Critical Success Factors for Broad Zero Trust Adherence Across Federal Agencies

Jordan Hernaez

Dr. Karahan

CYSE 698

07/26/2026

Table of Contents

Abstract **3**

1 Introduction **4**

2 Defining Zero Trust Architecture **7**

2.1 Core principles of Zero Trust *8*

2.2 Perimeter to identity-based security *9*

2.3 Components of Zero Trust *10*

3 Literature Review **12**

3.1 Research on Zero Trust adoption *12*

3.2 Maturity assessment frameworks *13*

3.3 Implementation barriers *14*

4 Critical Success Factors **16**

4.1 Identity, Credential, and Access Management *16*

4.2 Endpoint and device visibility *16*

4.3 Data classification and handling *17*

4.4 Automation, analytics, and continuous monitoring *17*

4.5 Governance, leadership, and workforce readiness *18*

4.6 Standardized cross-agency maturity assessment *18*

5 Recommendations **20**

5.1 Prioritize identity modernization *20*

5.2 Improve asset and endpoint visibility *20*

5.3 Strengthen data governance *21*

5.4 Expand automation and analytics *21*

5.5 Develop consistent maturity benchmarks *22*

6 Conclusion **23**

7 Works Cited **24**

Abstract

An increase of occurrence and sophistication of attacks targeting U.S. federal agencies has necessitated the migration of traditional perimeter-based network security to a more comprehensive and modern identity-centric security. As agencies have migrated data and systems to cloud environments, a need for a more adaptive and restrictive approach to security has been identified. Zero Trust architecture has been adopted by the federal government as the gold standard for federal agencies to strive toward to achieve full Zero Trust maturity. Guidance from various policies, mandates, and orders has helped apply consistently and accelerate implementation across the federal government, but implementation remains siloed.

This paper examines the main critical success factors necessary for broad and comprehensive Zero Trust adoption across the federal government. Through extensive literature review, key factors including improving identity management policies, enhancing endpoint protection, implementing stricter data governance, user awareness, better standardization of maturity benchmarks, and expanding automation and continuous monitoring are vital to ensure Zero Trust is adopted and consistently applied across all federal agencies. In addition, numerous barriers are identified such as legacy infrastructure, disparity of fund allocation, inadequate inter-agency coordination, and access to technical expertise. In order to successfully adopt and mature Zero Trust across the federal government, a holistic approach is required, with clear actionable insights used to further improve and accelerate adoption.

1 Introduction

Since the publishing of the first national cybersecurity policy 1998 by then President Bill Clinton, the technological landscape has transformed dramatically (The White House, 1998). This radical shift in ideology has required a more efficient, expeditious, and comprehensive response from the federal government. Due to the sensitive nature of information stored and processed within the public sector, the need to better protect it has risen faster than the government has been able to secure it. In recent years, technology has seen an unprecedented boom in advancements. These advancements, such as cloud services and remote access to sensitive government systems have unveiled a new threat vector that most government agencies have yet to fully address. This has been demonstrated through various cybersecurity incidents, such as the 2025 CISA credentials leak, where a CISA contractor stored sensitive government credentials in a public GitHub repository for approximately six months, before it was finally identified and addressed (Cloud Security Alliance, 2026). Incidents like this outline the need to migrate current network defense strategies away from perimeter-based defenses and assumed trust.

Federal agencies have invested heavily into perimeter-based defenses. This strategy focuses on defending networks from external threats, but once inside, there is a level of assumed trust that users and devices operate under. This trust can be exploited through insecure credentials, phishing, and software/hardware vulnerabilities. Once a threat actor is able to access the network, they can operate relatively unrestricted. Another such example of an attack exploiting this weakness is the SolarWinds Cybersecurity incident of 2020, wherein threat actors compromised source code for one of their network management products called Orion. After the source code was compromised, unbeknownst to SolarWinds, an update containing the

compromised source code was pushed to thousands of customers, many of which were federal agencies (Benzel et al., 2021). Once inside, threat actors were able to exfiltrate an undetermined amount of sensitive information, in part due to the assumed trust within the perimeter of the network.

