and tool implementations and operations

CISA recommends architecture designs—notably around zero trust—as agencies implement at their discretion.

- ✓ Drives greater standardization of controls, tools, and architectures
- ✓ Retains efficiency for agencies, who are still able to design and implement in-house capabilities
- ✗ Varied results depending on differing agency abilities and competencies



CISA maintains centralized design of security architectures and tools through zero trust architecture (ZTA), blueprinting, and other developments for a standardized model and toolset.

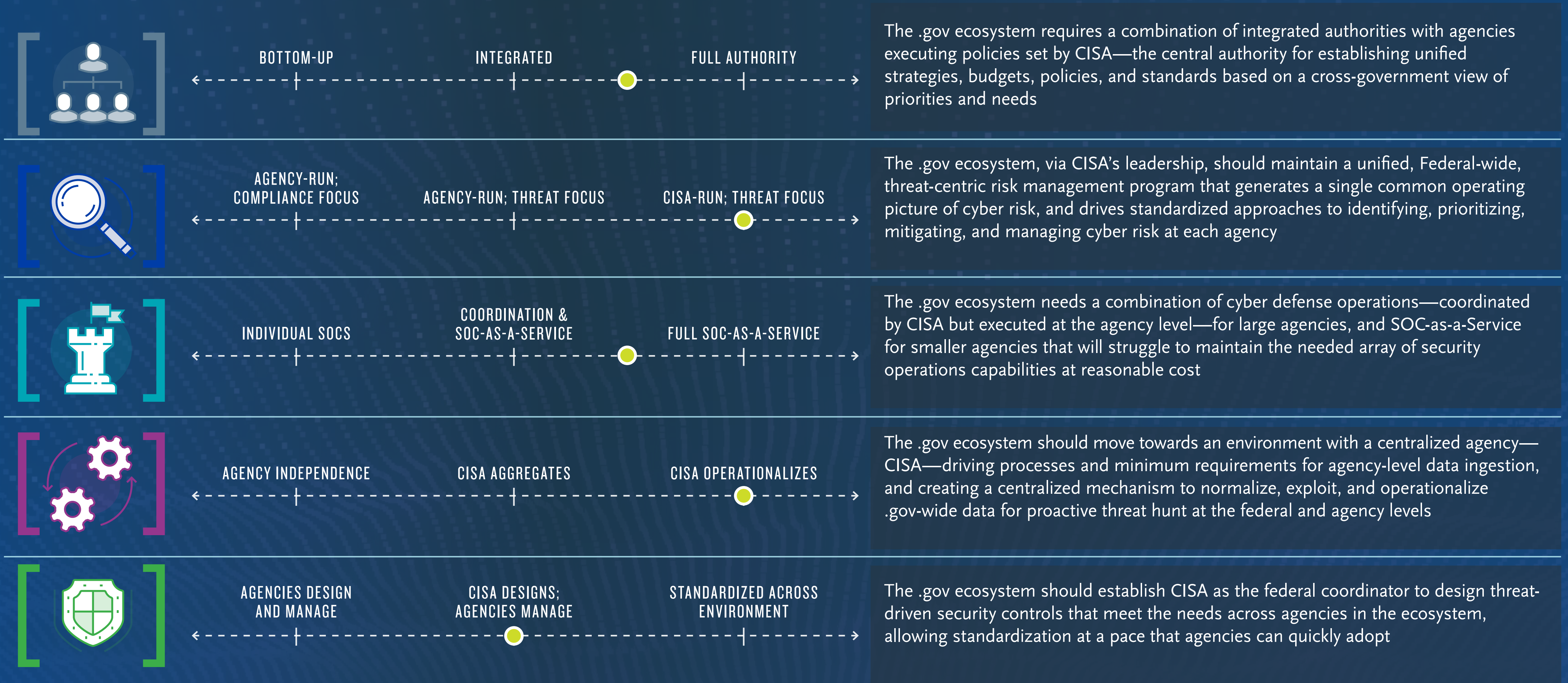
CISA has greater oversight in tuning security controls for agencies based on the priorities for .gov.

- ✓ Ensures standardized architectures, tools, and controls across ecosystem
- ✓ More oversight for continuous improvement
- ✗ Slower implementation due to agencies needing help from CISA to ensure appropriate deployment and alignment with .gov priorities



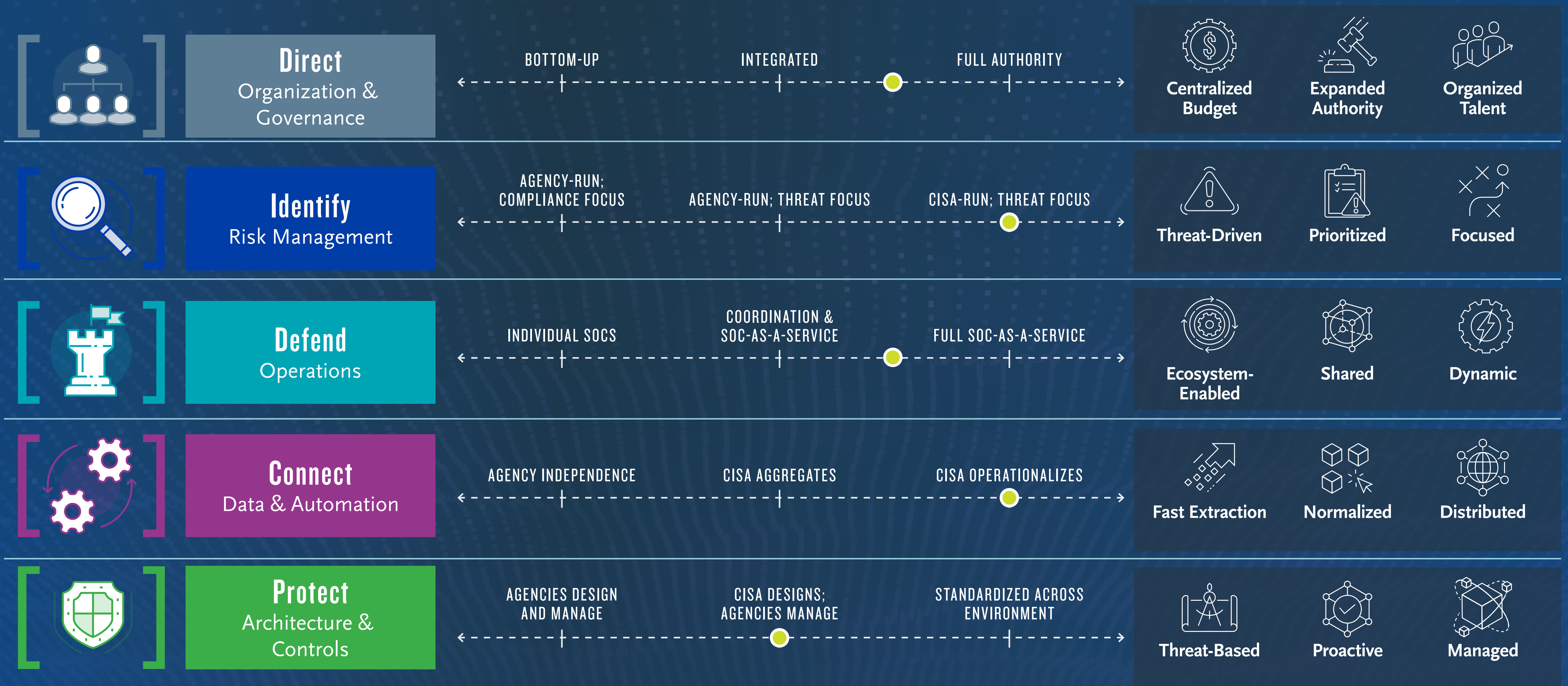
Evaluation Criteria **1** Coverage: Breadth of Solution **2** Efficiency: Speed of Implementation **3** Effectiveness: Ability to Mitigate

