THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

NSTAC REPORT TO THE PRESIDENT

Zero Trust and Trusted Identity Management

February 23, 2022

Contents

Figures

Tables

Executive Summary

In May 2021, in the aftermath of a series of significant cybersecurity incidents, the White House tasked the President's National Security Telecommunications Advisory Committee (NSTAC) with conducting a multi-phase study on "*Enhancing Internet Resilience in 2021 and Beyond.*" The tasking directed NSTAC to focus on three key cybersecurity issues foundational to United States national security and emergency preparedness:

1. Software Assurance in the Commercial Information and Communications Technology Supply Chain.

2. Zero Trust and Trusted Identity Management.

3. The Convergence of Information Technology (IT) and Operational Technology (OT).

This report focuses on #2, Zero Trust and Trusted Identity Management. Zero trust is a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified.

Also in May 2021, President Biden issued *Executive Order (EO) 14028: Improving the Nation's Cybersecurity*,[1] underscoring the urgency of U.S. Government action to address these growing risks. It states, "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."

Among several directed actions, the EO specifically identifies "Advancing towards Zero Trust Architectures" as one such bold change. In the months following the EO, the U.S. Government has issued a series of policy documents further clarifying the Federal Government's strategic approach to zero trust implementation, culminating in the release of the Federal Zero Trust Strategy[2] on January 26, 2022 . Since the zero trust policy environment remains in its infancy, this is a timely, significant opportunity to deeply consider industry expertise in the early stages of the Federal Government's zero trust journey.

Report Focus and Scope

The guidance and recommendations in this report recognize the U.S. Government's broad opportunity and responsibility to help catalyze cybersecurity transformation through zero trust adoption.

---

[1] *Executive Order (EO) 14028: Improving the Nation's Cybersecurity*, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[2] Office of Management and Budget, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

- Section 1 characterizes the magnitude of this opportunity, with many U.S. departments and agencies at a pre-implementation point with ample opportunity to shape and define successful zero trust outcomes.

- Section 2 summarizes several industry zero trust best practices and deployment models that can aid the Federal Government's implementation efforts.

- Section 3 focuses on recommendations for how the U.S. Government can leverage technologies and new governance models to directly influence effective zero trust strategy implementation across the Federal Government enterprise.

- Section 4 provides a range of recommendations on how the U.S. Government can positively influence and incentivize zero trust adoption for non-federal entities, including state, local, tribal, and territorial and critical infrastructure communities.

Summary of Key Conclusions

- The U.S. Government should be applauded for its strategic emphasis on adopting zero trust as a transformative approach to cybersecurity. Having the highest levels of Government, including by Presidential EO, acknowledge zero trust is critical to raise awareness and accelerate adoption of its principles, both within federal agencies and across the broader national ecosystem.

- Current U.S. Government policies such as the Federal Zero Trust Strategy[3] are well grounded in industry best practices but deliberately restrained in scope to cover directed actions over just a 2½-year period. This short-term focus is appropriate, as many federal agencies are early in their zero trust journeys and need to be accountable to concrete, short-term actions to build momentum.

- However, absent additional significant action, the U.S. Government risks zero trust becoming an incomplete experiment—a collection of disjointed technical security projects measured in years—rather than the foundation of an enduring, coherent, and transformative strategy measured in decades.

- To realize zero trust as a true strategy that meaningfully transforms cybersecurity outcomes over the next decade and beyond, the U.S. Government must take a series of policy actions now to institutionalize a culture of zero trust. Zero trust principles must be fully integrated into existing and new federal governance structures, policies, and programs and not be viewed as a standalone initiative.

Summary of Recommendations

Current and future Administrations must view the federal zero trust transition as a national imperative and as such, put the required leadership prioritization, funding, and accountability mechanisms in place to sustain a whole-of-government commitment over the next decade. Toward that goal, NSTAC makes 14 recommendations,

[3] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

shown in Table 1. Nine key recommendations (shown in bold) fall across the different areas of focus, and NSTAC suggests prioritizing these recommended actions.

Table 1: Zero Trust Report Recommendations at a Glance, with Key Recommendations Identified

Category	Recommendations	
3. Addressing Barriers and Enablers to Federal Government Zero Trust Strategy Implementation	3.1 Address Oversight and Establish Maturity Metrics	3.1.1. **Enhance Accountability with Progress Metrics for Zero Trust Strategy Implementation**
		3.1.2. **Enhance Transparency and Support Continuous Improvement with a Progress Metric**
		3.1.3. **Establish a Working Group to Develop Zero Trust Maturity Models for Key Federal Enterprise Infrastructure Services**
	3.2 Address Governance Barriers and Enablers for a Sustained Federal Commitment to Zero Trust	3.2.1 Incorporate Zero Trust Principles into Federal Cybersecurity Policies ▪ **Clarify the Alignment Between Zero Trust Strategy and FISMA Requirements** ▪ Automate FISMA Compliance Tasks
		3.2.2 Incorporate Zero Trust Practices into Federal Cybersecurity Programs ▪ Leverage CISA Cybersecurity Division Programs and Services ▪ Clearly Align CISA's Continuous Diagnostics and Mitigation Program with Zero Trust ▪ **Establish a Civilian Zero Trust Program Office** ▪ **Prioritize Creating a CISA Shared Security Service for Internet-Accessible Asset Discovery** ▪ Establish Synergy Between the Proposed Civilian and Defense Zero Trust Program Offices
		3.2.3. Incorporate Zero Trust Practices into Federal Cybersecurity Budget and Procurement Processes ▪ Broaden the Scope of Acquisition Vehicles ▪ Encourage Departments and Agencies to Identify Additional Funding for Zero Trust ▪ Communicate Anticipated Federal Technology Procurements that Support Zero Trust
	3.3. Address Technology Barriers and Enablers for a Sustained Federal Commitment to Zero Trust	3.3.1. **Assess Zero Trust Ecosystem Technology Interoperability in a Special Publication**
		3.3.2. Encourage Cloud Adoption
		3.3.3 Explore New Trusted Identity Methods
4. Energizing the Federal Government Role in Incentivizing	4.1. Raise and Sustain Public Awareness	
	4.2. **Develop and Mature Standards and Guidelines, including Internationally**	
	4.3. **Incentivize Zero Trust in Federal Grants Funding for IT Security Modernization**	
	4.4. Consider Federal Procurement Preferences for Zero Trust Alignment	

Category	Recommendations
Non-Federal Zero Trust Adoption	4.5. Consider Regulatory Relief Actions

Details of the Nine Key Recommendations

1. **Enhance Accountability for Measuring Federal Zero Trust Progress**: The Federal Chief Information Security Officer (CISO), working in close coordination with the National Cyber Director, should establish or enhance existing metric-based reporting requirements tied to industry best practices for zero trust implementation (see Section 2, Table 5 and Table 6) with reporting accountability at the agency CISO-level or above. (See Section 3.1.1)

2. **Enhance Transparency for Federal Zero Trust Progress**: The Federal Government must commit to transparency in documenting lessons learned in their zero trust journey, to both foster a culture of continuous improvement within government and to educate the broader national ecosystem. The Office of Management and Budget (OMB) should require agencies to publish at least one zero trust use case annually, documenting implementation lessons learned. OMB, in conjunction with the National Institute of Standards and Technology (NIST), should convene an annual working group to review use cases, and as appropriate, update existing federal zero trust guidelines and standards accordingly. (See Section 3.1.2)

3. **Develop Zero Trust Maturity Models for Key Federal Enterprise Infrastructure Services**: OMB, working through the Federal CISO Council, should undertake a comprehensive process to identify enterprise infrastructure services that are currently ubiquitous across federal agencies and likely to continue to be for at least the next 5 years. Once identified, the Federal CISO Council should establish an interagency working group to create corresponding Zero Trust Maturity Models for how to protect each service, modeled after the Zero Trust Maturity Model use case NSTAC created for Directory Services (e.g., Active Directory) in Appendix B. (See Section 3.1.3)

4. **Align Zero Trust Principles to Key Governance and Compliance Frameworks**: OMB should issue a memo clarifying the strategic alignment between the principles of the Zero Trust Strategy[4] and agency compliance requirements under the Federal Information Security Management Act (FISMA)[5] and its related standard *NIST 800-53: Security Controls for Information Systems and Organizations.*[6] Further, OMB should task NIST with producing a special publication mapping zero trust to the security controls of NIST SP-800-53,[7] to help

[4] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[5] U.S. Congress, Federal Information Security Management Act of 2002, March 2002, https://www.congress.gov/bill/107th-congress/house-bill/3844.

[6] National Institute of Standards and Technology (NIST), *Special Publication (SP) 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*, September 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[7] Ibid.

agencies avoid seeing a conflict between their regular compliance obligations and pursuit of long-term transformation through zero trust adoption. (See Section 3.2.1)

5. **Establish a Civilian Zero Trust Program Office**: The Cybersecurity and Infrastructure Security Agency (CISA) should establish a dedicated Zero Trust Program Office for federal civilian agencies to host implementation guidance, reference architectures, capability catalogs, training modules, and generally serve as a civilian government knowledge management center of excellence for zero trust. To the extent practicable, the proposed civilian Program Office should coordinate and share best practices with the recently established Department of Defense Zero Trust Program Office. (See Section 3.2.2)

6. **Create a CISA Zero Trust Shared Security Service for Internet-Accessible Asset Discovery**: CISA should clarify how its existing shared service technology offerings can help agencies achieve zero trust. Further, CISA should establish a new shared service offering to help agencies develop a "Complete understanding of their Internet-accessible assets," a foundational capability for any entity beginning to implement zero trust, as explicitly highlighted in the Federal Zero Trust Strategy.[8] (See Section 3.2.2)

7. **Assess Zero Trust Ecosystem Technology Interoperability**: NIST, as an extension of their existing zero trust work in the National Cybersecurity Center of Excellence (NCCoE), should produce an assessment of technology interoperability strengths and weakness across the commercial, government, and open source zero trust technology solution ecosystem. This NIST publication should inform potential future policy action and investment targeted for enhancing commercial or open-source solutions to make zero trust architecture adoption more efficient. (See Section 3.3.1)

8. **Advance Zero Trust in International Standards Bodies**: The U.S. Government, led by NIST and in close partnership with industry partners, should start on a multi-year path to advance zero trust within international standards bodies. Continued maturity of current zero trust guidelines is vital; their evolution into consensus-based, broadly recognized international standards can be a foundational underpinning of a variety of U.S. Government policy actions to incentivize zero trust adoption nationally, as has been done with the NIST Cybersecurity Framework.[9] (See Section 4.2)

9. **Prioritize Zero Trust Adoption in Federal IT Modernization Grant Funding**: CISA should prioritize zero trust projects in its discretionary authority to award IT security modernization grants for states and localities. This opportunity is particularly acute in CISA's administration of the State and Local Cybersecurity Improvement Act[10] (part of the Infrastructure Investment and Jobs Act [IIJA][11]), under which they are due to distribute over $1 billion over the next 4 years (through 2026). The Secretaries of Transportation, Commerce, and Energy

---

[8] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[9] NIST, Cybersecurity Framework, Accessed January 25, 2022, https://www.nist.gov/cyberframework.

[10] U.S. Congress, State and Local Cybersecurity Improvement Act, July 2021, https://www.congress.gov/bill/117th-congress/house-bill/3138.

[11] U.S. Congress, Infrastructure Investment and Jobs Act, June 2021, https://www.congress.gov/bill/117th-congress/house-bill/3684.

also have discretionary authority under the IIJA[12] to require funding recipients to demonstrate "sound cybersecurity practices" as a condition of receiving funds under their areas of jurisdiction. They should exercise this authority to incentivize adoption of zero trust principles, as appropriate. (See Section 4.3)

[12] U.S. Congress, Infrastructure Investment and Jobs Act, June 2021, https://www.congress.gov/bill/117th-congress/house-bill/3684.

1. Introduction to Zero Trust and the U.S. Federal Government's Zero Trust Strategy

1.1. History of Zero Trust and Foundational Principles

Zero Trust is a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified.

Zero Trust was born in 2008, when John Kindervag at Forrester Research developed the earliest conceptions. At the time, network perimeter-based security approaches were dominated by a trust model, which designated the external interface of a traditional legacy firewall as "untrusted" and the internally facing interface as "trusted." Kindervag began to recognize this trust model as a fundamental cause of many data breaches and concluded that security controls needed to be more granular and decoupled from the concept of trust. After two years of primary research, Kindervag published the first report on Zero Trust: *"No More Chewy Centers: Introducing the Zero Trust Model of Information Security"* in September 2010.[13]

In the years since, different definitions for Zero Trust have been proposed, though most remain tightly anchored to the original security principles of comprehensive visibility, least privilege access, and continuous risk-based evaluation and authentication. In addition, an entire ecosystem of models and tools have emerged around the Zero Trust concept. Numerous reference architectures have been created that map the core principles to security capabilities and specific technologies to achieve Zero Trust outcomes. New tools to assist in design, conceptualization and implementation of Zero Trust have also been created. Many of these models have now been widely validated through years of industry and government implementation. Section 2 explores some of these models as vital resources that can help federal agencies institutionalize Zero Trust principles within their own organizational security culture.