In 2021 then President Joe Biden signed an executive order directing federal agencies to adopt Zero Trust architecture. Zero trust security assumes that nothing within a given network can be trusted, and requires continuous monitoring and verification of all users, devices, and applications running within the network. Additionally, access should be granted to entities following least-privilege access, and conduct real-time risk assessment (Rose et al, 2020). Following this executive order, the Cybersecurity and Infrastructure Security Agency (CISA) published the Zero Trust Maturity Model to provide agencies with a structured framework to assist agencies in implementing Zero Trust within their networks (CISA, 2023). Since then, CISA has regularly updated their Zero Trust Maturity Model, and federal agencies have been tasked with deadlines to adoption.

Although the Office of Management and Budget (OMB) had established deadlines for federal agency Zero Trust adoption, many agencies were not able to meet the requirements set forth. U.S. federal agencies have vastly differing missions, in addition to levels of funding, technical expertise, and network security. As a result, for most agencies, their current levels of zero trust maturity vary wildly. Additionally, within each agency they continue to leverage legacy hardware and software that is costly and time-consuming to either integrate with or have replaced by Zero Trust compliant methodology altogether. Technology notwithstanding, each agency must also grapple with the development and enhancement of identity governance, cybersecurity policy, and user awareness. Implementing technology alone is not sufficient to

ensure timely and successful adoption of Zero Trust architecture. Research into Zero Trust adoption suggests that implementation success requires a holistic approach – integrating technical controls, risk management, cultural shifts, and leadership buy-in.

The goal in this research is to determine the critical success factors necessary for comprehensive and standardized Zero Trust adoption across federal agencies. The first objective is to define Zero Trust architecture through reviewing government agency/presidential mandates and orders. Afterwards, a literature review is conducted to understand current barriers to implementation and identify the cause of uneven maturity levels across federal agencies. Next, factors of successful adoption will be identified and the barriers to adoption will be analyzed. Finally, recommendations are presented to ensure consistent compliance and maturity levels, enhance cross-organizational collaboration, and further improve upon Zero Trust architecture. Without the consideration of the defined critical success factors, the modernization of federal agency cybersecurity infrastructure will continue to be applied unevenly, and cyber incidents will only increase in damage and frequency.

2 Defining Zero Trust Architecture

Zero Trust architecture is a fundamentally different approach to network security than what has been implemented in the past. Traditionally, federal agencies have implemented perimeter-based security, which strictly controls traffic inbound and outbound of the agency's networks. However, once inside the network, identities are assumed as trusted, granting broad user permissions once access is gained. With Zero Trust architecture, at no point is any identity considered trusted within the network. Whether the identity is attempting outside access into the network, or an identity already resides within the network, no level of trust is assumed, and every request to access resources within the network requires initial and ongoing authentication and authorization. Additionally, various contextual factors must also be validated, such as location, classification, identity behavior, and real-time threat monitoring. Through Zero Trust architecture, compromise is always considered as possible or likely, which minimizes opportunities for threat actors to move freely within the network once inside.

In 2010, Zero Trust was introduced by a cybersecurity expert at Forrester Research known as John Kindervag. Within the Forrester Research published document, Kindervag asserted that perimeter-based network security was no longer enough, and ubiquitous security throughout the network was required. Since its initial debut, Zero Trust evolved from a concept to a comprehensive enterprise security architecture through support and guidance from CISA, the National Institute of Standards and Technology (NIST), and OMB. Their support has enabled federal agencies to transition to identity-centric security, while also accommodating modern computing and work environments (Kindervag, 2010).

As of current, Zero Trust implementation within federal agencies is a major priority to enhance cybersecurity resilience for the present and future. NIST Special Publication 800-207

defines Zero Trust Architecture as a collection of cybersecurity principles that eliminate assumed trust and continuously evaluating legitimacy of access requests (NIST 2020). Zero Trust architecture implements a defense-in-depth approach through maintaining and enhancing perimeter-based security, in conjunction with endpoint and application security, network segmentation, encryption, and continuous monitoring that can remain flexible to the continuously evolving threat landscape.