THE RECOMMENDED DESIGN CHOICES BRING THE FEDERAL CYBERSECURITY VISION STATE INTO FOCUS























Vision State Recommendation

CLEAR RECOMMENDATIONS ALIGN TO THE DESIGN CHOICES AND CODIFY THE VISION STATE ATTRIBUTES FOR THE .GOV ENVIRONMENT

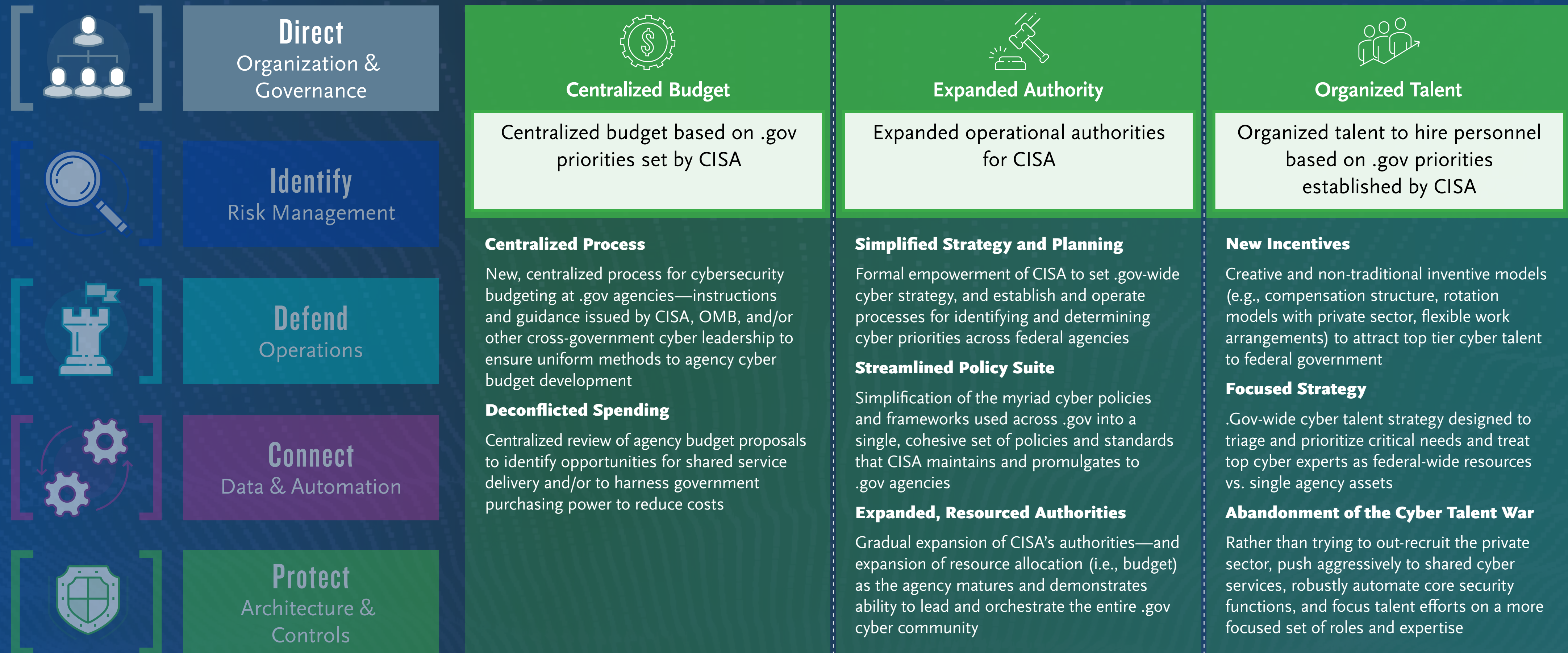


Vision State Recommendation

THE ATTRIBUTES ALIGN DIRECTLY TO THE FEDERAL CYBERSECURITY FRAMEWORK

		ATTRIBUTES			
	Direct Organization & Governance	 Centralized Budget <i>Centralized budget based on .gov priorities set by CISA</i>	 Expanded Authority <i>Expanded operational authorities for CISA</i>	 Organized Talent <i>Organized talent to hire personnel based on .gov priorities established by CISA</i>	
	Identify Risk Management	 Threat-Driven <i>Threat-driven identification of vulnerabilities</i>	 Prioritized <i>Risk-based prioritization of actions to mitigate vulnerabilities</i>	 Focused <i>Focused strategy and policies driven by threat-based environment</i>	
	Defend Operations	 Ecosystem-Enabled <i>Ecosystem-focused for full range cyber operations</i>	 Shared <i>Fused cyber operations and capabilities across agencies</i>	 Dynamic <i>Proactive cyber operations with a focus on threat hunting and offensive cyber</i>	
	Connect Data & Automation	 Fast Extraction <i>Streamlined data extraction for federal analytics</i>	 Normalized <i>Normalized data sets to improve proactive threat hunting</i>	 Distributed <i>Distributed data and analysis for full environment view of cyber operations</i>	
	Protect Architecture & Controls	 Threat-Based <i>Threat-based architecture design and security controls</i>	 Proactive <i>Proactive, threat-driven security controls</i>	 Managed <i>CISA manages and monitors architectures and controls for continuous improvement</i>	

VISION STATE ATTRIBUTES IN THE DIRECT ELEMENT FOCUS ON CENTRALIZATION AND EXPANSION OF CISA'S AUTHORITIES



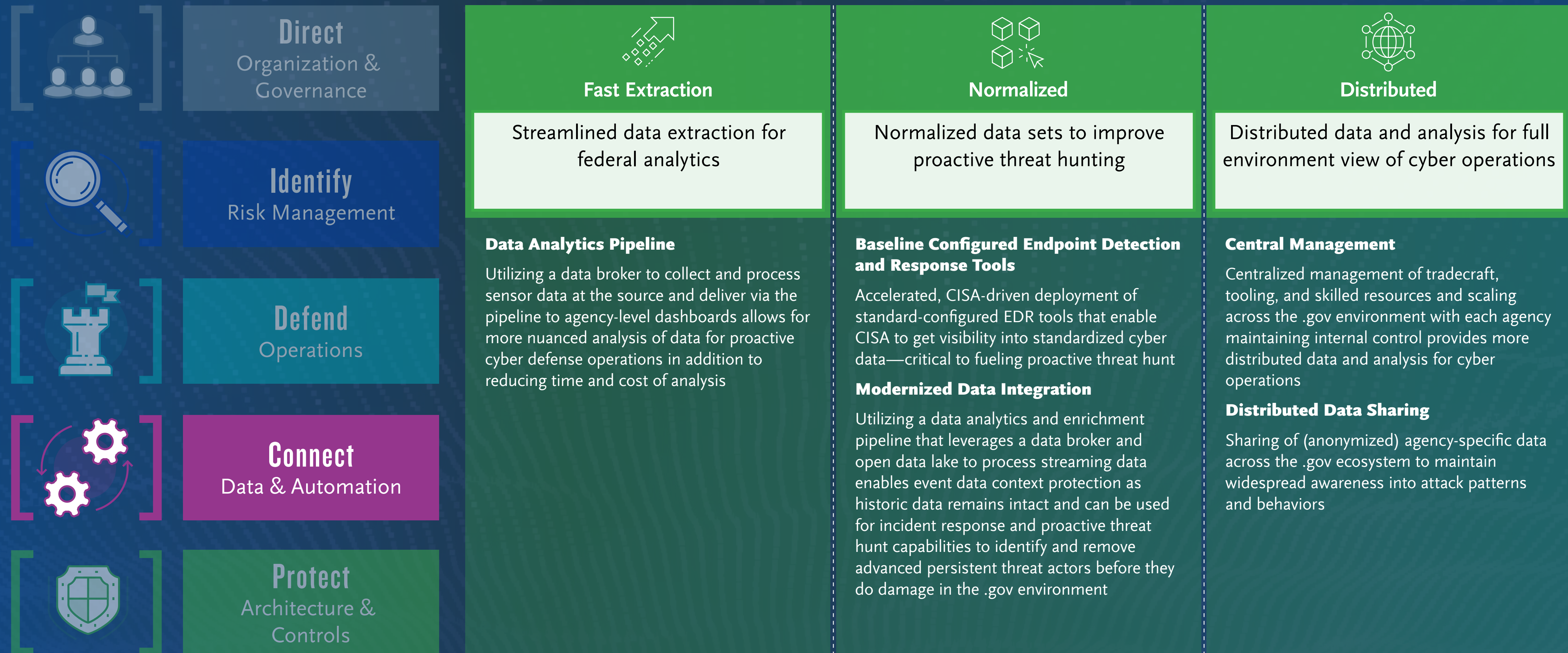
VISION STATE ATTRIBUTES IN THE IDENTIFY ELEMENT UTILIZE A THREAT-DRIVEN FOCUS ON FEDERAL RISK MANAGEMENT