1.2. Zero Trust and the Federal Government's Cybersecurity Strategy

While the initial concept of Zero Trust was created over a decade ago, the federal government's Zero Trust journey—at least from a strategic policy perspective—remains in its infancy.

Certainly, many federal government cybersecurity practitioners have for several years implemented discrete projects and network defense strategies underpinned by the tenets of Zero Trust. As early as 2018, the White

[13] John Kindervag, *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*, September 14, 2010, Updated September 17, 2010, https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf.

House's Federal Chief Information Officer Council established a dedicated working group to work with the National Institute of Standards and Technology (NIST) on preliminary standards development for Zero Trust.[14]

Multiple department and agency-specific cybersecurity documents articulate the importance of adopting a Zero Trust mindset and a desire to apply its principles to their organization's cybersecurity strategy. Recent efforts to publicly articulate the Federal Government's views on Zero Trust and develop a common lexicon include the *NIST Special Publication (SP) 800-207: Zero Trust Architecture*[15] (2020) and the *Department of Defense (DoD) Zero Trust Reference Architecture*[16] (2021).

With the May 2021 *Executive Order (EO) 14028: Improving the Nation's Cybersecurity*,[17] the U.S. Government formally embraced Zero Trust as a true federal-government-wide cybersecurity priority. EO 14028 kicked off a series of interagency policy actions that fortified Zero Trust as a bona fide federal strategy, complete with accountability timelines, metrics to measure progress and maturity, and a recognized need to align Zero Trust initiatives with budgetary cycles and existing procurement vehicles. The January 2022 *National Security Memorandum 8 (NSM-8): Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* underscored that the requirements of EO 14028 apply to National Security Systems as well.[18]

Additional policy documents, such as the Federal Zero Trust Strategy, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, [19] (2022) and the draft CISA *Zero Trust Maturity Model*[20] (2021), have made clear that the U.S. Government sees Zero Trust as not just an important concept but as a foundational framework of the U.S. Government's cybersecurity strategy going forward. Zero Trust principles appear likely to guide the U.S. Government adoption and deployment of new technologies across the full landscape of devices and systems, including information technology, the Internet of Things, operational technology, cloud, containers, and mobile environments (including fifth generation [5G] and sixth generation [6G] communications) in the years and decades to come.

---

[14] Sylvia Burns, Federal Deposit Insurance Corporation, "NSTAC ZT-IdM Subcommittee Briefing," Briefing to the NSTAC Zero Trust and Trusted Identity Management (ZT-IdM) Subcommittee. Arlington, VA, October 13, 2021.

[15] NIST, SP 800-207: Zero Trust Architecture, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final.

[16] Department of Defense (DoD), *Zero Trust Reference Architecture*, February 2021, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf.

[17] *EO 14028: Improving the Nation's Cybersecurity*, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[18] *National Security Memorandum 8 (NSM-8): Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, The White House, January 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems.

[19] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[20] Cybersecurity and Infrastructure Security Agency (CISA), *Zero Trust Maturity Model* (draft), June 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

Table 2: U.S. Government Zero Trust Guideline Comparison

Federal Guideline/Policy	Scope/Purpose	Zero Trust Definition	Pillars/Tenets of Zero Trust Architecture
NIST SP 800-207: Zero Trust Architecture[21] (August 2020)	The basis for which many other federal zero trust guidelines rely upon, it provides the definition and framework for the key tenets of Zero Trust Architecture, as well as a roadmap to migrate and deploy zero trust security concepts to an enterprise environment.	"A cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated."	**Tenets** 1. All data sources and computing services are resources. 2. All communication is secured. 3. Access to resources is granted on a per-session basis. 4. Access to resources is determined by dynamic policy. 5. All assets are monitored and measured by the enterprise. 6. All authentication and authorization are dynamic and strictly enforced before access. 7. Information about assets, network infrastructure and communications is collected and used to improve security.
Department of Defense Zero Trust Reference Architecture[22] (February 2021)	Describes potential security features and architectural controls that DoD plans to execute across its systems to advance its information network to an interoperable zero trust end state.	Adapted from NIST SP 800-207[23]: "An evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."	**Pillars** 1. User 2. Device 3. Network/Environment 4. Applications and Workload 5. Data 6. Visibility and Analytics 7. Automation and Orchestration
National Security Agency (NSA), *Embracing a Zero Trust Security Model*[24] (February 2021)	Explains the zero trust security model and its benefits, as well as challenges for implementation, with the hope of assisting those seeking a zero trust security model.	"A security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries."	**Tenets** 1. Never trust, always verify. 2. Assume breach. 3. Verify explicitly.

[21] NIST, *SP 800-207: Zero Trust Architecture*, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final.

[22] DoD, Zero Trust Reference Architecture, February 2021, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf.

[23] NIST, *SP 800-207: Zero Trust Architecture*, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final.

[24] National Security Agency (NSA), Embracing a Zero Trust Security Model, February 2021, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

Federal Guideline/Policy	Scope/Purpose	Zero Trust Definition	Pillars/Tenets of Zero Trust Architecture
CISA *Zero Trust Maturity Model*[25] (June 2021, pre-decisional draft)	Assists federal agencies with their zero trust migration plans and provides an overview of the zero trust pillars and how agencies may mature their deployments from "Traditional" to "Advanced" and "Optimal" states.	Adapted from NIST SP 800-207[26]: "Zero Trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."	**Pillars** 1. Identity 2. Device 3. Network/Environment 4. Applications and Workload 5. Data **Additional Cross-Cutting Foundational Elements:** ▪ Visibility and Analytics ▪ Automation and Orchestration ▪ Governance
OMB Federal Zero Trust Strategy: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles[27] (January 2022)	Puts federal agencies on a common roadmap for Zero Trust Architecture, requiring agencies to meet specific cybersecurity objectives to achieve zero trust security goals by the end of Fiscal Year (FY) 2024.	Uses DoD Zero Trust Reference Architecture tenet: "The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted."	**Pillars*** 1. Identity 2. Devices 3. Networks 4. Applications and Workloads 5. Data *Cross-references the CISA five pillars that underpin the Zero Trust Maturity Model

The National Security Telecommunications Advisory Committee (NSTAC) believes that zero trust, if strategically and effectively implemented, has the potential to be transformative for the critical national security, public safety, and citizen services that require a secure and resilient U.S. government. Achieving zero trust will not be a static achievement with a single finish line. Instead, zero trust will be a continuous journey that will evolve with changes to both the technology and threat landscape. Ensuring this whole-of-government zero trust journey is ultimately measured in years and decades, not months, will require a tremendous and sustained commitment of leadership, personnel, and resources.

As many federal agencies remain in the early stages of their zero trust implementation, the U.S. Government has a vital opportunity to lay the foundation of an enduring Zero Trust strategic framework. Critically, this is an opportunity to avoid the implementation failures of cybersecurity strategies of the past—when siloed security technologies led to manual integration, increased management complexity, and ultimately, less effective cybersecurity. This opportunity—and responsibility— for the U.S. Government extends to both the federal

[25] CISA, *Zero Trust Maturity Model* (draft), June 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

[26] NIST, *SP 800-207: Zero Trust Architecture*, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

[27] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

enterprise (by directly influencing implementation) and the broader national ecosystem (by fostering greater zero trust adoption through example and appropriate policy incentives).

NSTAC is uniquely positioned to support this effort, based on years of practical experience implementing zero trust within member organizations and in customer and partner environments. Working in true public-private partnership will help avoid legacy security strategy pitfalls and realize zero trust's full potential to shape a safer and more secure future.

2. Industry Standards and Best Practices for Zero Trust Implementation

Section 1 discussed the history of zero trust and how the initial 2010 concept evolved into an overarching, comprehensive cybersecurity strategy embraced by the Federal Government. Countless organizations have begun successful zero trust journeys—often starting with small projects to protect specific assets before maturing and scaling zero trust deployments across their enterprise as part of a comprehensive risk management strategy.

Zero trust is a journey of continuous refinement. Along the road to maturity, organizations are likely to have made many costly mistakes and learned valuable lessons. This collective experience has helped establish several industry best practices for zero trust design and deployment. Examples of industry-developed models, including the Five-Step Process for Zero Trust Implementation and the *Zero Trust Maturity Model*[28] introduced in this section, are valuable tools for federal entities beginning or advancing their zero trust journey.

However, some federal agencies (and many private sector organizations) lack basic visibility of the data, assets, applications, and services in their organization, and as a result, are not yet ready to begin their zero trust journey. A fundamental prerequisite to zero trust is a comprehensive understanding of critical systems and their exposures to determine where to enforce zero trust policies in a risk-prioritized manner. The Cybersecurity and Infrastructure Security Agency (CISA) can empower civilian agency zero trust implementation through a shared services offering for this type of internet-accessible asset discovery capability, which Section 3 explores in greater detail.

2.1. Industry-Developed Models for Zero Trust Implementation

Before discussing these models, we first need to introduce a few foundational concepts, building on the Zero Trust definitions and key tenets introduced in Table 2. Table 3, below, identifies and defines these key concepts.

[28] John Kindervag, ON2IT BV, "NSTAC ZT Briefing," Briefing to the NSTAC (ZT-IdM) Subcommittee. Arlington, VA, September 8, 2021.

Table 3: Key Zero Trust Foundational Concepts and Definitions

Key Concept	Definition
Protect Surface	The area that the zero trust policy protects. ▪ Each protect surface contains a single data, applications, assets, and services (DAAS) element. ▪ Each zero trust environment will have multiple protect surfaces.

Data, Applications, Assets, and Services (DAAS)	The sensitive resources that go into individual protect surfaces.
	▪ **Data** – The sensitive data that poses the greatest risk if exfiltrated or misused.
	  o Examples include payment card information, protected health information, personally identifiable information, and intellectual property.
	  o In the government context, this also includes Classified Information, National Security Information, and Controlled Unclassified Information.
	▪ **Applications** – The applications that use sensitive data or control critical assets.
	▪ **Assets** – The assets, including an organization's information technology (IT), operational technology (OT), or Internet of Things devices.
	▪ **Services** – The services an organization most depends on.
	  o Examples include Domain Name System, Dynamic Host Configuration Protocol, Directory Services, Network Time Protocol, and customized Application Programming Interfaces.

Kipling Method Policy	A method for Zero Trust policy creation.
	▪ A Layer 7 (application) technology determines what traffic can transit the micro-perimeter at any point in time and prevents unauthorized access to the defined protect surface.
	▪ Describes the Who, What, When, Where, Why, and How of resource access:
	  o **Who** should be allowed to access a resource?
	  o **What** application is the asserted identity allowed to use to access the resource?
	  o **When** is the asserted identity allowed to access the resource?
	  o **Where** is the resource located?
	  o **Why** is the user (the Who) allowed to access the resource?
	  o **How** should traffic be processed as it accesses a resource?

Zero Trust Architecture	The tools and technologies deployed to build and maintain a zero trust environment. ▪ Conceived on a "per protect surface" basis. ▪ Designed from the inside out, starting at the protect surface and moving outwards.
Zero Trust Environment	The place where zero trust controls and policies are deployed. ▪ Can contain multiple protect surfaces ▪ Can include traditional on-premises networks such as data centers, public clouds, private clouds, on endpoints, or across a software-defined network.

2.1.1. *Five-Step Process for Zero Trust Implementation*

The first zero trust networks needed a new design paradigm to scale their implementation. The scope of zero trust can be large and all-encompassing, so breaking the process into smaller and more manageable components is important. The Five-Step Process for Zero Trust Implementation[29] accomplishes this (Figure 1).

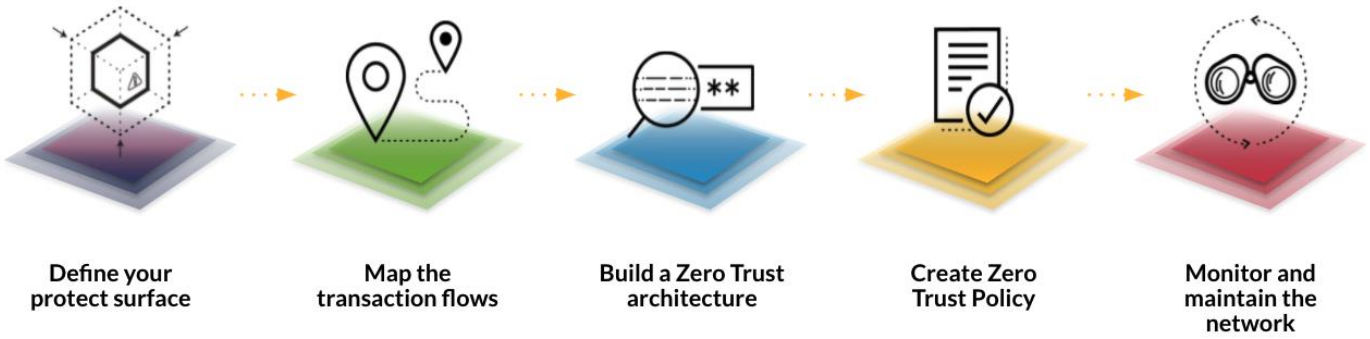

Figure 1: Five-Step Process for Zero Trust Implementation[30]

These implementation steps are designed to be flexible, repeatable, and technology agnostic. This process allows an organization to start with a small, bounded initial protect surface (or set of DAAS elements), work through the rest of the steps with that initial protect surface to establish their approach, and then add additional protect surfaces as their zero trust strategy matures and expands. Table 4 specifies the activities in each of the five steps.