2.1 Core principles of Zero Trust

There are several foundational principles that underpin Zero Trust architecture. One of the most recognizable is “never trust, always verify.” Every identity within the network must be initially and continuously authenticated and authorized prior to accessing an organizational resource. This shifts the philosophy that access to resources is not a one-time event, but a continuous evaluation and analysis of contextual information during an authentication session.

Another principle is the idea of least-privilege, which defines the minimum permissions necessary to perform authorized mission or job functions. Historically, organizations have granted broad and unrestrictive permissions to users within their networks. Through the concept of least-privilege, permissions are assigned with restrictions based on roles and responsibilities of the user. When needed, users can temporarily elevate their privileges when, with immediate revocation of elevation once the elevated privilege is no longer needed. This idea reduces the attack vectors for threat actors in the event of a compromised account (Rose et al., 2020).

Continuous monitoring and verification of access is another core component of Zero Trust. Information about user sessions, geographic location, and other potentially abnormal activity is constantly collected and analyzed throughout the network, with alerts and revocation of access through machine learning and automated threat detection when abnormal activity is identified.

This real-time alerting and revocation allow the protection of resources to minimize the foothold threat actors can establish within a compromised network.

Segmentation of network resources is a principle of Zero trust that allows organizations to divide sections of their networks into smaller zones that are governed by more granular access policies than the greater network. In the event that an attacker gains access to the wider network, an additional barrier with more restrictive access controls exists at the front of the segmented network zone that prevents them from moving laterally through the network. It also supports the ability for the organization to better contain and address cybersecurity incidents by shutting down compromised zones of the network without disrupting traffic through the greater network.

Lastly, Zero Trust assumes that a cyber incident is not possible, but inevitable. As a result, organizations design their networks to maximize mitigation capability in addition to prevention capability. This principle encompasses automated detection of compromise, rapid quarantine of affected systems, and robust recovery procedures to ensure minimal downtime after a breach.

2.2 Perimeter to identity-based security

A longstanding approach to network security has focused on protecting the network perimeter, hardening the point of access from the internal network to the wider internet. Implementing this approach constituted robust firewall policies, as well intrusion prevention and detection systems. However, once inside the network, broad and relatively unrestricted access to resources is provided. This approach was relatively efficient and effective in the time of on-premises deployment models, where an organization's network assets were all contained within the network itself. In the current technological age, many organizations are now migrating many of their services and resources to external providers, such as cloud computing and remote work employees. As organizations continue to migrate much of their capabilities to cloud platforms

and continue to support remote workers, organizational resources are no longer confined within its own network boundaries. This presents a substantial security risk that traditional perimeter-based security mechanisms cannot fully address.

Identity-based security can better address these challenges by making identity the security boundary rather than the overarching network itself. Access to resources within the network must consider the context of the access, including authentication, user behavior, location, data classification, and device trust level. This allows organizations to dynamically address access control when abnormal activity is detected, such as a user logging in from a different country than they have historically.

Multi-factor authentication (MFA) is a core component of Zero Trust architecture, as in order to authenticate, a user must provide not only what they know (i.e., a password), but what they have (i.e., a smartphone authenticator app, securely generated token key, etc.). When used in conjunction with privileged access management (PAM), and contextual based access controls, identity-centric security drastically reduces the attack surface able to be leveraged by attackers. In the federal agency context, authentication and authorization are provided authoritatively by the agencies themselves, requiring cloud computing environments to make calls back to them to validate the access a user is requesting. This allows them to enforce consistent and comprehensive access policies to applications outside of their traditional organizational network boundary.

2.3 Components of Zero Trust

Successful implementation of Zero Trust architecture requires a comprehensive and holistic implementation of various technical and organizational components into a cohesive security structure. NIST Special Publication 800-207 identifies several core elements of this

architecture that support continuous authentication and monitoring, coupled with risk-based authorization mechanisms.