VISION STATE ATTRIBUTES IN THE DEFEND ELEMENT EXPAND AND INTEGRATE FEDERAL CYBER DEFENSE OPERATIONS



VISION STATE ATTRIBUTES IN THE CONNECT ELEMENT MODERNIZE AND ACCELERATE FEDERAL DATA COLLECTION AND ANALYSIS

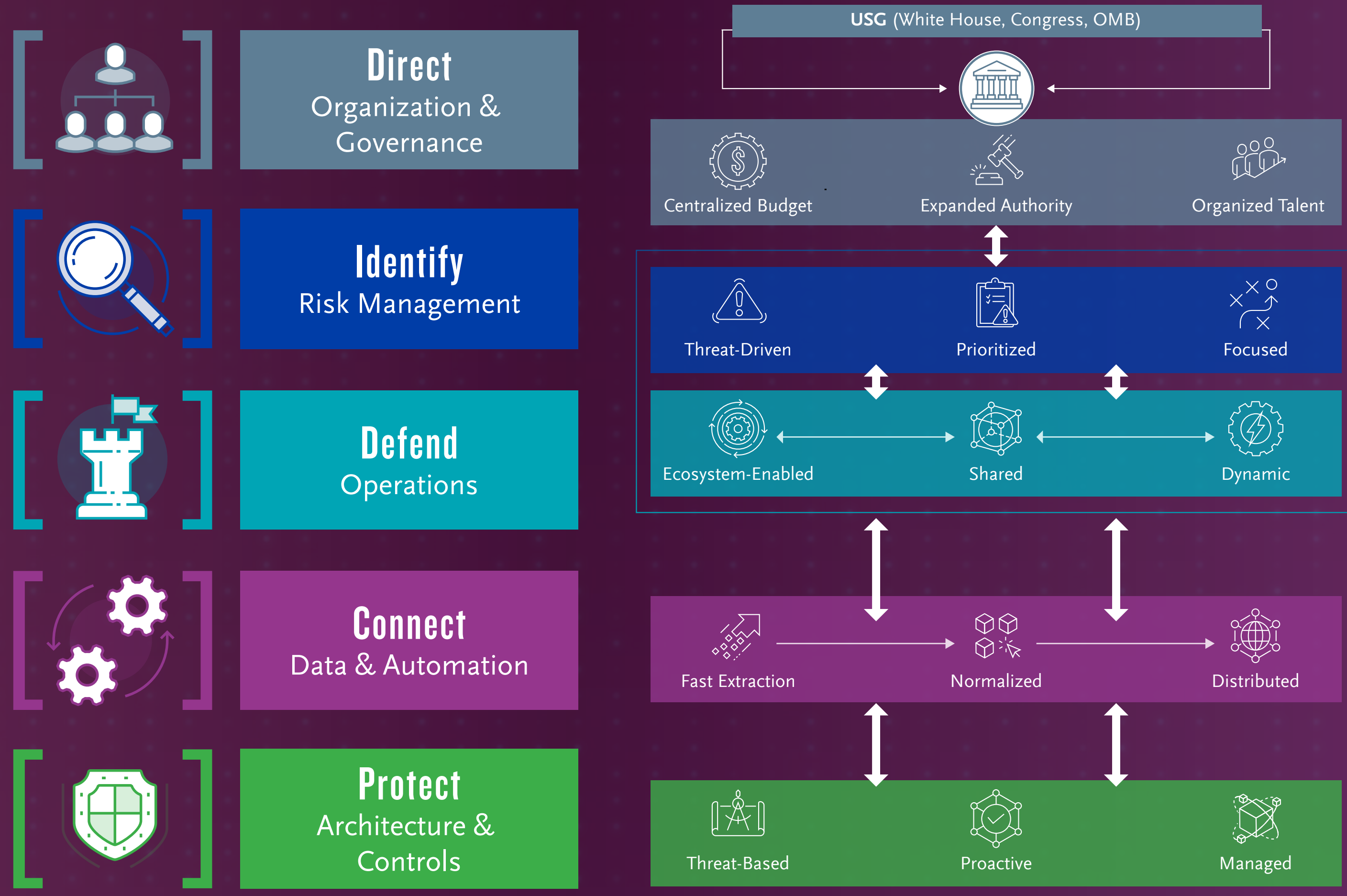


VISION STATE ATTRIBUTES IN THE PROTECT ELEMENT SHIFT THE FEDERAL MINDSET TOWARD ZERO TRUST



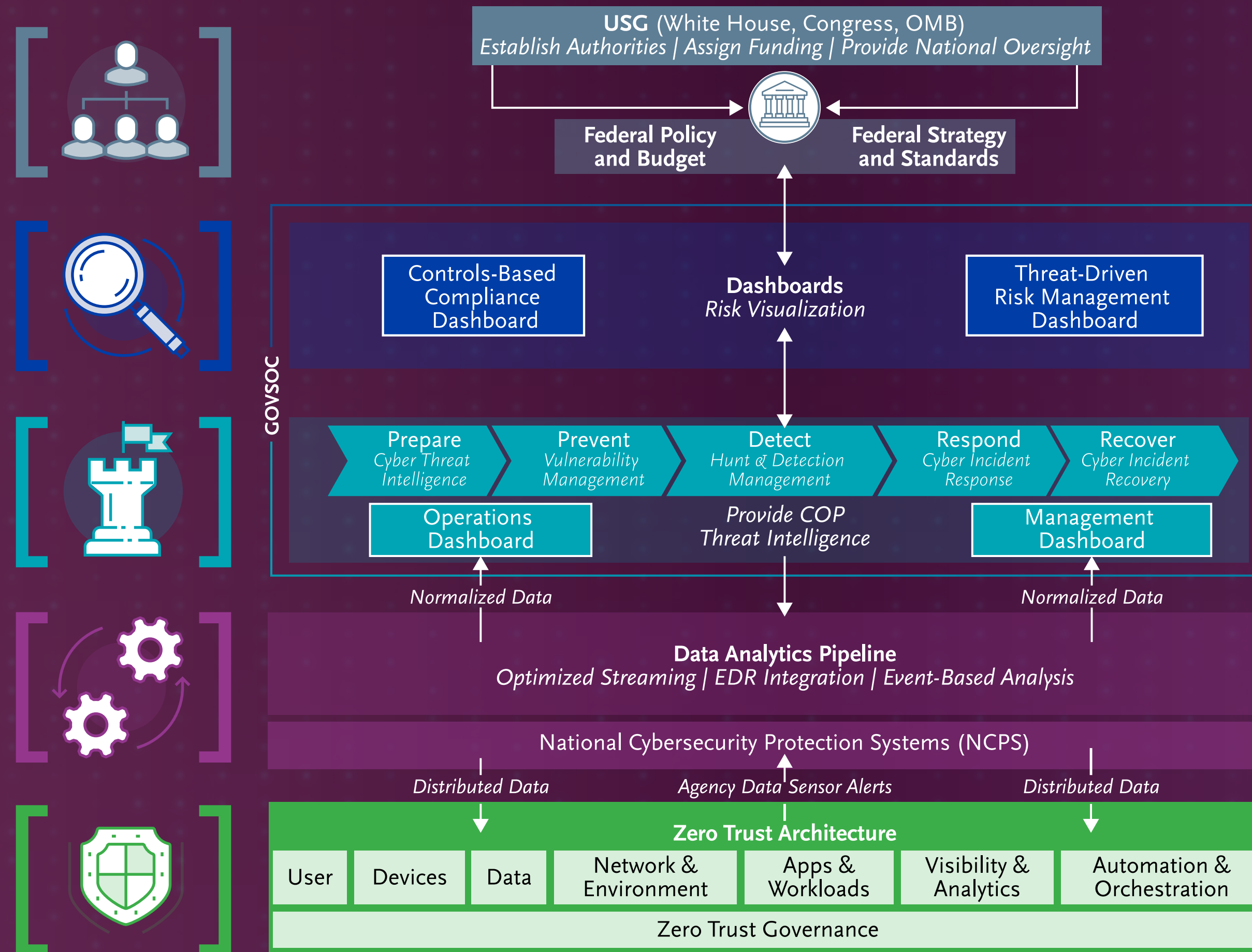
4 SECURING .GOV

THE VISION STATE ATTRIBUTES ALIGN ACROSS THE FIVE LAYERS OF THE FEDERAL CYBERSECURITY FRAMEWORK



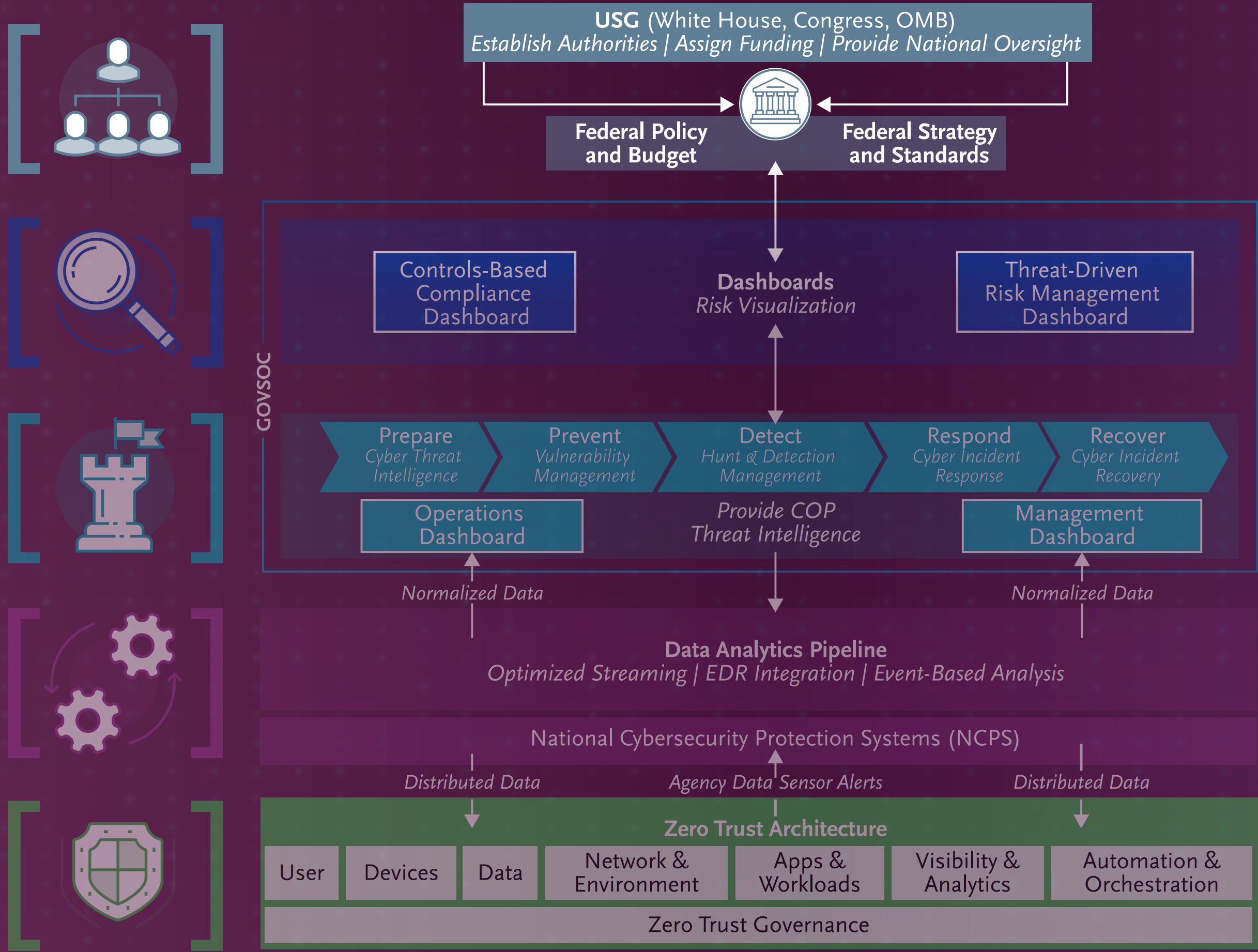
Derived from the recommended design options, the vision state attributes provide a reference point for the .gov ecosystem. Each attribute addresses a specific need for CISA and federal agencies, and provides the content and insights for an actionable, practical roadmap for transforming federal cybersecurity.

THESE ATTRIBUTES TRANSLATE INTO A COMPREHENSIVE VIEW OF THE .GOV ECOSYSTEM—SPANNING CAPABILITIES AND ROLES



Across the framework, the vision state attributes translate into a detailed architecture view covering the key capabilities, technologies, and roles required for a secure and resilient future.