Table 4: Five-Step Process for Zero Trust Implementation[31]

Step	Activities
1. Define the Protect Surface	Identify the DAAS elements to protect (i.e., the protect surface).
2. Map the Transaction Flows	Understand how the networks work by mapping the transaction flows to and from the protect surface, including how various DAAS components interact with other resources on the network. These transaction flows directly inform where to place proper controls.
3. Build a Zero Trust Architecture	Design your zero trust architecture, tailored to the protect surface(s) determined in steps 1 and 2. The way traffic moves across the network specific to the data in the protect surface should determine the design. The architectural elements cannot be predetermined, though a good rule of thumb is to place the controls as close as possible to the protect surface.
4. Create a Zero Trust Policy	Instantiate zero trust as a Layer 7 (application) policy statement. Use the Kipling Method of zero trust policy writing to determine who or what can access your protect surface. Consider both person and non-person entities.

[29] John Kindervag, ON2IT BV, "NSTAC ZT Briefing," Briefing to the NSTAC (ZT-IdM) Subcommittee. Arlington, VA, September 8, 2021.

[30] Ibid.

[31] Ibid.

Step	Activities
5. Monitor and Maintain the Network	Inspect and log all traffic, all the way through Layer 7 (application). The telemetry from this process helps prevent significant cybersecurity events and provides valuable security improvement insights over the long term. As a result, each subsequent protect surface can become more robust and better protected over time.

2.1.2. Zero Trust Maturity Model

Because zero trust is a process of continuous improvement, progress is best measured through the framework of a maturity model. The draft CISA *Zero Trust Maturity Model*[32] frames progress in this manner, referencing many common industry best practices.

Appendix A includes an example of one type of industry-developed *zero trust maturity model*, directly mapped to the Five-Step Process for Implementing Zero Trust.[33] This framework measures the maturity of an individual protect surface, containing a single DAAS element, at five levels of maturity: Initial, Repeatable, Defined, Managed, and Optimized.

2.2. Industry-Developed Technology Capabilities to Enable Zero Trust

In addition to the industry-developed models to support implementation and assess maturity that Section 2.1 introduced, private sector technology innovation has helped lead the way for zero trust-enabling security capabilities. Industry-led developments such as domain- and platform-agnostic zero trust security models and concepts (e.g., least privilege, risk-graded, adaptive security, and micro-segmentation) have paved the way for the U.S. Government's zero trust transition. Furthermore, recent advances in artificial intelligence and machine learning-augmented multi-source data fusion, real-time monitoring, behavioral analytics, and security orchestration and automated response tools offer additional, vital building blocks for enterprise-scale, risk-adaptive, and hopefully future-threat-resistant zero trust solutions.

In developing this report, several industry representatives briefed NSTAC on their employment of zero trust. For example, the NSTAC heard about how 5G networks are incorporating elements of zero trust, including the following:

- Encryption across the radio, transport and core segments of the network for both administrative traffic and applications.
- Using micro-segmentation.

[32] CISA, *Zero Trust Maturity Model* (draft), June 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

[33] John Kindervag, ON2IT BV, "NSTAC ZT Briefing," Briefing to the NSTAC Zero Trust – Identity Management Subcommittee. Arlington, VA, September 8, 2021.

- Running 5G network functions as applications in a cloud environment with unique security controls.
- Using strong authentication and identity management leveraging encryption not available in prior general cellular networks.
- Enhanced diagnostics, logging, threat analytics, and mitigation capabilities through concepts such as mobile edge computing.
- Strict data access policies.

These techniques are consistent with many of the principles in CISA's draft *Zero Trust Maturity Model*[34] and NIST 800-207.[35] These 5G applications are only one example of how critical infrastructure is incorporating zero trust. Other sectors and portions of communications networks are incorporating similar concepts and security technology capabilities.

However, in discussing the role of technology in enabling zero trust outcomes, the NSTAC is intentionally choosing to not advocate for particular security technologies. Zero trust should be realized as a true strategy that evolves over a long-term horizon, not merely a few years. Considering that, advocating for the latest specific zero trust-enabling technology would be a short-sighted endeavor.

However, there is also distinct need to more concretely articulate how zero trust principles translate to security capability imperatives and even classes of technologies. To accomplish this, the NSTAC evaluated industry best practices for protecting one enterprise infrastructure use case, Directory Services (e.g., Active Directory), leveraging the industry-developed *Zero Trust Maturity Model* introduced as Appendix A. Directory Services was chosen specifically because it is a core enterprise service, common to nearly all federal agencies and likely to persist for at least the next decade. Directory Services also has the benefit of being a service that straddles the line of both legacy and modern needs. Appendix B presents this use case.

This example can help federal agencies conceptualize how zero trust principles can become concrete actions that achieve increasing levels of measurable security maturity, including actions they are tasked to accomplish by the Federal Zero Trust Strategy.[36] This NSTAC report describes maturity in terms of security outcomes, not the specific technologies needed to achieve those outcomes, because those underlying technology solutions will evolve significantly over time. The NSTAC recommends that the Office of Management and Budget (OMB) undertake a comprehensive process to create additional Zero Trust Maturity Models for other key enterprise infrastructure services, a recommendation we highlight in more detail below in Section 3.1.3.

---

[34] CISA, *Zero Trust Maturity Model* (draft), June 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

[35] NIST, *SP 800-207: Zero Trust Architecture*, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final.

[36] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

3. Addressing Barriers and Enablers to Federal Government Zero Trust Strategy Implementation

3.1. Address Oversight and Establish Maturity Metrics

3.1.1. Enhance Accountability with Progress Metrics for Zero Trust Strategy Implementation

Section 2, Appendix A, and Appendix B included definitions of zero trust architectures in their most mature and fully realized form. These mature definitions may have a more limited utility as practical near-term recommendations for agencies implementing the short-term actions described in the Zero Trust Strategy (which is intentionally restrained in scope to a period of just 2½ years, through the conclusion of FY2024).

The reality is that federal departments and agencies are in dramatically different phases of maturity in their zero trust deployments. Some have well-defined zero trust reference architectures mapped to specific security controls and well-developed governance constructs to accelerate adoption across their enterprises. Other federal entities, burdened by legacy infrastructure built on the prior concept of implicit trust, lack some of the basic network and asset visibility necessary to even begin implementing a zero trust-focused project in the near term. The zero trust journey – beginning or maturing – has no one-size-fits-all approach.

To its credit, two of the U.S. Government's foundational policy documents, the Federal Zero Trust Strategy[37] and the draft CISA *Zero Trust Maturity Model*,[38] are clear-eyed about this reality. In its first pages, the Federal Strategy acknowledges this, characterizing the strategy as "a starting point, not a comprehensive guide to a fully mature zero trust architecture."

The Federal Zero Trust Strategy[39] goes on to describe a series of actions agencies must take between now and the end of FY2024, which concludes on September 30, 2024. These specific and concrete actions are identified across each of the five zero trust pillars (Identity, Devices, Networks, Applications and Workloads, and Data). For example, the Applications pillar states, "Agencies must identify at least one internal-facing FISMA Moderate application and make it fully operational and accessible over the public internet."

This level of specificity is important and necessary to fulfill the Federal Zero Trust Strategy's[40] apparent goal: jump-starting agencies' zero trust efforts through quick wins to build momentum. But achievement of those action-oriented goals alone should not be considered the sole measure of success. Over-focusing on near-term tactical goals can distract from the big-picture cultural shift that zero trust requires for long-term, sustained

---

[37] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[38] CISA, *Zero Trust Maturity Model* (draft), June 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

[39] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[40] Ibid.

impact. This is especially true given the broad maturity spectrum across federal agencies. For some, the Federal Zero Trust Strategy's[41] technical goals are easily or already achieved; for others, their achievement is a significant stretch.

This report, looking to the longer term, is not focused on commenting on the technical ambition of the Federal Zero Trust Strategy's[42] actions for the next 2½ years. The Strategy is clear in its intent; it doesn't endeavor to describe actions that would get agencies to fully mature zero trust architectures. But NSTAC is charged to make recommendations with a long-term perspective. As such, the recommendations in Section 3 largely focus on actions that can be taken to sustain zero trust as a federal cyber strategy well beyond the 2½-year time horizon. Actions taken now can both foster short-term achievement and institutionalize organizational cultural habits as building blocks for long-term transformation.

To that end, rather than propose technical success metrics, NSTAC strongly encourages federal agencies to reference the industry best-practice models in Section 2. These process-oriented principles, if firmly rooted in federal organizations after 2½ years, will be the best predictor of long-term success and sustained commitment to zero trust. Most relevant is the Five-Step Process for Zero Trust Implementation[43] model. Table 5, below, maps the implementation steps to specific actions and quantifiable progress metrics; NSTAC recommends that the Federal Chief Information Security Officer (CISO), working in coordination with the National Cyber Director (NCD), establish reporting requirements tied to these metrics for sustained accountability at the agency CISO-level or above.

Table 5: Five-Step Process for Zero Trust Implementation with Suggested Quantifiable Progress Metrics

Step	Activities	Quantifiable Progress Metric- Reporting Requirements
1. Define the Protect Surface	Identify DAAS elements to protect (i.e., the protect surface).	▪ Organizational inventory of total DAAS elements (protect surfaces) on the agency roadmap for future Zero Trust deployments
2. Map the Transaction Flows	Understand how the networks work by mapping the transaction flows to and from the protect surface, including how various DAAS components interact with other resources on the network. These transaction flows directly inform where to place proper controls	▪ Percentage of instrumented and validated traffic flows (as a function of total traffic flows)

[41] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[42] Ibid.

[43] John Kindervag, ON2IT BV, "NSTAC ZT Briefing," Briefing to the NSTAC Zero Trust – Identity Management Subcommittee. Arlington, VA, September 8, 2021.

Step	Activities	Quantifiable Progress Metric- Reporting Requirements
3. Build a Zero Trust Architecture	Design your zero trust architecture, tailored to the protect surface(s) determined in steps 1 and 2. The way traffic moves across the network specific to the data in the protect surface should determine the design. The architectural elements cannot be predetermined, though a good rule of thumb is to place the controls as close as possible to the protect surface.	▪ Percentage of DAAS elements (as a function of the total) that an enforcement point protects
4. Create a Zero Trust policy	Instantiate zero trust as a Layer 7 (application) policy statement. Use the Kipling Method of zero trust policy writing to determine who or what can access your protect surface. Consider both person and non-person entities.	▪ Percentage of DAAS elements (as a function of the total) that a defined zero trust policy protects
5. Monitor and Maintain the Environment	Inspect and log all traffic, all the way through Layer 7 (application). The telemetry from this process helps prevent significant cybersecurity events and provides valuable security improvement insights over the long-term. As a result, each subsequent protect surface can become more robust and better protected over time.	▪ Month-over-month true and false positive percentages for security incidents for zero trust deployments (to quantify efficacy and provide a closed feedback loop for zero trust technology and policy refinement)

3.1.2. Enhance Transparency and Support Continuous Improvement with a Progress Metric

In addition to these five implementation steps, NSTAC also believes the Federal Government should adopt an additional tenet: Commit to Transparency and Continuous Improvement. To lead by example, it is vital that the Federal Government's zero trust journey be as publicly transparent as possible. As agencies move through the five implementation steps, publicly documenting successes and lessons learned is critical to foster a culture of continuous improvement across public and private sector organizations in their zero trust journeys. To reinforce this ethos, NSTAC recommends OMB establish an additional reporting metric, requiring each agency to publish one Zero Trust use case annually, documenting implementation lessons learned (Table 6). In addition, OMB, working in conjunction with NIST, should convene an annual working group to review use case studies, and as appropriate, update existing zero trust guidelines and best practice standards accordingly.