There are three main components that facilitate these access decisions. The first is the Policy Enforcement Point (PEP). This is the mechanism by which user access is granted or denied, based on decisions made by the Policy Decision Point (PDP). The PDP is the point at which access policies created and managed in the Policy Administration Point (PAP) are evaluated and a decision to grant or deny access is made.

In conjunction with access policies, endpoint security mechanisms are continuously evaluating the security posture of the devices that are requesting access on the user's behalf. Some examples of these mechanisms are Endpoint Detection and Response (EDR) software, antivirus software, and configuration compliance tools such as Ansible. These tools can identify and report back anomalies to the organization prior to access being requested, blocking access to the network entirely.

Lastly, data security is a core component of Zero Trust architecture. Data is classified based on sensitivity and risk, and ensure this data is encrypted both at rest and in transit, with access to said data monitored continuously. This idea expands the boundary of protection from not only the network itself, but the data housed within the network as well. If an attacker were to gain access into the network, this data will not be easily accessible or exfiltrated.

3 Literature Review

Zero Trust architecture adoption has been increasingly recognized as the natural next step in approaching network security, as traditional perimeter-based security has been shown to be inadequate in protecting networks in the current technological environment. For federal agencies, Zero Trust has become the key focus in network modernization, driven by directives and mandates, past and current cybersecurity incidents, and the ever-evolving threat landscape.

3.1 Research on Zero Trust adoption

Research into Zero Trust adoption has shown that its adoption is a natural and necessary evolution to better secure enterprise networks. Namely, the NIST Special Publication 800-207 has become the de facto standard for how to implement Zero Trust within both the public and private sectors. The original introduction of the Zero Trust concept by Kindervag (2010) in their paper has been prolific in discussions on the topic. Kindervag asserted that internal networks themselves are not fundamentally trustworthy, and as such organizations should abolish the idea of "assumed trust" (Kindervag, 2010). This research laid the foundation for the current concept of Zero Trust as it is understood and applied today.

Jiang et al. (2023), argue that the cultural and organizational challenges to mature and comprehensive Zero Trust adoption are vastly underestimated. Although many facets of Zero Trust can be easily adopted, true Zero Trust maturity requires high levels of leadership buy-in, cross-organizational/team collaboration, and user awareness campaigns. Without these commitments organizational implementation of Zero Trust becomes siloed. This can result in true Zero Trust maturity across the federal government. Research into Zero Trust and cyber resilience has also yielded interesting insights. It was found that when organizations implement

Zero Trust principles across their network, there are significantly reduced opportunities for lateral movement within a network following initial network compromise (Ge & Zhu, 2023).

Ahn et al. (2010) had additional concerns with cloud service adoption and its impact on network security. With the migration of resources from internal networks to cloud solutions, traditional network boundaries have become obscure. The inability to exert complete control over resources outside of the organizational network boundary has given rise to identity-centric security a necessity.

Researchers have consistently acknowledged that implementation of Zero Trust architecture across federal agencies has remained siloed. Due to the disparity in mission, resources, funding, technical expertise, and current legacy support, most federal agencies are finding it difficult to implement Zero Trust architecture evenly.

3.2 Maturity assessment frameworks

The assessment of current and future Zero Trust maturity is essential to measure effectiveness of implementation as well as providing guidelines to future improvement. Maturity models such as the one defined by CISA and its 5 pillars provide agencies with well-defined methods to benchmark implementation progress as well as support consistent adoption across the federal government.

De Bruin et. Al (2005) argues that technical maturity alone should not be considered when developing a maturity model. Organizational awareness, policy enforcement, and operational alignment significantly influence the ability to mature an organization within a maturity model. Federal agencies could deploy advanced technical controls such as MFA or endpoint security but if they fail to enforce policies consistently, make users aware of the cultural

shift required, or fail to align operational processes with their vision, maturity cannot be achieved.