DIRECT CAPABILITIES AND ROLES

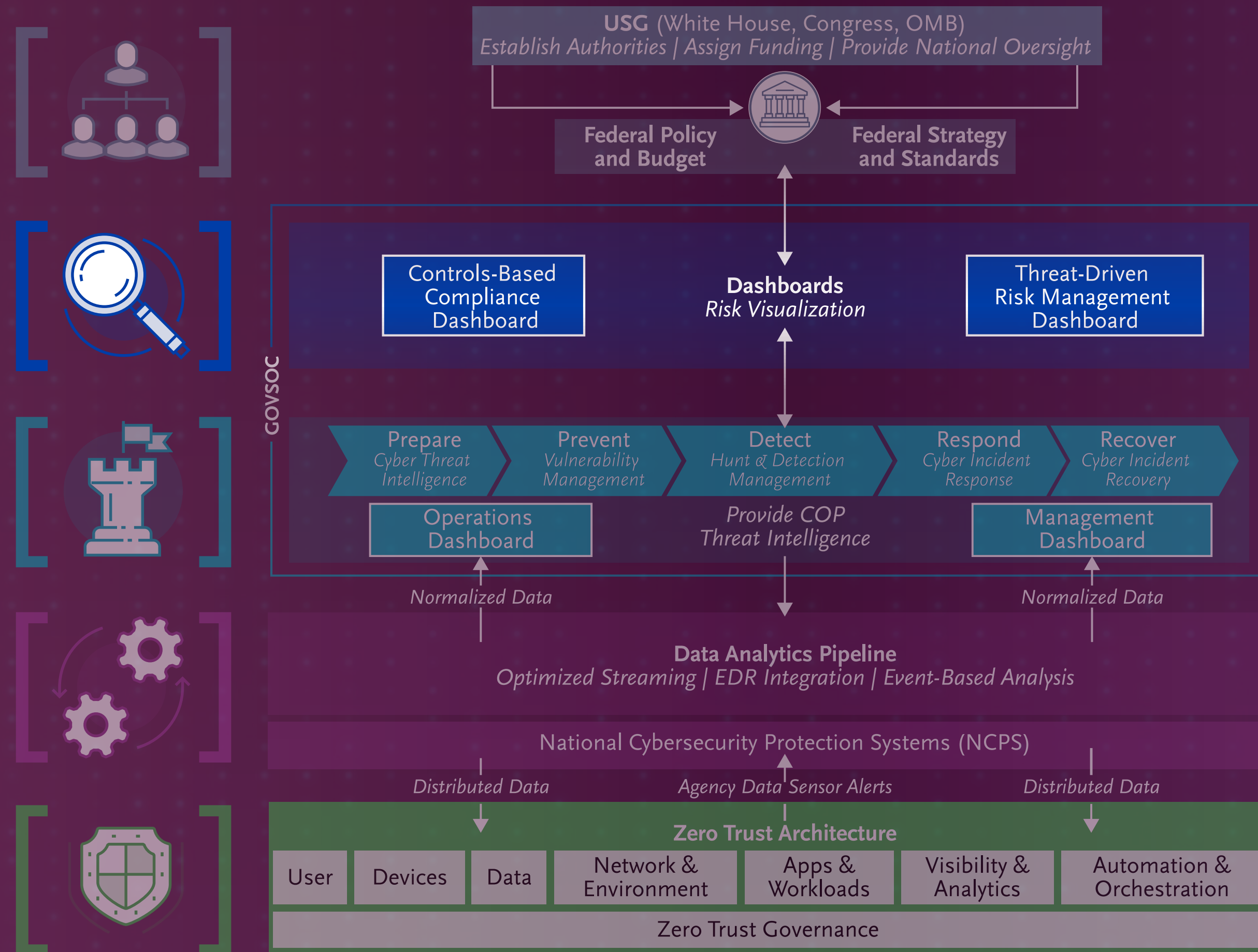


CISA, as the central authority for federal cybersecurity, sets cyber priorities for the .gov environment. Based on these priorities, CISA advises national leadership on needed budgetary allocations for .gov cybersecurity spending and areas earmarked for specific funding attention, providing a structured, **centralized budget** for .gov agencies. The White House, Congress, and the Office of Management and Budget (OMB) ultimately arbitrate final decisions.

CISA operates with **expanded authorities** that include setting the overall federal strategy for .gov, the specific cybersecurity policies and standards agencies must adhere to—pending approval by Congress—and maintain oversight with annual reviews

CISA implements and oversees **federal cyber talent** and resourcing activities to hire personnel based on .gov-wide priorities and needs. CISA provides advisory services and reviews of personnel for specific positions in agencies to guide agency-level decisions.

IDENTIFY CAPABILITIES AND ROLES

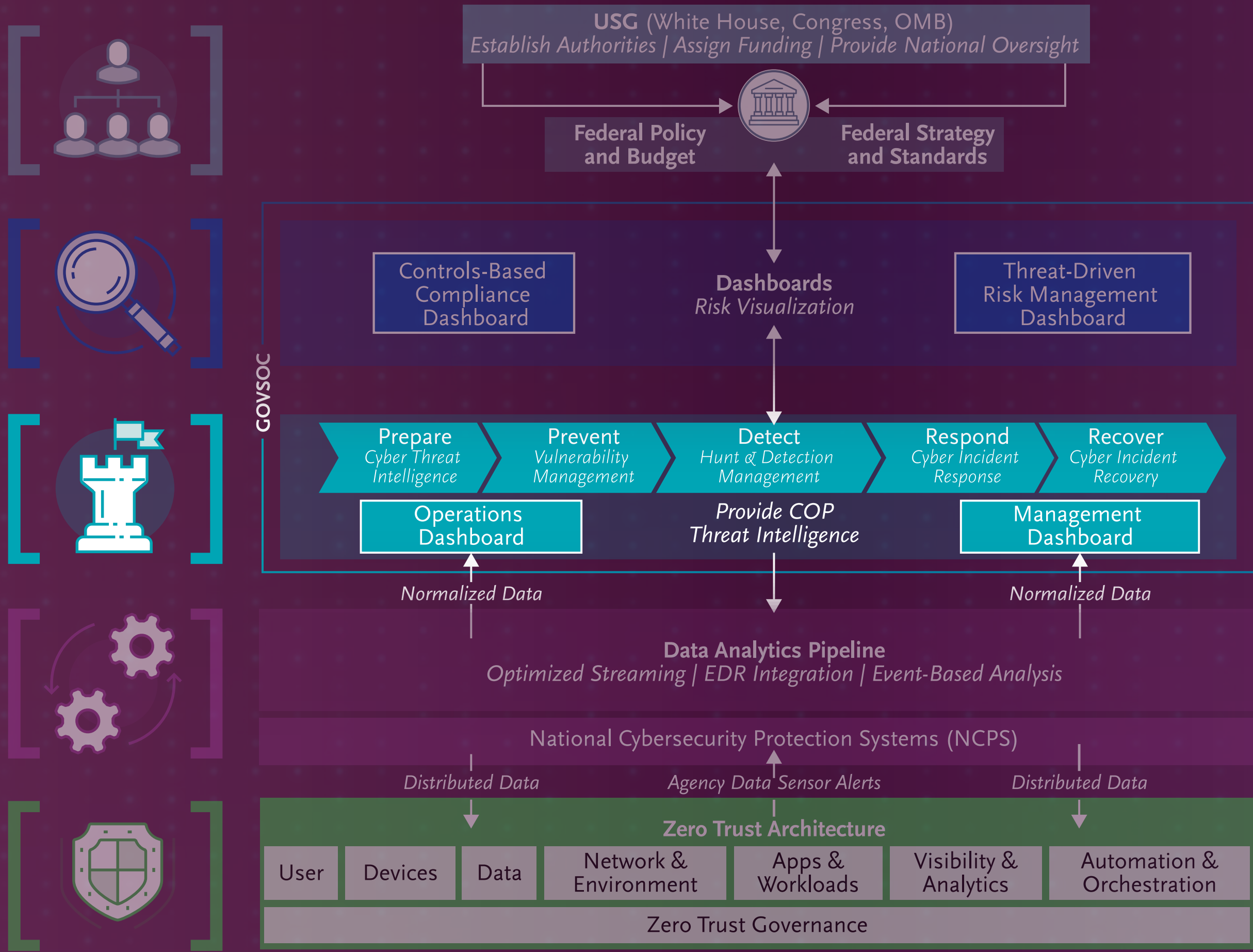


In addition to current compliance dashboards, CISA utilizes risk visualization dashboards based on **threat-driven scenarios** that include third-party and supply chain threats, updated as threats change throughout the ecosystem.

CISA develops risk management strategies, policies, and standards that are **threat-centric and accelerate the agency-level use of threat and countermeasure modeling**. CISA updates .gov risk management guidance based on evolutions to the threat landscape

Through a centralized SOC (GOVSOC in vision state architecture view) function, CISA leverages federal-wide threat and risk dashboards to conduct **risk-based prioritization** of threats and vulnerabilities for mitigation. CISA provides prioritization data via visualized dashboards to agencies, helping them with mitigation and other security operations activities.