Table 6: Additional Tenet with Suggested Quantifiable Progress Metric

Tenet	Activities	Quantifiable Progress Metric
Commit to Transparency and Continuous Improvement	Publicly document successes and lessons learned	▪ Document lessons learned in at least one zero trust use case (published annually)

3.1.3. Establish a Working Group to Develop Zero Trust Maturity Models for Key Federal Enterprise Infrastructure Services

OMB can also play a vital role in assessing the most significant government-wide cybersecurity risks, to help agencies prioritize the assets most critical to protect with zero trust deployments. To this end, the NSTAC

recommends that OMB, working through the Federal CISO Council, undertake a comprehensive process to identify the federal enterprise infrastructure services that are:

1. Currently ubiquitous across federal agencies.

2. Likely to continue to be ubiquitous for at least the next five years.

Once these services are identified, the NSTAC recommends that OMB establish an interagency working group, facilitated through the Federal CISO Council, to create corresponding Zero Trust Maturity Models for each service. These Zero Trust Maturity Models template can be modeled after the Directory Services use case the NSTAC created and is featured in Appendix B.

3.2. Address Governance Barriers and Enablers for a Sustained Federal Commitment to Zero Trust

"Governance" encompasses all the systems by which an organization is controlled and operates, and the mechanisms by which it is held to account. In this report, this term describes all the budgetary, personnel, and accountability mechanisms that should be reformed or newly established to maintain zero trust as an integrated, sustained federal strategy over the long term.

Each individual agency is ultimately responsible for modernizing their own cybersecurity postures consistent with zero trust principles in furtherance of EO 14028.[44] However, the White House and those entities the EO tasks with aiding implementation must appropriately recognize the magnitude of this transformation challenge. Those implementing entities, including CISA and the General Services Administration (GSA), can take several concrete actions to assist and empower otherwise under-resourced agencies in implementing zero trust, discussed in the subsections below. Some of these recommended actions are acknowledged in the existing Federal Zero Trust Strategy,[45] and some are newly articulated in this report.

Ultimately, the key to successfully institutionalizing zero trust in the Federal Government is to keep it from being seen as just another new federal requirements by integrating its principles into existing workstreams. Zero trust principles should be cemented into the core of existing and new federal governance structures, policies, and programs. As the Federal Government adopts new technologies, modernizes or incrementally maintains systems, and adopts new information security policies, zero trust needs to be a central tenet for managing cybersecurity risk.

---

[44] *EO 14028: Improving the Nation's Cybersecurity*, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[45] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

3.2.1. Incorporate Zero Trust Principles into Federal Cybersecurity Policies

One of the most important ways to accelerate and institutionalize zero trust adoption across the Federal Government is to anchor its principles to existing and well-understood federal cybersecurity policies that agencies regularly interact with.

Clarify the Alignment Between Zero Trust Strategy and FISMA Requirements

Federal agencies have significant existing reporting responsibilities to demonstrate security compliance, most notably in alignment with the Federal Information Security Management Act (FISMA)[46] and its underlying standard NIST 800-53: Security Controls for Information Systems and Organizations.[47] FISMA[48] compliance requires a substantial level of effort and expense for agencies. Clearly mapping the required actions outlined in the Federal Zero Trust Strategy[49] to the controls of NIST 800-53[50] will demonstrate that these dual efforts are not in conflict, incentivizing a continued and institutionalized commitment to maturing zero trust deployments.

Absent the increased clarity of such a mapping, agencies may see zero trust risk management activities as unconnected to FISMA compliance requirements, the latter of which carries a much stronger incentive-driving potential of penalty. To address this, NSTAC recommends that OMB issue a memo clarifying the strategic alignment between the principles of the Zero Trust Strategy[51] and agency compliance requirements under FISMA.[52] Further, the NSTAC recommends that OMB task NIST with producing a special publication explicitly mapping zero trust principles to the security controls of NIST SP-800-53,[53] reducing any potential perceived barriers to an agency's pursuit of long-term transformation through zero trust adoption.

Automate FISMA Compliance Tasks

FISMA-related compliance tasks also need to be optimized and, in some cases, automated to enable the transition to zero trust. When agencies make fundamental changes in their environments (as happens often

---

[46] U.S. Congress, Federal Information Security Management Act of 2002 (FISMA), March 2002, https://www.congress.gov/bill/107th-congress/house-bill/3844.

[47] NIST, *SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*, September 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[48] U.S. Congress, FISMA, March 2002, https://www.congress.gov/bill/107th-congress/house-bill/3844

[49] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[50] NIST, *SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*, September 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[51] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[52] U.S. Congress, FISMA, March 2002, https://www.congress.gov/bill/107th-congress/house-bill/3844.

[53] NIST, SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations, September 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

during a zero trust transition), they are required by FISMA[54] to run through a cycle of tasks to assess and reauthorize systems to operate. Many agencies will struggle to keep up with these tasks in a legacy environment, which will further slow or limit their transition to zero trust. An increased emphasis on education and training around zero trust visibility, analytics, and orchestration tools could help agencies automate how they assess the health and risk posture of zero trust implementations to manage these ongoing FISMA[55] tasks. These training and education capabilities could be one type of service offered through the proposed Civilian Zero Trust Program Office, detailed further below.

3.2.2. Incorporate Zero Trust Practices into Federal Cybersecurity Technology Programs

Zero trust adoption can be further institutionalized by connecting its principles to well-understood federal cybersecurity programs that agencies regularly interact with and procure technologies from.

Leverage CISA Cybersecurity Division Programs and Services

For the civilian government, the CISA Cybersecurity Division plays a critical role in protecting the federal ".gov" domain. CISA offers a variety of programs and services that can be leveraged as shared services or vehicles for procuring technologies to enable zero trust outcomes. Examples include the Continuous Diagnostics and Mitigation (CDM) Program, Cybersecurity Quality Service Management Office (QSMO), Cybersecurity Assessments, Cybersecurity Training, High Value Asset Program, Threat Hunting, National Cybersecurity Protection System Program, and the Trusted Internet Connections Program.

Clearly Align CISA's Continuous Diagnostics and Mitigation Program with Zero Trust

The CDM program [56] deserves special attention. This program has, though its goal of implementing Information Security Continuous Monitoring (ISCM),[57] been the vehicle by which most federal agencies have procured and implemented core capabilities that help form a foundation for achieving zero trust. CDM is unique in that it represents both a program and a set of requirements that agencies must meet, so clear alignment between CDM and Zero Trust goals is critical.

The GSA Buyer's Guide, which explicitly maps Zero Trust principles to specific technologies available within federal procurement programs, including CDM, is a valuable asset for agencies to reference.[58] Federal government alignment of zero trust principles through well-known procurement vehicles like CDM can both improve federal cybersecurity posture and provide a beneficial model for state, local, tribal, and territorial governments who procure zero trust-enabling technologies off CDM schedules. Expanding this approach to map

---

[54] U.S. Congress, FISMA, March 2002, https://www.congress.gov/bill/107th-congress/house-bill/3844.

[55] U.S. Congress, FISMA, March 2002, https://www.congress.gov/bill/107th-congress/house-bill/3844.

[56] CISA, Continuous Diagnostics and Mitigation, Accessed January 25, 2022, https://www.cisa.gov/cdm.

[57] NIST, *SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf.

[58] Lawrence Hale and Justin Morgan, General Services Administration (GSA), "How GSA Can Help Agencies with Their ZTA Journey," Briefing to the NSTAC Zero Trust – Identity Management Subcommittee. Arlington, VA, October 13, 2021.

zero trust technologies with other major federal cybersecurity procurement programs would be similarly beneficial.

Establish a Civilian Zero Trust Program Office

CISA plays a vital role in empowering other federal civilian government organizations in implementing zero trust. From its administration of CDM to its management of the Trusted Internet Connections program,[59] many of CISA's major current initiatives strongly align to Zero Trust principles.

However, CISA's zero trust-relevant guidance and shared service offerings are not centrally located in a way that is conducive to civilian agency access. To address this, NSTAC recommends that CISA establish a dedicated Civilian Zero Trust Program Office. This Program Office would host zero trust implementation guidance, reference architectures, capability catalogs, playbooks, training modules, and generally serve as a civilian government knowledge management center of excellence.

Prioritize Creating a CISA Shared Security Service for Internet-Accessible Asset Discovery

The Civilian Zero Trust Program Office should also include a technology implementation function and be a common hub for CISA's shared service offerings relevant to zero trust implementation. For existing shared service offerings offered through QSMO, including Vulnerability Disclosure, Security Operations Services, and Protective Domain Names System services, CISA should clearly articulate how agencies can leverage these services to enable zero trust outcomes. New shared service offerings should also be established, especially to provide foundational capabilities necessary for under-resourced agencies early in their zero trust journey. One such example, Discovering Internet-Accessible Applications, should be prioritized. This service should provide continuous and dynamic asset mapping as static data pulls will have limited utility in a constantly evolving threat environment. The Federal Zero Trust Strategy[60] explicitly highlights this capability imperative:

> To effectively implement a zero trust architecture, an organization must have a complete understanding of its internet-accessible assets, so that it may apply security policies consistently and fully define and accommodate user workflows. In practice, it can be very challenging for a large, decentralized organization to track every asset reliably,
>
> For agencies to maintain a complete understanding of what internet-accessible attack surface they have, they must rely not only on their internal records, but also on external scans of their infrastructure from the internet. CISA will provide data about agencies' internet-accessible assets obtained through public and private sources. This will include performing scans of agencies' information technology infrastructure.

[59] CISA, Trusted Internet Connections, January 2022, https://www.cisa.gov/tic.

[60] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

Establish Synergy Between the Proposed Civilian and Defense Zero Trust Program Offices

The January 2022 *NSM-8: Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* requires that National Security Systems meet or exceed the requirements of the May 2021 *EO 14028: Improving the Nation's Cybersecurity,* including the zero trust requirements.[61]

The Department of Defense (DoD) has been aggressively implementing several programs over the last few years to deliver capabilities across the defense enterprise that are foundational to achieving the pillars identified in DoD's Zero Trust Architecture, released in February 2021. Such programs include Identity Credentialing and Access Management (ICAM) and Comply-to-Connect (C2C). ICAM provides the cybersecurity elements for access management and irrefutable identification across the DoD. C2C is a defense-wide requirement that stipulates that no device or application is granted network privileges until it complies with all DoD security requirements, including patch status, updates, proper configuration, and a host of other specific attributes. In 2019, private sector collaborators at DreamPort, a hub for testing and examining cyber products and services to advance capabilities of the cyber warfighter, leveraged these and other capabilities to instantiate a zero trust architecture that was subsequently deployed on a key DoD enclave.

In the fall of 2021, the DoD created a Zero Trust Program Office to manage the strategic defense enterprise-wide deployment of its zero trust program. A key priority of that office should be to closely align the zero trust activities of the military services with the DoD's zero trust goals. The Defense Information Systems Agency (DISA) will play a key central role providing enterprise services across the DoD to enable these zero trust capabilities and outcomes.

To the extent practicable, the proposed Civilian Zero Trust Program Office should coordinate closely with the Defense Zero Trust Program Office. Working in partnership and with key enabling entities, such as DISA and the CDM Program Office, coordination activities between the two offices could include:

1. Agreeing on a single set of zero trust pillars (Table 2 of this report shows some minimal disparity among stated pillars).

2. Establishing a common lexicon for zero trust goals and capabilities.

3. Agreeing on joint federal milestones for zero trust implementation.

4. Establishing a unified method to measure the maturity of department and agency zero trust implementations.

[61] *EO 14028: Improving the Nation's Cybersecurity*, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

3.2.3. Incorporate Zero Trust Practices into Federal Cybersecurity Budget and Procurement Processes

The governance process that supports annual program, planning, budgeting, and execution is key to embedding Zero Trust strategies in modernization funding needs when agencies and OMB formulate their budget requests. OMB should coordinate closely with the NCD during the budget formulation process to confirm that agencies' annual budget requests are sufficient to support their zero trust and overarching cybersecurity needs and objectives. Broadly speaking, the long-term horizon required to achieve zero trust maturity requires more flexible budgeting options that can support multi-year funding.

Broaden the Scope of Acquisition Vehicles

Federal acquisition vehicles are the primary approach to acquire subject matter expertise to perform information technology modernization projects in the Federal Government. The quality of the acquisition vehicle structure, associated scope, and statements of work are also key to rapidly advancing federal agencies to zero trust. NSTAC recommends that acquisition vehicle structures facilitate a wide-ranging scope to support zero trust, including strategy; planning; assessments; architecture; engineering; application modernization; data lifecycle management; continuous integration/continuous delivery; development, security, and operations (DevSecOps); operations and maintenance; and security operations and management.