Additionally, these maturity assessment frameworks place heavy emphasis on a continuous improvement cycle. In order to adapt and evolve to meet the ever-changing threat landscape, achieving zero trust maturity is not a one and done ordeal. It requires constant development and enhancement to existing processes and technologies to ensure that gaps in security do not begin to appear after maturity is reached.

3.3 Implementation barriers

Although support for Zero Trust is broad, there are several barriers to implementation and maturity that severely complicate the ability for the federal government to implement Zero Trust across their networks. Factors such as organizational complexity, financial constraints, technical expertise, and legacy infrastructure severely limit the speed at which agencies can modernize their networks. This contributes to a relatively inconsistent implementation across the federal government.

Legacy infrastructure is one of the most concerning and prolific barriers. Many federal agencies are operating many of their systems and applications on dated hardware/software, some developed decades before any modern cybersecurity standards were established. These systems lack support for modern governance and management protocols, encryption ciphers, or APIs necessary to integrate with modern security mechanisms. Enhancing or replacing these systems would require a substantial financial investment. For legacy systems that are merely modified to support modern security mechanisms, a new host of concerns where the legacy infrastructure interfaces with modern infrastructure now emerges and requires consideration (Rose et al., 2020)

Organizational complexity can also influence the ability for a federal agency to reach full Zero Trust maturity. Complex organization structures in addition to siloed information systems/application development can severely limit the ability to effectively coordinate Zero Trust implementation. As a result, these limitations have been shown to be more of a challenge to address than the technical challenges themselves.

Technical expertise is another concern to successful implementation. Qualified personnel that can effectively and efficiently implement Zero Trust architecture are in short supply, which can further delay and degrade implementation efficacy. Furnell (2020) argues that the lack of qualified personnel not only slows implementation, but increases reliance on a contracted workforce, which can present its own risks through supply chain compromise.

Lastly, financial constraints remain a strong barrier for organizations to consistently apply Zero Trust architecture across the federal government. Each government agency is allocated its own budget, with some agencies receiving substantially higher budgets than others, depending on mission and allocation from Congress. This is acknowledged in the NIST Special Publication 800-207, which acknowledges that agencies with limited resources will face challenges in adopting Zero Trust at a standardized level.

4 Critical Success Factors

Achieving consistent Zero Trust maturity across all federal agencies requires a holistic, multi-facet approach. As a result, six key factors to success have been identified as essential to comprehensive, consistent Zero Trust maturity across the federal government.

4.1 Identity, Credential, and Access Management

Identity, Credential, and Access Management (ICAM) is the core success factor to Zero Trust implementation. This is due to the shift from perimeter-based network security to identity-centric security. For a mature Zero Trust agency, identity and access requests must be authenticated and authorized constantly, with other contextual factors such as location, device status, and login frequency being cited as requirements prior to accessing a resource. MFA has also been cited as a core component critical to successful Zero Trust implementation, which adds an additional layer of security to user accounts by requiring something they have in addition to something they know such as a password. Additionally, mechanisms such as Single Sign On (SSO) facilitate standardized authentication across information system by centralizing identity access policy enforcement. Lastly, limiting users to least-access privilege, with comprehensive and strict PAM enforcement ensures that damage caused though compromise is limited.

4.2 Endpoint and device visibility

Strict visibility into endpoint and device access is paramount to government having insight into all devices connecting to their network. Currently, thousands of devices and endpoints currently exist, and actively connect to agency networks. Zero Trust requires agencies monitor and maintain lists of all access requests to internal network endpoints. This ensures that all devices connecting to the network are appropriately patched, managed, and configured to limit vulnerabilities that can propagate from compromised devices into the main internal

network. EDR can significantly improve organizational security through collecting telemetry data from connecting devices and identifying and addressing anomalous events in real time. Additionally, as new devices connect to the network, they must remain visible to the agency as a precursor to access, ensuring the agency can deny access to devices that do not meet a defined security threshold.