DEFEND CAPABILITIES AND ROLES

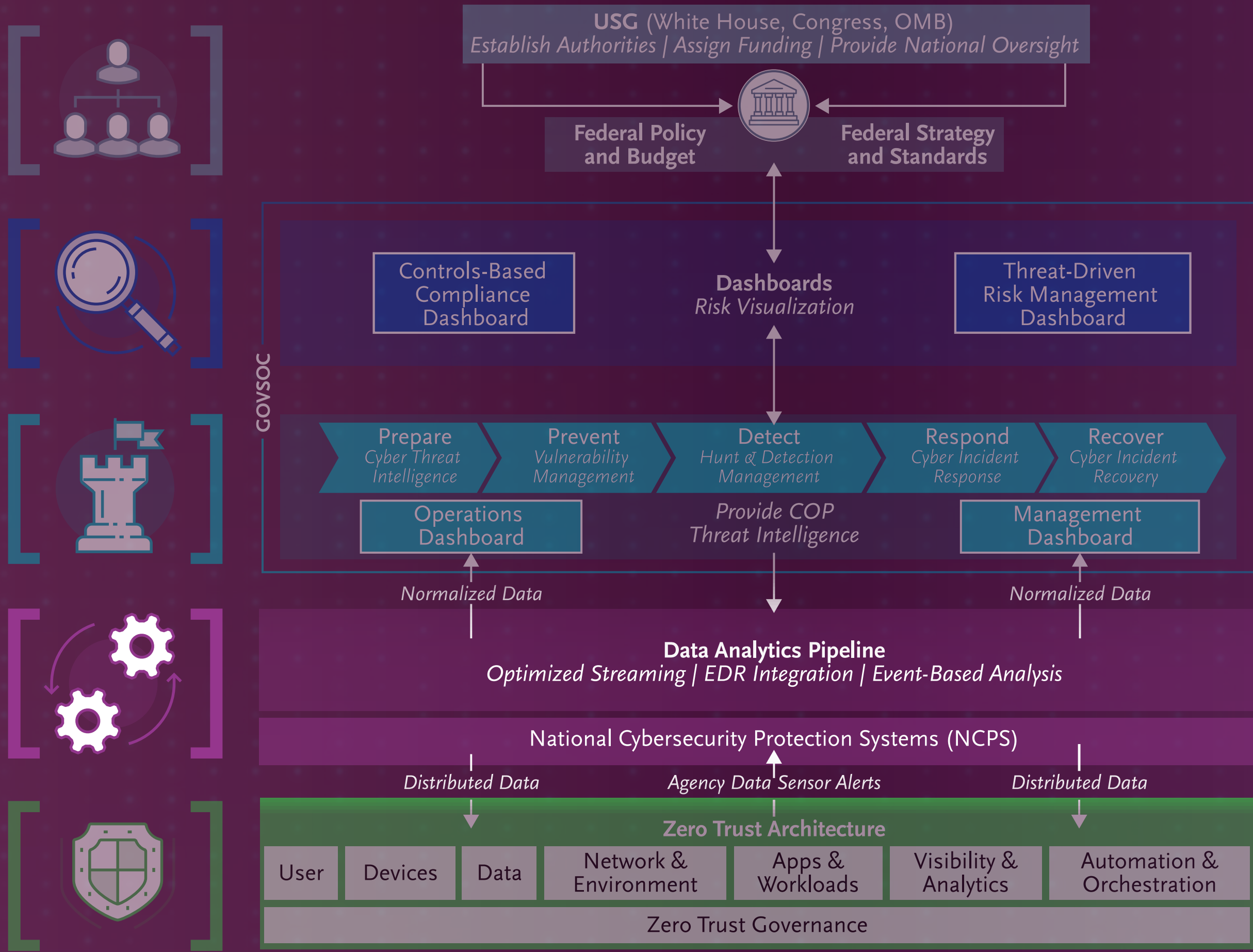


CISA creates mandates and incentives that **drive adoption of proactive cyber defense capabilities across .gov agencies**, with focus on automated and real-time threat and vulnerability management that aggregates and disseminates findings and solutions for the entire .gov

CISA—through the GOVSOC—collaborates with agency-level SOCs to create fused cyber defense operations and capabilities, enabling a Common Operating Picture (COP) for the .gov ecosystem. In addition, the SOC **shares threat intelligence and capabilities** with smaller agencies without the resources (budgetary or personnel) to do so independently.

CISA utilizes standardized, normalized data from EDRs across the .gov to conduct **dynamic, proactive threat hunt** across the .gov ecosystem. Agencies with SOCs, in parallel, engage in proactive threat hunt activities while the GOVSOC helps smaller agencies—or provides—threat hunt capabilities.

CONNECT CAPABILITIES AND ROLES

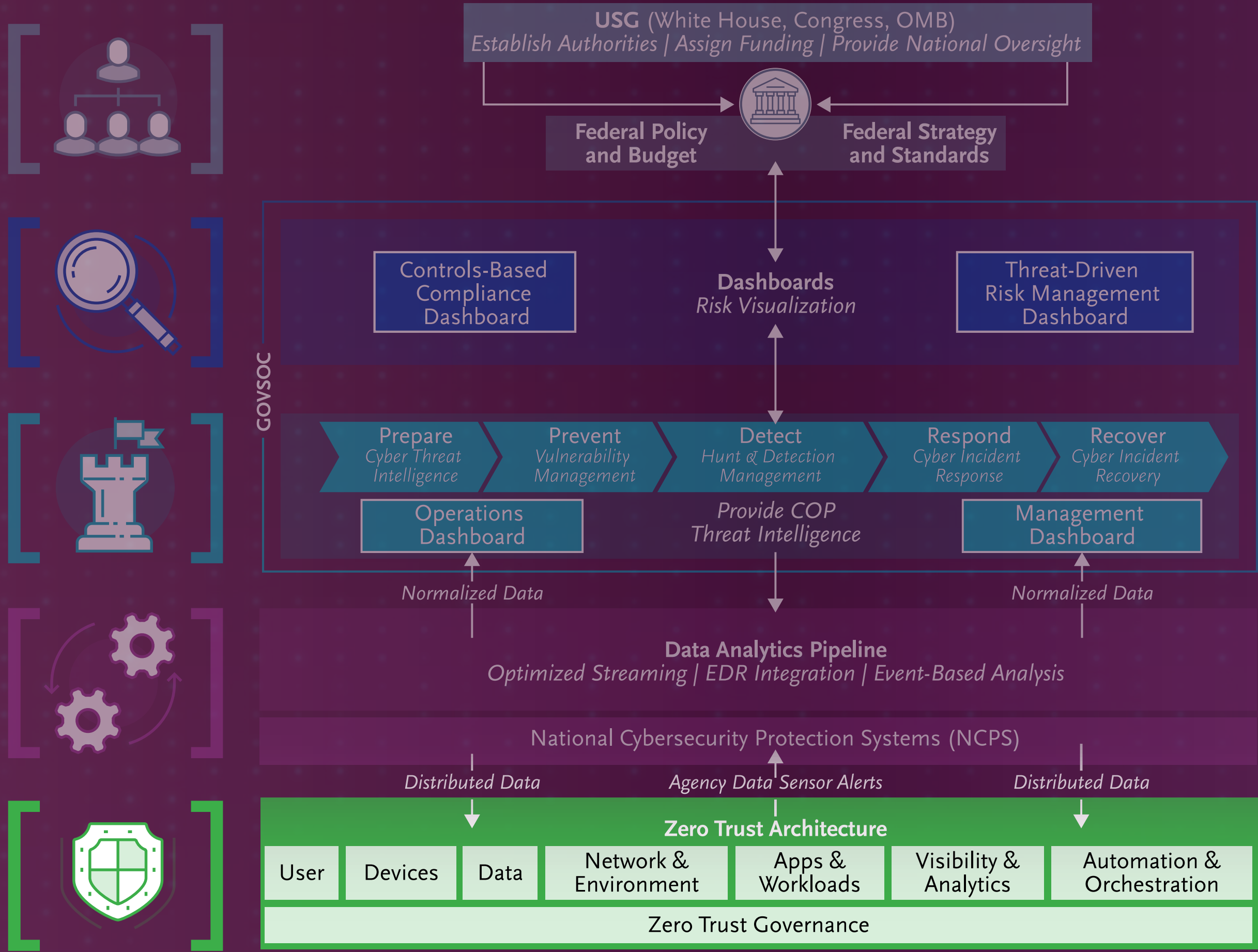


To improve federal analytics, CISA implements a data analytics pipeline for streamlined, **fast data extraction** utilizing EDR sensor and telemetry data ingestion across agencies in the .gov environment. The acceleration of data extraction cascades to faster analysis and the ability for CISA to provide actionable intelligence to agencies for threat hunt.