Encourage Departments and Agencies to Identify Additional Funding for Zero Trust

Departments and agencies will continue to plan and request funding for their cybersecurity and zero trust needs within their own budget processes and receive support for procuring and deploying cybersecurity capabilities through centralized programs like CDM and centralized entities like the DISA for the defense enterprise. All agencies should also contemplate other funding sources that could accelerate implementation of their zero trust architectures. In particular, the Technology Modernization Fund (TMF) is a promising funding source for agencies' implementations of zero trust. TMF is an innovative funding vehicle, authorized by Section 4(a) of the Modernizing Government Technology (MGT) Act of 2017,[62] that gives agencies additional ways to quickly deliver services to the American public, better secure sensitive systems and data, and efficiently use taxpayer dollars. The MGT Act specifically authorized TMF to fund projects "for technology-related activities to improve information technology, and to enhance cybersecurity across the Federal Government."[63] In September 2021, nearly $60 million dollars in TMF funding was awarded to the Department of Education,[64] Office of Personnel Management,[65] and GSA[66] for zero trust-focused projects.

---

[62] U.S. Congress, Modernizing Government Technology (MGT) Act of 2017, May 2017, https://www.congress.gov/bill/115th-congress/house-bill/2227.

[63] Ibid.

[64] The TMF, Awarded Projects page: "Zero Trust Architecture," https://tmf.cio.gov/projects/#zero-trust-architecture.

[65] The TMF, Awarded Projects page: "Advancing Zero Trust," https://tmf.cio.gov/projects"/#advancing-zero-trust.

[66] The TMF, Awarded Projects page: "Zero Trust Networking," https://tmf.cio.gov/projects/#zero-trust-networking.

Communicate Anticipated Federal Technology Procurements that Support Zero Trust

To help industry better prepare, compete, and innovate to deliver the specific technologies that zero trust requires, both today and in the future, the U.S. Government must be more transparent and intentional about the specific technologies it intends to procure in the pursuit of its zero trust goals. Although it was not specifically focused on zero trust, *Cal-Secure*, the five-year information security maturity roadmap recently released by the State of California, is a representative example of a government entity concretely articulating its technology procurement needs. This document contains a "Horizon Map" with a roadmap of strategic cybersecurity initiatives and capabilities, arranged in priority order so state agencies can "build and operationalize each capability to increase maturity."[67] Emulating this degree of clarity and transparency around intended Federal Government procurements will help industry plan for and respond more efficiently to government technology requirements for zero trust.

3.3. Address Technology Barriers and Enablers for a Sustained Federal Commitment to Zero Trust

One byproduct of zero trust's rise in popularity is the emergence of a "noisy" private sector security market, with many vendors re-branding technologies to narrowly apply to one discrete function of a comprehensive zero trust architecture. While having more technologies gives the impression of greater flexibility, a proliferation of multiple solutions also increases management complexity, with the burden of manual integration too often placed on the end user. This end-user integration burden not only leads to security challenges, because it introduces friction and complexity into security architectures, but also leads to operational inefficiencies that disincentivize progressive zero trust adoption. For a more end-user-friendly experience, end-to-end integration is critical, where telemetry from endpoints, network, and cloud aggregate to inform automated zero trust policy enforcement based on comprehensive visibility.

As a strategic undertaking, zero trust is best approached with private industry partners who recognize it not as a single technology, but a comprehensive cybersecurity strategy achieved with the help of flexible and interoperable technologies. In other words, ideal private industry partners should be outcome-focused on end users successfully achieving holistic cybersecurity goals. End users (e.g., federal agencies) have a continuum of maturity across the zero trust pillars, focused on making incremental progress in successive iterations. Inflexible products, services, technologies, and vendors can prevent agencies from applying stronger user authentication, conducting better asset verification, implementing additional Protect Surfaces, or completing other steps necessary to increase zero trust maturity.

Componentized technologies that leverage and integrate with a customer's existing security technologies are more adaptable and conducive to realistic progress. To that end, it is incumbent on private industry to validate that their technologies natively integrate to address multiple pillars of a comprehensive zero trust architecture, or

[67] State of California, *Cal-Secure: State of California Executive Branch Multi-Year Information Security Maturity Roadmap 2021*, https://cdt.ca.gov/wp-content/uploads/2021/10/Cybersecurity_Strategy_Plan_FINAL.pdf.

otherwise effectively interoperate with a large enough ecosystem of technologies, to provide a friendly, end-user-centric experience.

3.3.1. Assess Zero Trust Ecosystem Technology Interoperability in a Special Publication

Zero trust security best practices such as least privilege enforcement, continuous access monitoring and verification, and micro-segmentation are already being implemented by many organizations within the U.S. Government and industry. However, the lack of interoperability-focused standards for zero trust technologies could negatively impact Zero Trust deployment efforts in the long term if not properly addressed. Existing zero trust guidelines such as NIST SP 800-207[68] provide the necessary high-level framework for deploying zero trust-based systems, but do not address the component-level interfaces needed to enable true plug-and-play of multi-vendor zero trust solutions. A lack of interoperability standards typically results in proprietary, closed solutions, vendor lock-in, increased complexity, and higher maintenance costs. It also risks preventing the U.S. Government and others from freely choosing and combining best-in-class zero trust technologies in an extensible, vendor-neutral, and more future-proof manner.

To address this, OMB should task NIST with exploring how component-level interface standardization could further improve interoperability between commercial, Government, and open source zero trust solutions. This is a natural extension of the existing work being executed by NIST's National Cybersecurity Center of Excellence (NCCoE) Zero Trust Architecture lab.[69]

NCCoE is currently producing a series of "practice guides"—reference architectures that demonstrate how to successfully integrate specific named cybersecurity technologies to meet industry-leading best practice standards for multiple zero trust use cases. Without endorsing particular products, the practice guides will highlight a set of technologies that have proven successful in achieving zero trust implementation and maturity. The practice guides will help federal and private sector organizations understand the key components of a zero trust architecture and prioritize their zero trust technology investments accordingly.

NIST's extensive work at the NCCoE to validate what "works" from a component integration standpoint gives NIST a uniquely valuable perspective on what isn't working—including specific areas where interoperability breaks down in the zero trust technology ecosystem, because of poor application programming interfaces (APIs) or for other reasons. These lessons learned should be documented in a NIST special publication to directly inform potential policy actions and investment to enhance the commercial or open-source technology interoperability ecosystem.

In light of the several taskings that this report recommends for NIST and the NCCoE, NSTAC strongly emphasizes the need for increased funding for NIST. NIST plays a vital role in advancing the U.S. Government's cybersecurity

---

[68] NIST, *SP 800-207: Zero Trust Architecture*, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final.

[69] Alper Kerman, and Scott Rose, National Institute of Standards and Technology, "ZTA; Implementing a ZTA," Briefing to the NSTAC Zero Trust – Identity Management Subcommittee. Arlington, VA, September 22, 2021.

best practices, including for zero trust, in close and direct partnership with industry expertise, but NIST"s budget for cybersecurity has not kept pace with the increased demand on its resources.

3.3.2. Encourage Cloud Adoption

Faster adoption of cloud services will significantly accelerate federal agencies' adoption of zero trust. Cloud-based architectures enable enterprises to:

1. More easily identify their DAAS; know where they are and who is accessing them; and restrict access according to their policies (i.e., define and monitor their protect surfaces).

2. Facilitate mapping transaction flows as well as implementing access controls and user and application segmentation.

3. Continuously inspect and log all traffic to identify anomalous activity and create and enforce policies, accordingly.

The promise of cloud services to enable zero trust implementation is appropriately acknowledged in *EO 14028: Improving the Nation's Cybersecurity*,[70] which includes several requirements and provisions to accelerate federal agencies' movement to secure cloud services. The Federal Zero Trust Strategy[71] similarly emphasizes the importance of cloud adoption to achieving zero trust.

This cloud modernization, to balance the U.S. Government's dependency on on-premises infrastructure and applications, is urgent. The COVID-19 pandemic revealed significant challenges in quickly scaling and securing remote workforces and highlighted the imperative of federal zero trust adoption, leveraging the cloud to help securely authenticate users outside traditional enterprise perimeter-based work environments.

3.3.3. Explore New Trusted Identity Management Methods

In its study tasking, NSTAC was asked to specifically review the role of trusted identity management systems in implementing zero trust.

Nearly every briefer emphasized the foundational importance of identity in implementing zero trust. In a 2021 survey of nearly 1,300 network security professionals, almost 43% of respondents identified "Identity and Access Management" as the first task to address as they begin to move to zero trust ("Network Security" placed second, at 20.8%).

NSTAC ultimately views identity as one pillar of a multi-pillar framework of a comprehensive zero trust architecture. U.S. Government policy documents, including the Federal Zero Trust Strategy, articulate this same

---

[70] *EO 14028: Improving the Nation's Cybersecurity*, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[71] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

position. But trusted identity management solutions are unquestionably foundational, as zero trust is based on a continuous cycle of credentialing, verifying, and authorizing identity for person and non-person entities.

Currently, the Federal Government remains too dependent on physical form factors of authentication, such as personal identity verification and common access cards. But these methods have significant operational challenges, as most require physical smart card readers, which mobile environments cannot accommodate. The Federal Government's strategic approach to identity must evolve, especially in the context of increasingly distributed and remote work environments where data and applications are accessed from a broad range of devices and locations.

Examples of newer or emerging forms of multi-factor identification include physical biometrics, behavioral biometrics, and user and entity behavior analytics authentication. Many of these approaches are detailed extensively in *NIST SP 800-63-3: Digital Identity Guidelines*,[72] of which a new revision is under development, estimated to be published in Fall 2022.

As the Federal Government contemplates new identity management solutions, they should also consider how to apply zero trust principles to protect core enterprise services (e.g., Directory Services) that play a fundamental role in managing digital identities and enforcing least privilege role-based access based on those identities (see the Directory Services Use Case in Appendix B).

4. Energizing the Federal Government Role in Incentivizing Non-Federal Zero Trust Adoption

In addition to its direct influence over how the Federal Zero Trust Strategy[73] is effectively implemented across federal entities, the U.S. Government has a significant capacity to influence zero trust architecture adoption across the broader national—and even international—cybersecurity ecosystem. It is imperative for the U.S. Government to exercise this responsibility to help raise the cybersecurity baseline for the state, local, tribal and territorial and critical infrastructure entities that underpin our collective national security and public safety.

The spectrum of policy tools available to the U.S. Government cover a broad range of "carrots and sticks," from public awareness campaigns to federal funding incentives to targeted regulatory action. Each has well-established models in other domains of cybersecurity best practice adoption to explore for their applicability to incentivizing zero trust adoption.

[72] NIST, "Roadmap: NIST SP 800-63-3: Digital Identity Guidelines," June 2017, https://www.nist.gov/identity-access-management/roadmap-nist-special-publication-800-63-3-digital-identity-guidelines.

[73] Ibid.

4.1. Raise and Sustain Public Awareness

One of the most basic, yet powerful, tools the U.S. Government possesses is its strategic messaging platform. This is especially true at the highest levels of Government, such as the White House, which have the capacity to fundamentally reshape national dialogues by virtue of the principles they strategically champion.

To that end, the U.S. Government should be applauded for the role they have already played in elevating the national conversation around zero trust. Zero trust's prominence in the May 2021 *EO 14028: Improving the Nation's Cybersecurity*,[74] was a game-changer in bringing more mainstream awareness to the concept. The likely effect this had on catalyzing or advancing zero trust conversations within boardrooms and among information security teams cannot be overstated.

The U.S. Government now has the responsibility to sustain that messaging cadence—to not just raise general awareness about zero trust, but to lead by example in defining meaningful implementation standards and best practices to transform the Nation's cybersecurity posture. This requires a steadfast commitment to delivering regular status updates on the federal Zero Trust Strategy,[75] with radical transparency about implementation successes and failures, as recommended above in Section 3.1, Table 6. This ongoing communication would send an important signal to the broader national cybersecurity ecosystem that zero trust is a journey of continuous maturity and not a static end state.

4.2. Develop and Mature Standards and Guidelines, Including Internationally

In the last few years, the U.S. Government has undertaken a series of efforts to produce guidelines to define the core components or pillars that constitute a zero trust architecture. Table 2 details representative examples: the *NIST SP 800-207: Zero Trust Architecture*,[76] the *Department of Defense Zero Trust Reference Architecture*,[77] NSA's *Embracing a Zero Trust Security Model*,[78] and the draft CISA *Zero Trust Maturity Model*.[79]

However, these zero trust guidelines, from a U.S. Government perspective, remain in relatively early stages of maturity. Guideline development work must continue to advance in partnership with industry expertise and in coordination with existing industry and international standards bodies. As one prominent example, zero trust principles should be advanced in relevant international information security standards, such as the International

---

[74] *EO 14028: Improving the Nation's Cybersecurity*, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[75] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[76] NIST, *SP 800-207: Zero Trust Architecture*, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final.

[77] Department of Defense (DoD), *Zero Trust Reference Architecture*, February 2021, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf.