4.3 Data classification and handling

Data protection is by extension a fundamental concept of Zero Trust architecture. Federal government agencies regularly store and process Personally Identifiable Information (PII), Personal Health Information (PHI), and sensitive information about military and diplomatic operations. Appropriately classifying and handling of sensitive data allows agencies to implement risk-based access controls that are set in accordance with the sensitivity of the data being secured. Based on the level of sensitivity, government agencies protect each level of data with differing and increasing security requirements, such as encryption at rest and in transit, secure communication protocols, and validation of access.

4.4 Automation, analytics, and continuous monitoring

Due to the high level of audit and transaction data collected by Zero Trust compliant systems, it would be impossible to manually review and analyze this data. Utilizing automated analysis and continuous monitoring, this data becomes actionable and leveraged to further secure the agency from compromise or extensive damage resulting from compromise. Continuous monitoring allows for real time collection and analysis of data, which can then identify and quarantine anomalous behavior prior to compromise. As a result, Indicators of Compromise (IoC) are identified and remediated quickly, minimizing the potential for damage. This can be

facilitated and even enhanced by AI to conduct predictive analysis on historical data to anticipate and identify compromise before it occurs.

4.5 Governance, leadership, and workforce readiness

Although technical advancements can assist in securing agency networks, these controls alone cannot achieve Zero Trust maturity. De Bruin et. Al (2005) argues that in order to effectively implement model maturity, every facet of the organization must be considered and addressed. Governance, leadership, and workforce readiness are strong requirements to ensure Zero Trust maturity, and without considering them this maturity cannot be achieved. Efforts must be coordinated across all departments of the agency, including cybersecurity, IT, HR, and operations. Leadership must be willing to commit resources not only for the immediate implementation of Zero Trust but continued financial support to ensure that support can be sustained. The governance process establishes the agency-wide policies and priorities for Zero Trust adoption and promote consistent implementation across various departments. Without formal governance policies, agencies will implement Zero Trust inconsistently.

4.6 Standardized cross-agency maturity assessment

In order to facilitate cross-agency collaboration, government-wide standards and benchmarks must be established. Agencies vary wildly in mission, size, and resources, so a consistent framework must be established to appropriately implement Zero Trust architecture. CISA provides a Zero Trust maturity model that helps facilitate Zero Trust adoption but lacks a mechanism or recommendation for how agencies should collaborate to ensure consistent implementation across the federal government. Research suggests that in order to facilitate better cross-organizational benchmarking, maturity assessments should evaluate organizational outcomes as opposed to current deployment status. An agency may show a high level of

operational maturity from their currently deployed technology, but the outcomes of these deployments may not reflect the same level of maturity Jiang et al. (2023). With cross-organizational collaborating and Zero Trust implementation, sustained cybersecurity resilience will exist throughout the federal government.

5 Recommendations

Clearly, achieving broad and consistent Zero Trust adoption across federal agencies requires comprehensive and fundamental changes to existing security policy and infrastructure. Identity modernization, endpoint visibility, improved data governance, enhanced automation, and consistent maturity benchmarks are a clear path forward to sweeping Zero Trust adoption.

5.1 Prioritize identity modernization

As the foundation for Zero Trust architecture, identity-centric network security should be the highest priority for federal agencies. This can be achieved through requiring MFA for all federal agency systems access. These MFA mechanisms should be phishing resistant and be tied to a user's identity through a smart card or security key. Risk based authentication should also be implemented across all networks, constantly evaluating contextual information to determine the level of verification required prior to access being granted. This approach not only improves security but minimizes the friction for users when accessing resources. For privileged users, secure PAM solutions should be implemented to ensure additional monitoring, and stricter authentication requirements when compared to traditional users. Lastly, wherever possible, ICAM systems should be consolidated to ensure consistent access policy enforcement across disparate applications and agencies.