CISA optimizes streaming through the data analytics pipeline to provide improved, **normalized data sets** to augment proactive threat hunting by CISA. and individual agency threat hunt teams across the .gov environment.

CISA, leveraging the data analytics pipeline, shares **distributed data** and event-based analysis through the National Cybersecurity Protection System (NCPS) across .gov agencies, enabling the full environment view required for comprehensive cybersecurity operations at agencies and the federal level.

PROTECT CAPABILITIES AND ROLES



CISA provides packages of diagnostics, templates, blueprints, roadmaps, and architectures that **enable accelerated agency-level transformation to zero trust-based security**. CISA consults with agencies on zero trust implementation plans and continually updates its available packages of zero trust-based artifacts

CISA maintains best practice product lists and roadmaps—and provides shared services—that enable the entire .gov to access core protective controls quickly and in a cost-effective manner. Available controls and tools change based on threat and technology evolutions

CISA **manages and monitors implemented zero trust architectures** as well as security tools and controls to provide continuous improvement across the seven pillars of zero trust (and governance) to support threat-driven security for agencies across the .gov environment.

KEY ACTIONS CAN MOVE THE .GOV ENVIRONMENT ALONG THE ROADMAP TOWARDS ITS VISION STATE



DIRECT

- Empower Federal CISO within CISA
- Expand CISA's authorities
- Centralize federal cyber budgeting
- Refine acquisition guidelines
- Unify managing policies
- Organize cyber talent



IDENTIFY

- Establish risk management strategy
- Build threat-based approach
- Continuously improve risk prioritization
- Integrate asset and risk management practices
- Solidify cyber risk practices
- Create interdependent cyber risk programs



DEFEND

- Transition from static to dynamic threat indicators
- Employ cyber fusion operations
- Build proactive threat hunt
- Establish concrete incident response
- Leverage threat intelligence
- Modernize NCPS



CONNECT

- Modernize data integration layer
- Create data analytics pipeline
- Integrate EDR sensor data for normalization and enrichment

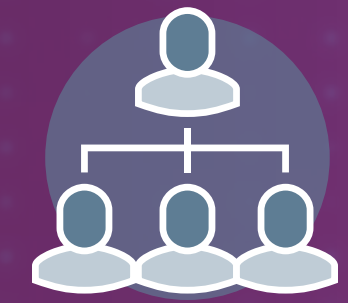


PROTECT

- Establish secure, federated cloud
- Deploy commoditized services
- Pursue SOAR solutions
- Extend perimeter security protection
- Modernize cloud technologies

To drive transformation, CISA and other federal agencies should begin execution of specific actions—aligned to the five elements of the Federal Cybersecurity Framework—that will enable cybersecurity maturity gains and progress toward realization of the .gov vision state architecture.

KEY ACTIONS TOWARD STRENGTHENING FEDERAL ORGANIZATION AND GOVERNANCE



DIRECT

Organization & Governance

Empower Federal CISO

USG empowers a federal CISO role within CISA (separate from CISO within OMB) to centralize accountability for .gov cybersecurity and facilitate “dotted-line” reporting and integration of primary cyber functions between federal agencies

Expand CISA’s Authorities

USG empowers CISA to advise and develop federal policies, budgets, strategies, and prioritized standards for federal agencies to implement; instruct CISA to monitor progress and provide refinements on an annual basis

Centralize Federal Cyber Budgeting

USG establishes CISA, as the central cyber authority, with a mandate to review, deconflict, and provide overarching guidance on agency cyber budgets in addition to giving recommendations to OMB for national oversight and annual budget reviews

Refine Acquisition Guidelines

USG creates greater flexibility for cyber vendor and security tool acquisition via CISA governance mechanisms to improve agency response to threats across the broader environment

Unify Managing Policies

CISA manages the .gov environment risk—via the federal CISO—by disseminating policies and guidance to agency-level CISOs to streamline implementation and adoption parameters, accelerating cybersecurity policy implementation and response time through simplification and centralization

Organize Cyber Talent

CISA provides guidance and support to agencies that govern hiring practices for qualified personnel based .gov-wide assessments responding to skills needs, new policy requirements, and risk prioritization based on the current threat environment

KEY ACTIONS TOWARD OPTIMIZING FEDERAL RISK IDENTIFICATION AND MITIGATION



IDENTIFY Risk Management

Establish Risk Management Strategy

CISA establishes a comprehensive, threat-driven, automated, and real-time risk management strategy to delineate boundaries for directing risk-based decisions for agencies across the .gov ecosystem

Build Threat-Based Approach

CISA and federal agencies shift activities to focus on threat scenarios and kill chain analysis (instead of simply seeking compliance) to assess security posture, identify gaps, and mitigate risks based on threats

Continuously Improve Risk Prioritization

CISA utilizes periodic assessments of cyber controls performance against identified threat use cases using likelihood, impact, and controls performance to calculate risk measured against overall risk tolerance to improve risk prioritization for federal and agency use

Integrate Asset and Risk Management Practices

CISA integrates asset and risk management processes to understand business and mission processes, facilitating a deeper understanding of cyber incident mission disruption

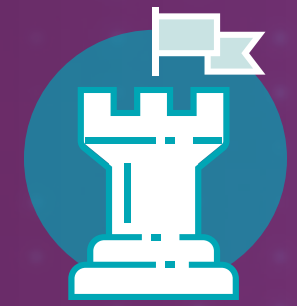
Solidify Cyber Risk Processes

CISA creates and solidifies processes for assessing, prioritizing, and mitigating agency-wide cybersecurity risks based on the aggregation of system-level risk data from federal and agency data pipeline collection

Create Interdependent Cyber Risk Programs

CISA supports agency creation of interdependent cyber risk programs with shared roles and responsibilities across stakeholders and capabilities, enabling collaboration in an organized, structured, transparent manner

KEY ACTIONS TOWARD OPTIMIZING FEDERAL RISK IDENTIFICATION AND MITIGATION



DEFEND Operations

Transition from Static to Dynamic Threat Indicators

CISA oversees federal agencies' pivot from static threat indicators—which are often outdated—toward cloud-enabled defensive systems hardened with zero-trust architecture and provisioned with shared security controls, increasing mission capabilities and enhancing cost effectiveness

Employ Cyber Fusion Operations

Through an established federal SOC (GOVSOC), CISA employs cyber fusion solutions to bolster data aggregation, synthesis, and analysis across risk, monitoring, detection, incident response, recovery, and other functions

Build Proactive Threat Hunt

CISA, through the GOVSOC—and agencies with their own threat hunt teams—employ persistent threat hunt operations to detect subtle attacker actions versus sitting back and employing a reactive security posture

Establish Concrete Incident Response

CISA articulates to agencies the requirements for incident monitoring and response with concrete procedures and information flow mechanisms in addition to timelines and standards—also employed by the GOVSOC, overseen by CISA

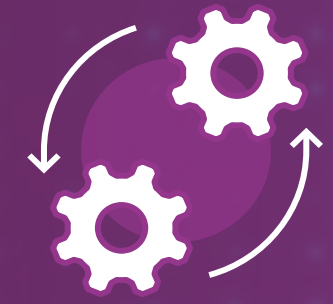
Leverage Threat Intelligence

CISA fully leverages cyber threat intelligence collected through the National Cybersecurity Protection System (NCPS) as the stable foundation for incident response and management processes to make more informed decisions for threat response operations

Modernize NCPS

CISA assists USG in modernizing the NCPS to monitor all types of federal network traffic to include signature-based, anomaly-based, and stateful monitoring

KEY ACTIONS TOWARD ENHANCING FEDERAL DATA INGESTION, INTEGRATION, AND ANALYSIS



CONNECT

Data & Automation

Modernize Data Integration Layer

USG authorizes funds to modernize the data integration layer by implementing a data analytics and enrichment pipeline, leveraging a data broker and open data lake to enable event data context protection—keeping historic data intact that can then be used for improved incident response and proactive threat hunt