[78] NSA, *Embracing a Zero Trust Security Model*, February 2021, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

[79] CISA, *Zero Trust Maturity Model* (draft), June 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 series developed by the ISO and IEC Joint Technical Committee (JTC 1) for Information Technology).[80]

Continued maturity of these guidelines is vital. Establishing consensus-based, broadly recognized zero trust standards (not just guidelines) is a foundational imperative for a variety of policy-based actions by which the U.S. Government could incentivize zero trust adoption. Many of these proposed policy actions, dependent on widely accepted and mature zero trust standards, are detailed below.

To address this need, the NSTAC recommends the U.S. Government, led by NIST and in close partnership with industry, should start on a multi-year path to help mature zero trust guidelines by:

- Developing proposed standards.
- Introducing those standards in international, consensus-based standards bodies.
- Pushing for the adoption of those standards.

These foundational actions could then inform additional U.S. Government potential action, including

- Taking those newly adopted standards and consider their applicability as federal purchasing requirements.
- Assessing the state of zero trust to determine whether voluntary adoption model is working sufficiently or should be supplemented by regulatory-based action.

When considering various policy levers to incentivize zero trust adoption, the U.S. Government should look first at a variety of existing models already used to encourage adoption of other commonly accepted cybersecurity best practices, such as the NIST Cybersecurity Framework.[81] These policy levers, ranging from purely voluntary to regulatory options, are explored below.

4.3. Incentivize Zero Trust in Federal Grants Funding for IT Security Modernization

Over the last several years, the Federal government has enacted an increasing number of programs that extend grant and funding opportunities to states and local governments for information technology and security

[80] ISO and IEC Joint Technical Committee (JTC 1) for Information Technology, ISO/IEC 27001: Information Security Management (landing page), https://www.iso.org/isoiec-27001-information-security.html.

[81] NIST, Cybersecurity Framework, https://www.nist.gov/cyberframework.

modernization. Recent examples include the 2020 Coronavirus Aid, Relief, and Economic Security Act,[82] the 2021 American Rescue Plan Act,[83] and the 2021 Infrastructure Investment and Jobs Act (IIJA).[84]

As these types of grant programs increase, the U.S. Government has a responsibility to distribute and implement grants in a way that measurably increases the cybersecurity baseline for recipient organizations. One way to incentivize better cybersecurity is by making state and local entity grant access conditional upon demonstrating how the funds will be used toward fulfilling commonly accepted cybersecurity best practices. With continued maturity of its underlying guidelines, such an approach can and should be extended to zero trust—with alignment to *NIST SP 800-207: Zero Trust Architecture*,[85] CISA's draft *Zero Trust Maturity Model*[86] or other to-be-developed standards serving as the baseline for unlocking federal security modernization funding.

One especially significant opportunity to incentivize widespread zero trust adoption through conditional federal grants is in the implementation of the State and Local Cybersecurity Act[87] (part of the IIJA).[88] The Act gives CISA the authority to administer over $1 billion in cybersecurity funding for states and localities over the next 4 years, between 2022–2026.[89] Incentivizing funding of projects aligned to core zero trust principles can and must be prioritized. In administering these distributions, it is critical for CISA to define acceptable zero trust-aligned project scopes more narrowly, such as "inventorying internet-accessible assets" or "reducing accounts with privileged access" to deploy these grant allocations in a targeted and appropriate way.

Furthermore, under the IIJA, the Secretaries of Transportation, Commerce, and Energy have additional discretionary authority to require funding recipients to demonstrate "sound cybersecurity practices" as a condition of receiving funds under their areas of jurisdiction. They too should exercise this authority to incentivize cybersecurity best practices, including zero trust best practices, to grant applicants as appropriate. The Commerce Department's authority to consider cybersecurity in its administration of the broadband provisions of the IIJA is one particularly critical example. The Secretary of Commerce, acting through the National Telecommunications and Information Administration, should advocate for the importance of zero trust principles to help enhance network reliability, availability and the cybersecurity of broadband networks.

---

[82] U.S. Congress, Coronavirus Aid, Relief, and Economic Security Act, March 2020, https://www.congress.gov/bill/ 116th-congress/house-bill/748.

[83] U.S. Congress, American Rescue Plan Act of 2021, March 2021, https://www.congress.gov/bill/117th-congress/house-bill/1319.

[84] U.S. Congress, Infrastructure Investment and Jobs Act, June 2021, https://www.congress.gov/bill/117th-congress/house-bill/3684.

[85] NIST, *SP 800-207: Zero Trust Architecture*, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final.

[86] CISA, *Zero Trust Maturity Model* (draft), June 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

[87] U.S. Congress, State and Local Cybersecurity Improvement Act, July 2021, https://www.congress.gov/bill/117th-congress/house-bill/3138.

[88] U.S. Congress, Infrastructure Investment and Jobs Act, June 2021, https://www.congress.gov/bill/117th-congress/house-bill/3684.

[89] Ibid.

4.4. Consider Federal Procurement Preferences for Zero Trust Alignment

The breadth of the federal government's procurement power can be a strong behavioral driver for organizations seeking to conduct business with the U.S. Government. In one recent and notable example, EO 14028[90] called for the Secretary of Commerce, through NIST, to identify standards and guidelines to enhance software supply chain security. NIST is expected to issue these standards in February and May 2022 to help federal agencies assess procurement eligibility of software vendors based on demonstrated best practices.[91]

Such a model could provide procurement preferences to organizations that prioritize cybersecurity within their own enterprise environments by aligning with specifically articulated zero trust standards and best practices. With continued maturity of consensus-based zero trust standards to anchor these procurement decisions, the promise of vendors retaining eligibility to appear on Federal Supply Schedules, Federal Governmentwide Acquisition Contracts, and Blanket Purchase Agreements would be a powerful driver for zero trust adoption.

4.5. Consider Regulatory Relief Actions

In limited and sector-specific circumstances, the U.S. Government could also consider additional actions to incentivize zero trust adoption in more regulated sectors. As one example model in the Health Care sector, an amendment to the Health Information Technology for Economic and Clinical Health (HITECH) Act[92] requires the U.S. Department of Health and Human Services, when considering whether an entity should be fined for a Health Insurance Portability and Accountability Act (HIPAA) violation, to consider the extent to which the entity has demonstrated alignment to an established risk management framework, such as the NIST Cybersecurity Framework.[93] Such a model could extend to other regulated critical infrastructure sectors that can demonstrate prioritization of cybersecurity through alignment with a commonly accepted zero trust best practice standard, as these standards sufficiently mature.

5. Conclusion

In 2018, the President's National Security Telecommunications Advisory Committee (NSTAC) undertook a significant study—defining a playbook for the U.S. Government to establish an ambitious, sweeping effort to fundamentally change the Nation's cybersecurity trajectory. The *Report to the President on a Cybersecurity*

---

[90] *EO 14028: Improving the Nation's Cybersecurity*, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[91] Ibid.

[92] U.S. Department of Health and Human Services, Health Information Technology for Economic and Clinical Health (HITECH) Act, February 2009, https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

[93] Brian Ceseratto, Patricia Wagner, and Alaap Shah, Epstein Becker Green, "HITECH Act Amendment Incentivizes Adoption of NIST and Other Recognized Cybersecurity Safeguards as a Defense or Mitigation to HIPAA [Health Insurance Portability and Accountability Act] Enforcement," January 2021, https://www.healthlawadvisor.com/2021/01/08/hitech-act-amendment-incentivizes-adoption-of-nist-and-other-recognized-cybersecurity-safeguards-as-a-defense-or-mitigation-to-hipaa-enforcement/.

Moonshot,[94] argued that the President needed to galvanize the Nation toward bold, paradigm-shifting innovations in cybersecurity across technology, policy, education, and human behavior.

The May 2021 *EO 14028: Improving the Nation's Cybersecurity*[95] seemed to acknowledge one of the Moonshot report's underlying premises—that a continued culture of incremental progress is not sufficient to keep pace with the worsening cyber threat environment—stating, "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."[96]

One of the EO's key components, an effective federal (and broader national) transition to zero trust architectures can be one of these "bold changes." The widespread adoption and maturity of zero trust principles across government and industry would represent not just a technological shift but a critical cultural shift in our collective approach to cybersecurity. In other words, if zero trust is fully realized in its forthcoming implementation, as this report urges, it could be truly transformational for the Nation as originally envisioned in the Moonshot[97] report.

The Federal Zero Trust Strategy[98] is a welcome and necessary start to help agencies build momentum and establish the foundational building blocks of zero trust. But the Strategy alone will not meaningfully transform federal cybersecurity in the long term. Effective, lasting transformation can only be achieved through a sustained whole-of-government commitment to promoting strategic coherence, employing effective management and oversight, ensuring sustained financial investment, and fostering strong alignment of the fundamental principles of zero trust in existing federal cybersecurity programs, procedures, and policies. The U.S. Government can—and must— act now, by implementing this report's recommendations to institutionalize zero trust and lay the foundation for a cybersecurity transformation ultimately measured in decades, not years.

---

[94] President's National Security Telecommunications Advisory Committee (NSTAC), *NSTAC Report to the President on a Cybersecurity Moonshot*, November 2018, https://www.cisa.gov/publication/2018-nstac-publications-0.

[95] *EO 14028: Improving the Nation's Cybersecurity*, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[96] Ibid.

[97] NSTAC, *NSTAC Report to the President on a Cybersecurity Moonshot*, November 2018, https://www.cisa.gov/publication/2018-nstac-publications-0.

[98] OMB, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

Appendix A. Zero Trust Maturity Model[99]

	Maturity Stage	Initial (1)	Repeatable (2)	Defined (3)	Managed (4)	Optimized (5)
	Description and Characteristics	The initiative is undocumented and performed on an ad hoc basis with processes undefined. Success depends on individual efforts	The process is documented and is predictably repeatable, using lessons learned in the initial phase	Processes for success have been defined and documented	Processes are monitored and controlled; efficacy is measurable	Focus is on continuous optimization
Step of the Five-Step Process	1. **Define the Protect Surface**	The DAAS element is unknown or discovered manually; data classification is not done or is incomplete	The use of automated tools to discover and classify DAAS elements has begun but is not standardized	Data classification training and processes have been introduced and are maturing; protect surface discovery is becoming automated	New or updated DAAS elements are immediately discovered, classified as assigned to the correct protect surface in an automated manner	Discovery and classification processes are fully automated
	2. **Map the Transaction Flows**	Flows are conceptualized-based interviews and workshops	Traditional scanning tools and event logs are used to construct approximate flow maps	A flow mapping process is in place; automated tools are beginning to be deployed	Automated tools create precise flow maps; all flow maps are validated with system owners	Transaction flows are automatically mapped across all locations in real time
	3. **Build a Zero Trust Architecture**	With little visibility and an undefined protect surface, the architecture cannot be properly designed	Protect surface is established based on current resources and priorities	The basics of the protect surface enforcement is complete, including placing segmentation gateways in the appropriate places	Additional controls are added to evaluate multiple variables (e.g., endpoint controls, SaaS and API controls)	Controls are enforced using a combination of hardware and software capabilities

[99] CISA, *Zero Trust Maturity Model* (draft), June 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

Maturity Stage	Initial (1)	Repeatable (2)	Defined (3)	Managed (4)	Optimized (5)
4. **Create a Zero Trust policy**	Policy is written at Layer 3 (Network)	Additional "who" statements are being identified to address business needs; user IDs of applications and resources are known, but access rights are unknown	The team works with the business to determine who or what should have access to the protect surface	Custom user-specific elements are created and defined by policy, reducing policy space and number of users with access	Layer 7 (Application) policy is written for granular enforcement; only known allowed traffic and legitimate application communication is allowed
5. **Monitor and Maintain the Network**	Visibility into what is happening on the network is low	Traditional security information and event management or log repositories are available, but the process is still mostly manual	Telemetry is gathered from all controls and is sent to a central data lake	Machine learning tools are applied to the data lake for context into how traffic is used in the environment	Data is incorporated from multiple sources and used to refine steps 1–4; alerts and analyses are automated

Appendix B. Zero Trust Maturity Model Use Case: Directory Services

Directory Services (e.g., Active Directory, others) (defined as an asset in the DAAS nomenclature) is the infrastructure and software most organizations use to manage their digital identities and accounts. Because Directory Services is at the heart of controlling access rights, it is a prime target for attackers who can exploit it to grant themselves all the IT permissions they need to achieve their goals, such as stealing vital data or deploying ransomware at scale.

In a zero trust context, Directory Services is the underlying infrastructure that supports authentication and authorization. Its compromise would de facto render any zero trust implementation ineffective. For these reasons, preventing Directory Services compromises and monitoring it for suspicious behaviors is not only a security best practice, but paramount to the success of any zero trust initiative. Transitioning to authentication services that support modern authentication protocols with multifactor authentication (MFA) would be a significant step toward zero trust maturity.

Directory Services has two primary use cases: Administrative and User. Administrators maintain the system. Users connect to the network and authenticate to the system to access resources. Each use case requires its own controls. Zero trust requires placing controls as near to the asset as possible. For on-premises Directory Services, this usually means a next-generation firewall being placed logically close to the directory system.