Conduct Proactive Threat Hunt

CISA and federal agencies conduct proactive, persistent threat hunt using a distributed model with hunting conducted at the edge (agency-level) paired with a centralized team within CISA to coordinate across the federal environment, facilitating greater dashboard visibility through information processed to a common standard, enabling the centralized management of tradecraft, tooling, and skilled resources in addition to scalability across the .gov environment while agencies maintain internal control

Create Data Analytics Pipeline

CISA creates a data analytics pipeline within the NCPS to modernize data integration by enabling a data broker to quickly extract and process sensor data at the source and deliver via the data pipeline to agency-level and CISA-level dashboards for use in proactive threat hunt and other cyber mitigation activities

Integrate EDR Sensor Data for Normalization and Enrichment

CISA and federal agencies utilize the data analytics pipeline within the modernized NCPS to integrate EDR sensor data, telemetry, and CDM sensor data for normalization and enrichment providing a constantly updated common operating picture (COP) at the federal and agency levels built from ingested data across the .gov environment

KEY ACTIONS TOWARD IMPROVING FEDERAL ARCHITECTURES AND SECURITY CONTROLS



PROTECT Architecture & Controls

Establish Secure, Federated Cloud

CISA alleviates agency burdens and provides “.gov-as-a-service” where agencies maintain ownership of their applications, data, and processes but gain the benefit of advanced security services and scale advantages from cloud environments with pre-configured cyber defense and response tools integrated into a common, zero trust architecture

Deploy Commoditized Services

CISA provides scale, consistency, and visibility across the .gov environment—resolving situations created when protective and defensive controls, tools, and zero trust architecture designs are siloed within individual agencies

Pursue SOAR Solutions

CISA establishes and helps agencies implement comply-to-connect and build-in design security solutions to address the current fragmented and ineffectual security controls system

Extend Perimeter Security Protection

CISA and agencies extend security protections and privacy controls beyond network perimeter defense of the .gov environment and focus on safeguarding the data, systems, and network layers across the ecosystem

Modernize Cloud Technologies

CISA helps modernize cloud technologies and integrate new security controls within a standardized zero-trust architecture to prevent intrusions into federal networks and supports agencies as they move toward a standardized zero-trust architecture by providing guidance and oversight

A SECURE .GOV AND BEYOND

Ultimately, if adopted and implemented, the architecture and recommendations roadmap—detailed in the preceding pages and aligned to the Federal Cybersecurity Framework—coalesces into a mature, unified vision state. This vision state includes discrete, measurable, and comprehensive cybersecurity outcomes integrated into a new, transformed picture for federal cybersecurity.

However, even at this point, the federal cybersecurity journey will not be complete. Ongoing strategic challenges—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—will remain. However, the journey toward a secure and resilient .gov will be well underway.

GAO REPORT FINDINGS (MARCH 2021):

Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges

KEY TAKEAWAY

750 recommendations aligned to the four cybersecurity challenges identified by the GAO since 2010 **were not implemented** as of December 2020 while **67 of 103** priority recommendations were **likewise not implemented**¹³

APPENDIX

1 Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight	2 Securing Federal Systems and Information	3 Protecting Cyber Critical Infrastructure	4 Protecting Privacy and Sensitive Data
<p>Federal agencies struggle with:</p> <ul style="list-style-type: none"> • Designating authorities to oversee implementation of national cyber initiatives • Updating strategies based on emerging technologies (e.g., 5G) • Addressing cyber workforce shortages and implementing cyber workforce planning activities 	<p>Federal agencies struggle with:</p> <ul style="list-style-type: none"> • Strengthening and implementing agency incident response policies and practices • Addressing risks facing critical federal functions (e.g., COVID-19 response) • Establishing and overseeing modernization of legacy plans, policies, and systems (e.g., cloud migration) 	<p>Federal agencies struggle with:</p> <ul style="list-style-type: none"> • Implementing and reporting on improvements using NIST framework • Prioritizing oversight of evolving threats to critical infrastructure • Developing, prioritizing, and monitoring infrastructure protection plans to national and sector goals 	<p>Federal agencies struggle with:</p> <ul style="list-style-type: none"> • Protecting data shared with states and other external entities • Verifying the identities of users who access federal networks • Updating data policies based on technology changes (e.g., facial recognition technology [FRT])
<p>Status</p> <p>59% of recommendations implemented</p> <p>22% of priority recommendations implemented</p>	<p>Status</p> <p>75% of recommendations implemented</p> <p>34% of priority recommendations implemented</p>	<p>Status</p> <p>38% of recommendations implemented</p> <p>18% of priority recommendations implemented</p>	<p>Status</p> <p>54% of recommendations implemented</p> <p>75% of priority recommendations implemented</p>

[< Back to page 14](#)

SENATE REPORT FINDINGS (AUGUST 2021):

Federal Cybersecurity: America's Data Still at Risk

KEY TAKEAWAY

A 2019 Senate report analyzed systemic failures in eight key Federal agencies to comply with federal cybersecurity standards. Two years later, the **same issues remained**, and **seven agencies had not met basic cybersecurity standards** to protect sensitive data

Agency Findings

- ✘ Seven agencies used legacy systems or **applications no longer supported** by the vendor with security updates
- ✘ Seven agencies **failed to maintain** accurate and comprehensive IT asset inventories
- ✘ Seven agencies **failed to protect PII** adequately
- ✘ Six agencies operated systems **without current authorizations** to operate
- ✘ Six agencies **failed to install security patches** and other vulnerability remediation quickly
- ✘ Three agencies showed **very little improvement** since the subcommittee's report in 2019

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

Federal Government Findings

- ✘ **No single point of accountability** for federal cybersecurity, and highly-federated cyber responsibilities make government-wide information security improvements difficult
- ✘ Lack of a **unified cybersecurity strategy** to combat the current threat landscape
- ✘ Continued overreliance on **costly and difficult-to-serve legacy technology**, which diverts funding from other efforts
- ✘ **Failure to implement** certain key cybersecurity requirements, including encryption, user access limitations, or multifactor authentication

A **centrally-coordinated approach** for government-wide cybersecurity can support strategy development and implementation efforts across .gov

[< Back to page 14](#)

REFERENCES

- ¹ The White House (2020), *Appendix, Fiscal Year 2021 Budget of the U.S. Government*.
- ² John Costello and Mark Montgomery, Lawfare (2021), *How the National Cyber Director Position Is Going to Work*.
- ³ The White House (2021), *Executive Order on Improving the Nation's Cybersecurity*; The White House (2021), *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*.
- ⁴ Dr. Michael McGuire (2021), *Nation States, Cyberconflict and the Web of Profit*, HP.
- ⁵ C. Todd Lopez (2021), *In Cyber, Differentiating Between State Actors, Criminals Is a Blur*.
- ⁶ Michal Christine Escobar (2020), *Carnival Corp. Reveals Ransomware Attack*.
- ⁷ Security Magazine (2021), *Ransomware Soars With 62% Increase Since 2019*.
- ⁸ RiskBased Security (2020), *2020 Year End Report: Data Breach QuickView*.
- ⁹ CISA (2021), *Potential Threat Vectors to 5G Infrastructure*.
- ¹⁰ Derek Handova, *Security Boulevard* (2020), *How 5G and IoT Devices Open Up the Attack Surface on Enterprises*.
- ¹¹ Sean Frazier (2021), *Building Herd Immunity into Government Cybersecurity*.
- ¹² Joseph Marks, *Washington Post* (2021), *The Government's Facing a Severe Shortage of Cyber Workers When It Needs Them the Most*.
- ¹³ GAO (2021), *GAO-21-288: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*.

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 more than 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](https://www.boozallen.com). (NYSE: BAH)