The next step is to create policy, limiting access to the asset in both use cases. In the example in Table 7, access for administrators is shown following the Kipling Method for Zero Trust policy creation, first introduced in Table 3.

Table 7: Kipling Method Zero Trust Policy for Directory Services Administrator Role

WHO	WHAT	WHEN	WHERE	WHY	HOW
Admins MFA	Directory Admin Tool App	24/7	Dir_Server_Loc	metadata	IDS/DPI

An admin user (defined by group membership rather than source internet protocol [IP] address) who has successfully completed MFA can access servers that are part of the "Dir_Server_Loc" (defined by, for example, tags on workloads rather than destination IP addresses) using the "Directory Admin Tool App" (which is defined by web/client-server/SSH rather than port and protocol) at any time after passing Intrusion Detection System (IDS) and Deep Packet Inspection (DPI) checks. In this example, an additional "why" section allows logging of the justification of this specific access resource.

This exercise can be performed again for users, perhaps adding Just in Time rules to "WHEN." This would limit the timeframes that specific users or groups of users are allowed to use this system. Once access rules have been created and deployed for each of the use cases, the telemetry from the controls and systems are sent to some type of log collection technology for analysis. The purpose of this step is to learn from the telemetry to create a feedback loop in the zero trust system that allows for continuous improvement.

Table 8: Zero Trust Maturity Model for Directory Services

Maturity Stage	Initial (1)	Repeatable (2)	Defined (3)	Managed (4)	Optimized (5)
Directory Services (e.g., Active Directory, other)	Agencies lack a comprehensive inventory of their Directory Services infrastructure (both on-premise and in the cloud). The agency may have fragmented internal groups that use separate services or groups that use a specific service for a set of use cases that is unknown to either operations or security. **To move from (1) to (2)**, the agency must perform a comprehensive inventory of the targeted Directory Services infrastructure, protections in place, user accounts, and user groups to assess the scope of a future zero trust implementation.	Agencies have a comprehensive inventory of their Directory Services infrastructure (both on-premise and in the cloud). **To move from (2) to (3)**, the agency needs to develop processes to audit infrastructure for vulnerabilities and have a process to remediate those vulnerabilities in a timely manner. In addition, the agency develops a process to detect vulnerabilities, misconfiguration, and configuration drift, both in the infrastructure and for user accounts/user groups. The agency can employ the Kipling Method to expedite the process; determining use cases and placing users/groups in each, taking the opportunity to rationalize.	Agencies have well-defined processes for detecting and remediating vulnerabilities, misconfiguration, and drift in both Directory Services infrastructure, user accounts, and user groups. **To move from (3) to (4)**, agencies need to monitor Directory Services in real time for configuration drift and new attack path creation. In addition, internal procedures and tools must allow all security stakeholders visibility into the status of the directory services and to align their strategies around the defense of Directory Services.	Agencies monitor Directory Services in real time for configuration drift and the creation of new attack paths. All stakeholders have visibility into defense of Directory Services. **To move from (4) to (5)**, agencies need to include dynamic policies that consider post authentication user behaviors (e.g., behavioral biometrics) to determine access to resources, potentially including Just in Time provisioning of access. In addition, the agency implements real-time attack detection capabilities for reconnaissance, lateral movement, privilege escalation, and domain domination techniques and integrates these capabilities with their security operations center (SOC).	Agencies have a comprehensive inventory of their Directory Services infrastructure (both on-premise and in the cloud), user accounts, and user groups. The agencies monitor Directory Services infrastructure, user accounts, and user groups in real time for configuration drift, reconnaissance, lateral movement, privilege escalation, and domain domination techniques and integrates these capabilities tightly with their SOC. The agencies have implemented dynamic policies that consider post-authentication user behavior to determine access to resources.

Appendix C. Membership and Participants

Table 9: Subcommittee Leadership

Name	Organization	Role
Mr. John Donovan	NSTAC Chair	Subcommittee Co-Chair
Mr. Mark McLaughlin	Palo Alto Networks, Inc.	Subcommittee Co-Chair
Mr. Christopher Boyer	AT&T, Inc.	Working Group Co-Lead
Mr. Sean Morgan	Palo Alto Networks, Inc.	Working Group Co-Lead

Table 10: Subcommittee Membership

Name	Organization
Mr. Christopher Anderson	Lumen Technologies, Inc.
Mr. Jamie Brown	Tenable, Inc.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Mr. Sean Connelly	Cybersecurity and Infrastructure Security Agency (CISA)
Mr. Chris Day	Tenable, Inc.
Mr. Jon Goding	Raytheon Technologies Corp.
Ms. Katherine Gronberg	NightDragon Security, LLC
Mr. Ken Kaminski	Ericsson, Inc.
Mr. John Kindervag	ON2IT BV
Mr. Kent Landfield	Trellix
Mr. Jerry McLaughlin	Palo Alto Networks, Inc.
Mr. Richard Mosley	AT&T, Inc.
Mr. Thomas Patterson	Unisys Corp.
Mr. Jon Peterson	Neustar, Inc.
Mr. Rakesh Punjabi	Lumen Technologies, Inc.
Mr. Thomas Quillin	Intel Corp.
Mr. Sunjeet Randhawa	Broadcom, Inc.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. John Simms	CISA
Ms. Chelsea Smethurst	Microsoft Corp.
Mr. Robert Spiger	Microsoft Corp.
Dr. Torsten Staab	Raytheon Technologies Corp.
Mr. Quint Van Deman	Amazon Web Services, Inc.

Name	Organization
Dr. Claire Vishik	Intel Corp.
Mr. Milan Vlajnic	Communication Technologies, Inc.

Table 11: Briefers, Subject-Matter Experts

Name	Organization
Mr. Kevin Bingham	National Security Agency
Ms. Sylvia Burns	Federal Deposit Insurance Corporation
Mr. Sean Connelly	CISA
Dr. Chase Cunningham	Ericom Software, Inc.
Mr. Kevin Davis	NSA
Mr. Lawrence Hale	General Services Administration
Mr. Stephen Haselhorst	U.S. Air Force
Mr. Alper Kerman	National Institute of Standards and Technology
Mr. John Kindervag	ON2IT BV
Mr. David McKeown	Department of Defense
Mr. Eric Mill	Office of Management and Budget
Mr. Justin Morgan	GSA
Mr. Scott Rose	National Institute of Standards and Technology
Mr. Mark Ryland	Amazon Web Services Security
Mr. John Simms	CISA
Mr. Patrik Teppo	Ericsson, Inc.
Ms. Amy Zwarico	AT&T, Inc.

Table 12: Subcommittee Management

Name	Organization
Ms. DeShelle Cleghorn	President's National Security Telecommunications Advisory Committee (NSTAC) Alternate Designated Federal Officer (ADFO)
Mr. Scott Zigler	NSTAC ADFO
Ms. Emily Berg	Booz Allen Hamilton, Inc.
Dr. Philip Grant	Booz Allen Hamilton, Inc.
Ms. Laura Penn	Edgesource Corp.

Appendix D. Acronyms

Table 13: Acronyms

Acronym	Definition
5G	Fifth Generation
6G	Sixth Generation
ADFO	Alternate Designated Federal Officer
API	Application Programming Interface
C2C	Comply-to-Connect
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CNSSI	Committee on National Security Systems Instruction
COVID-19	Coronavirus Disease 2019
DAAS	Data, Applications, Assets, and Services
DevSecOps	Development, Security, and Operations
DISA	Defense Information Systems Agency
DoD	Department of Defense
DPI	Deep Packet Inspection
EO	Executive Order
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GSA	General Services Administration
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HSPD	Homeland Security Presidential Directive
ICAM	Identity Credentialing and Access Management
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IIJA	Infrastructure Investment and Jobs Act
IoT	Internet of Things
IP	Internet Protocol
ISCM	Information Security Continuous Monitoring
ISO	International Organization for Standardization

Acronym	Definition
IT	Information Technology
JTC	Joint Technical Committee
MFA	Multifactor Authentication
MGT	Modernizing Government Technology
NCCoE	National Cybersecurity Center of Excellence
NCD	National Cyber Director
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NSA	National Security Agency
NSM	National Security Memorandum
NSPD	National Security Presidential Directive
NSTAC	President's National Security Telecommunications Advisory Committee
OMB	Office of Management and Budget
OT	Operational Technology
QSMO	Quality Service Management Office
SaaS	Software-as-a-Service
SOC	Security Operations Center
SP	Special Publication
TMF	Technology Modernization Fund
U.S.	United States
U.S.C.	United States Code
ZT-IdM	Zero Trust and Trusted Identity Management
ZTA	Zero Trust Architecture

Appendix E. Definitions

Table 14: Definitions

Term	Definition	Source
Active Directory	A Microsoft directory service for managing identities in Windows domain networks (registered trademark).	▪ National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-16B NIST SP 1800-16C NIST SP 1800-16D
Adversary	Any individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.	▪ NIST SP 800-30
American Rescue Plan	A White House plan delivering direct relief to the American people, rescuing the economy, and starting to beat the virus.	▪ The White House, https://www.whitehouse.gov/american-rescue-plan/
Application Programming Interface	A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.	▪ NIST SP 1800-16C under "application program interface" from NIST Interagency or Internal Report (NISTIR) 5153
Artificial Intelligence	(1) A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement. (2) The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.	▪ American National Standards Institute International Committee for Information Technology Standards 172-220 (R2007) Information Technology -- American National Standard Dictionary of Information Technology ▪ Cited in NIST's *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*
Broadband	High-speed internet access that is always on and faster than dial-up access.	▪ Federal Communications Commission, https://www.fcc.gov/general/types-broadband-connections#:~:text=The%20%20term%20broadband%20commonly%20refers%20to%20high-speed%20Internet,transmission%20technologies%20%20such%20as:%20Digital%20Subscriber%20Line%20

Term	Definition	Source
Chief Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.	▪ NIST SP 800-18 Rev. 1 under Senior Agency Information Security Officer from 44 United States Code (U.S.C.), Sec. 3544 ▪ NIST SP 800-60 Vol. 1 Rev. 1 under Senior Agency Information Security Officer from 44 U.S.C., Sec. 3544 ▪ NIST SP 800-60 Vol. 2 Rev. 1 under Senior Agency Information Security Officer from 44 U.S.C., Sec. 3544
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	▪ NISTIR 8006 under "cloud computing"
Commercial-off-the-Shelf	Software and hardware that already exist and are available from commercial sources.	▪ NIST SP 800-161 under "commercial off-the-shelf" NIST SP 800-64 Rev. 2
Connectivity	Capacity for interconnecting platforms, systems, and applications.	▪ PCMag, https://www.pcmag.com/encyclopedia/term/connectivity
Continuous Diagnostics and Mitigation	A Congressionally established program to provide adequate, risk-based, and cost-effective cybersecurity assessments and efficiently allocate cybersecurity resources targeted at federal civilian organizations.	▪ NISTIR 8011 Vol. 1
Controlled Unclassified Information	Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under *EO 13526: Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.	▪ NIST SP 800-171 Rev. 2 under controlled unclassified information from EO 13556 ▪ NIST SP 800-172 under controlled unclassified information from EO 13556 ▪ NIST SP 800-171 Rev. 1 [Superseded] under controlled unclassified information from EO 13556
Counterfeit	An unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source.	▪ NIST SP 800-161, 18 U.S.C.

Term	Definition	Source
Critical Infrastructure	Sixteen sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.	▪ Cybersecurity Infrastructure Security Agency, https://www.cisa.gov/critical-infrastructure-sectors
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.	▪ Committee on National Security Systems Instruction (CNSSI) 4009-2015 from National Security Presidential Directive 54 (NSPD-54)/Homeland Security Presidential Directive 23 (HSPD-23) ▪ NIST SP 1800-25B under Cybersecurity from CNSSI 4009-2015 ▪ NSPD-54/HSPD-23 ▪ NIST SP 1800-26B under Cybersecurity from CNSSI 4009-2015 ▪ NSPD-54/HSPD-23 ▪ NIST SP 800-160 Vol. 2 from CNSSI 4009-2015 ▪ NIST SP 800-37 Rev. 2 ▪ NIST SP 800-53 Rev. 5 from OMB Circular A-130 (2016) ▪ NISTIR 7621 Rev. 1 under Cybersecurity from CNSSI 4009-2015
Cybersecurity Division	Leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector (the ".com" domain) to increase the security of critical networks. This occurs through the following functions: capacity delivery; threat hunting; operational collaboration; vulnerability management; capacity building; strategy, resources, and performance; and cyber defense education and training.	▪ CISA, https://www.cisa.gov/cybersecurity-division
Deep Packet Inspection	A method of examining the content of data packets as they pass by a checkpoint on the network.	▪ Fortinet, https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection
Development Operations	A set of practices for automating the processes between software development and information technology operations teams so that they can build, test, and release software faster and more reliably. The goal is to shorten the systems development life cycle and improve reliability while delivering features, fixes, and updates frequently in close alignment with business objectives.	▪ NIST SP 1800-16B ▪ NIST SP 1800-16C ▪ NIST SP 1800-16D

Term	Definition	Source
DevSecOps	Automates the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery.	▪ IBM, https://www.ibm.com/cloud/learn/devsecops
Directory Services	A distributed database service capable of storing information, such as certificates and certificate revocation lists, in various nodes or servers distributed across a network. (In the context of this practice guide, a directory services stores identity information and enables the authentication and identification of people and machines.)	▪ NIST SP 1800-16B under Directory Service from NIST SP 800-15 ▪ NIST SP 1800-16D under Directory Service from NIST SP 800-15
Emerging Technologies	Technologies that are currently developing and are expected to impact society in some significant way over the next 5 to 10 years.	▪ Independence University, https://www.independence.edu/blog/what-is-emerging-technology
EO 14028, Improving the Nation's Cybersecurity	Charges multiple agencies, including NIST, with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.	▪ Federal Register: Improving the Nation's Cybersecurity
Fifth Generation	The fifth installment of advanced wireless technology, bringing about increased bandwidth and capacity for advancements within the Internet of Things.	▪ Qualcomm, https://www.qualcomm.com/5g/what-is-5g
Hardware	The physical components of an information system.	▪ NIST SP 800-53 Rev. 4 under Hardware CNSSI 4009
Identity Management	(Also known as identity and access management) A fundamental cybersecurity concept focused on ensuring "the right people and things have the right access to the right [technology] resources at the right time."	▪ NIST: Identity and Access Management, https://www.nist.gov/identity-access-management
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.	▪ Federal Information Processing Standards 200 under Information Technology 40 U.S.C., Sec. 1401

Term	Definition	Source
Infrastructure Investment and Jobs Act	Requires brokers to report to the Internal Revenue Service the cost basis of digital assets transferred by their clients to non-brokers, similar to how securities brokers report stock and bond trades.	▪ Small Business Association of Michigan, https://www.sbam.org/the-infrastructure-investment-and-jobs-act-includes-tax-related-provisions-youll-want-to-know-about/
Internet of Things	Internet of Things (IoT) refers to systems that involve computation, sensing, communication, and actuation (as presented in NIST SP 800-183). IoT involves the connection between humans, non-human physical objects, and cyber objects, enabling monitoring, automation, and decision making.	▪ NIST SP 800-183
Internet Protocol	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.	▪ CNSSI 4009-2015
Internet Service Provider	A company that provides internet connections and services to individuals and organizations.	▪ Britannica, https://www.britannica.com/technology/Internet-service-provider
Intrusion Detection Systems	software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.	▪ NIST SP 800-31
Machine Learning	A branch of artificial intelligence focused on building applications that learn from data and improve their accuracy over time without being programmed to do so.	▪ IBM, https://www.ibm.com/cloud/learn/machine-learning
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.	▪ CNSSI 4009-2015 under malicious logic from Internet Engineering Task Force Request for Comments 4949 V2
National Security and Emergency Preparedness	Policies, plans, procedures, and readiness measures that enhance the ability of the U.S. Government to mobilize for, respond to, and recover from a national security emergency.	▪ Department of the Interior, https://www.doi.gov/sites/doi.gov/files/-900-dm-5-nsep-2021.pdf
Network Time Protocol	A protocol that allows the synchronization of system clocks (from desktops to servers).	▪ Science Direct, https://www.sciencedirect.com/topics/computer-science/network-time-protocol
Operating System	The software “master control application” that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.	▪ NIST SP 800-44 Version 2 ▪ NISTIR 7621 Rev. 1 from NIST SP 800-44 Version 2

Term	Definition	Source
Operational Technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.	▪ NIST SP 800-37 Rev. 2
Protocol	A set of rules governing the exchange or transmission of data between devices.	▪ Britannica, https://www.britannica.com/technology/protocol-computer-science
Security Orchestration, Automation, and Response	A stack of compatible software programs that enables an organization to collect data about security threats and respond to security events without human intervention.	▪ Business 2 Community, https://www.business2community.com/cybersecurity/security-orchestration-automation-and-response-soar-02447208#:~:text=Security%20Orchestration%2C%20Automation%2C%20and%20Response%20%28SOAR%29%20is%20a,the%20efficiency%20of%20physical%20and%20digital%20security%20operations
Sixth Generation	Sixth generation of wide-area wireless technology	▪ PCMag, https://www.pcmag.com/news/what-is-6g
Software Application	A software program hosted by an information system.	▪ CNSSI 4009-2015 from NIST SP 800-37 Rev. 1 ▪ NIST SP 1800-16B under Application from NIST SP 800-137 ▪ NIST SP 1800-16C under Application from NIST SP 800-137 ▪ NIST SP 1800-16D under Application from NIST SP 800-137 ▪ NIST SP 800-137 under Application from NISTIR 7298 ▪ NIST SP 800-37 Rev. 2 ▪ NIST SP 800-53 Rev. 5 from NIST SP 800-37 Rev. 2 ▪ NISTIR 7621 Rev. 1 under Application from CNSSI 4009-2015 ▪ NIST SP 800-37 Rev. 1 [Superseded] under Application
Software Developers	A person or group that designs and/or builds and/or documents and/or configures the hardware and/or software of computerized systems.	▪ Food and Drug Administration, Glossary of Computer System Software Development Terminology (8/95)

Term	Definition	Source
Software Development Lifecycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation, and maintenance, and ultimately its disposal that instigates another system initiation.	▪ CNSSI 4009-2015 from NIST SP 800-34 Rev. 1
Technology Modernization Fund	An innovative funding vehicle authorized by the Modernizing Government Technology Act of 2017 that gives agencies additional ways to deliver services to the American public more quickly, better secure sensitive systems and data, and use taxpayer dollars more efficiently.	▪ U.S. General Services Administration, https://www.gsa.gov/technology/government-it-initiatives/technology-modernization-fund
Third-Party Component	An external entity, including, but not limited to, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, with or without a contractual relationship to the first-party organization.	▪ NIST, https://csrc.nist.gov/glossary/term/Third_Party_Relationships
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or DoS.	▪ NIST SP 800- 53, CNSSI 4009, Adapted
Threat Environment	The online space where cyber threat actors conduct malicious cyber threat activity.	▪ An Introduction to the Cyber Threat Environment, https://icclr.org/wp-content/uploads/2019/05/Intro-to-cyber-threat-environment-e.pdf?x37853
Trustworthiness	The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.	▪ NIST SP 800-39, CNSSI-4009
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).	▪ NIST SP 800-161 under Verification from CNSSI 4009 ▪ ISO 9000 – Adapted ▪ NISTIR 7622 under Verification from CNSSI 4009, ISO 9000 – Adapted
Virtual Private Network	A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks.	▪ NIST SP 800-113 under Virtual Private Network
Zero Trust	A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.	▪ NIST SP 800-207, https://doi.org/10.6028/NIST.SP.800-207

Term	Definition	Source
Zero Trust Architecture	An architecture that treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized.	▪ NIST, https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

Appendix F. Bibliography

Bingham, Kevin, and Davis, Kevin, National Security Agency (NSA), "NSA Cybersecurity Directorate Zero-Trust (ZT) Overview," Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Zero Trust and Trusted Identity Management (ZT-IdM) Subcommittee, Arlington, VA, October 20, 2021

Burns, Sylvia, Federal Deposit Insurance Corporation, "NSTAC ZT-IdM Subcommittee Briefing," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, October 13, 2021

Ceseratto, Brian, Wagner, Patricia, and Shah, Alaap, Epstein Becker Green, "Health Information Technology for Economic and Clinical Health Act Amendment Incentivizes Adoption of NIST and Other Recognized Cybersecurity Safeguards as a Defense or Mitigation to HIPAA [Health Insurance Portability and Accountability Act] Enforcement," January 2020, https://www.healthlawadvisor.com/2021/01/08/hitech-act-amendment-incentivizes-adoption-of-nist-and-other-recognized-cybersecurity-safeguards-as-a-defense-or-mitigation-to-hipaa-enforcement/

Connelly, Sean, and Simms, John, Cybersecurity and Infrastructure Security Agency, "Zero-Trust Architecture [ZTA]," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, September 29, 2021

Cunningham, Chase, Ericom Software, "ZT and Some Hard Truths in Cybersecurity," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, November 10, 2021

Cybersecurity and Infrastructure Security Agency (CISA), Continuous Diagnostics and Mitigation, Accessed January 25, 2022, https://www.cisa.gov/cdm

CISA, Trusted Internet Connections, January 2022, https://www.cisa.gov/tic

CISA, *Zero Trust Maturity Model* (draft), June 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

Department of Defense (DoD), *Zero Trust Reference Architecture*, February 2021, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

Executive Order (EO) 14028: Improving the Nation's Cybersecurity, The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Hale, Lawrence, and Morgan, Justin, General Services Administration (GSA), "How GSA Can Help Agencies with Their ZTA Journey," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, October 13, 2021

Haselhorst, Stephen, U.S. Air Force, "Department of the Air Force - ZT," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, November 10, 2021

ISO and IEC Joint Technical Committee (JTC 1) for Information Technology, ISO/IEC 27001: Information Security Management (landing page), https://www.iso.org/isoiec-27001-information-security.html.

Kerman, Alper, and Rose, Scott, National Institute of Standards and Technology, "ZTA; Implementing a ZTA," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, September 22, 2021

Kindervag, John, *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*, September 14, 2010, Updated September 17, 2010, https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

Kindervag, John, ON2IT BV, "NSTAC ZT Briefing," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, September 8, 2021

McKeown, David, DoD, "DoD ZT Reference Architecture: Implementing ZT at Scale," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, October 27, 2021

Mill, Eric, Office of Management and Budget, "Review of the ZT Strategy," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, September 15, 2021

National Institute of Standards and Technology (NIST), Cybersecurity Framework, Accessed January 25, 2022, https://www.nist.gov/cyberframework

NIST, "Roadmap: NIST Special Publication (SP) 800-63-3: Digital Identity Guidelines," June 2017, https://www.nist.gov/identity-access-management/roadmap-nist-special-publication-800-63-3-digital-identity-guidelines

NIST, *SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*, September 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST, *SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

NIST, *SP 800-207: Zero Trust Architecture*, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

National Security Agency (NSA), *Embracing a Zero Trust Security Model*, February 2021, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

National Security Memorandum 8 (NSM-8): Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, The White House, January 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems

Office of Management and Budget, *M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, The White House, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

President's National Security Telecommunications Advisory Committee (NSTAC), *NSTAC Report to the President on a Cybersecurity Moonshot*, November 2018, https://www.cisa.gov/publication/2018-nstac-publications-0

Ryland, Mark, Amazon Web Services Security, "Amazon's Zero-Trust Journey: Insights and Lessons Learned," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, December 1, 2021

State of California, *Cal-Secure: State of California Executive Branch Multi-Year Information Security Maturity Roadmap 2021*, https://cdt.ca.gov/wp-content/uploads/2021/10/Cybersecurity_Strategy_Plan_FINAL.pdf

Teppo, Patrik, Ericsson, "Lessons Learned from Building Zero-Trust Architecture in Telco Networks," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, December 1, 2021

The Technology Modernization Fund (TMF), Awarded Projects page: "Advancing Zero Trust," https://tmf.cio.gov/projects"/#advancing-zero-trust

The TMF, Awarded Projects page: "Zero Trust Architecture," https://tmf.cio.gov/projects/#zero-trust-architecture

The TMF, Awarded Projects page: "Zero Trust Networking," https://tmf.cio.gov/projects/#zero-trust-networking

U.S. Congress, Federal Information Security Management Act of 2002, March 2002, https://www.congress.gov/bill/107th-congress/house-bill/3844

U.S. Congress, Modernizing Government Technology (MGT) Act of 2017, May 2017, https://www.congress.gov/bill/115th-congress/house-bill/2227

U.S. Congress, Coronavirus Aid, Relief, and Economic Security Act, March 2020, https://www.congress.gov/bill/116th-congress/house-bill/748

U.S. Congress, American Rescue Plan Act of 2021, March 2021, https://www.congress.gov/bill/117th-congress/house-bill/1319

U.S. Congress, Infrastructure Investment and Jobs Act, June 2021, https://www.congress.gov/bill/117th-congress/house-bill/3684

U.S. Congress, State and Local Cybersecurity Improvement Act, July 2021, https://www.congress.gov/bill/117th-congress/house-bill/3138

U.S. Department of Health and Human Services, Health Information Technology for Economic and Clinical Health (HITECH) Act, February 2009, https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

Zwarico, Amy, AT&T, "AT&T's Zero-Trust Roadmap," Briefing to the NSTAC ZT-IdM Subcommittee, Arlington, VA, December 1, 2021