5.2 Improve asset and endpoint visibility

Transparency into connecting assets and endpoints is a prerequisite for Zero Trust maturity to ensure that all external systems connecting to the internal network are trusted and appropriately secured. Continuous asset management that maintains a list of all authorized devices and applications should be established and maintained, with additional access controls or outright denials for unidentified devices attempting to access the network. Automation of

maintaining of this list should be implemented wherever possible to ensure new devices attempting to access the network are quickly identified and categorized based on their level of risk. EDR should be expanded to facilitate broad visibility into endpoint activity, enabling rapid identification and response to anomalous behavior. Devices connecting to the network must also be strictly managed by the agency and a baseline security configuration for these endpoints and devices should be established.

5.3 Strengthen data governance

Data governance policies must be strengthened to adhere to Zero Trust principles. Securing data in addition to the network itself allows for more granular access control, as well as minimization of damage caused by network compromise. Defining a clear data classification standard on how data should be labelled and what associated access controls accompany these labels should be established, with increasing security standards applying to increasingly sensitive data. Policies should also be established to promote cross-team collaboration across the agency, not just for the teams implementing the security measures.

5.4 Expand automation and analytics

Due to the increase of data collection from security auditing, device and endpoint connections, and need to expedite incident response, automated measures to collect, analyze, and address this data must be strengthened and expanded. Security, Orchestration, Automation, and Response (SOAR) tools should be leverages to automate routine security tasks. Implementing this capability can reduce response times, minimize loss, and allow incident response personnel to focus on higher priority tasks.

5.5 Develop consistent maturity benchmarks

A significant opportunity to ensure consistent Zero Trust adoption across all federal agencies lies in the development of comprehensive, standardized benchmarks for all federal agencies. Currently, Zero Trust adoption across federal agencies varies in maturity level. Establishing more actionable benchmarks for adoption would ensure that agencies are less concerned with "checking boxes," and more concerned with producing actionable insight that can be used to produce more accurate benchmarks of progress. Interagency collaboration should be included in these benchmarks, to not only allow accurate maturity analysis against peer agencies but facilitate information sharing to expedite consistent implementation of Zero Trust. Lastly, these benchmarks should be constructed in a way that facilitates and designates continued improvement. Reaching full Zero Trust maturity should be an ongoing evaluation, to ensure that agencies are remaining up to date on the current threat landscape.

6 Conclusion

Due to the current threat landscape, a shift from perimeter-based network security to identity-centric security is paramount to the current and future security of federal agencies. In order to facilitate this migration, Zero Trust architecture has been established as the foundation for federal agencies to implement. Guided by various mandates, memorandums, and executive orders, federal agencies are enhancing and replacing existing network security measures to adopt a more comprehensive, identity and data-based security model that assumes no entity connecting to their network can be trusted. Unfortunately, achieving full Zero Trust maturity across federal agencies remains a prevalent issue that requires a comprehensive shift and cross-agency collaboration to ensure consistent Zero Trust adoption across the federal government landscape. Critical success factors to Zero Trust adoption were identified through various sources, including government and peer-reviewed literature. The common thread throughout this literature demonstrates the need for a comprehensive, holistic approach to Zero Trust adoption that includes cross-agency collaboration, user awareness, and technical controls, in addition to governance improvement. ICAM was identified as the most foundational asset to prioritize in achieving full Zero Trust maturity, with the addition of endpoint security, automation enhancement, and comprehensive data governance. Several barriers to adoption were identified, with recommendations proposed to assist in the consistent implementation of Zero Trust architecture across federal agencies. Lastly, Zero Trust should result in a mindset shift within agencies, and after Zero Trust maturity is reached, continuous improvement of security and governance should be implemented to secure these agencies from future developments within the threat landscape.

7 Works Cited

Cloud Security Alliance AI Safety Initiative. (2026, June 3). *The hollowing of Cisa: Attrition, credential exposure, and defense risk* . Cloud Security Alliance. https://labs.cloudsecurityalliance.org/research/csa-research-note-cisa-institutional-capacity-systemic-risk/

de Bruin, T., Freeze, R. D., Kaulkarni, U., & Rosemann, M. (2005, January). Understanding the main phases of developing a maturity assessment model. https://www.researchgate.net/publication/27482282_Understanding_the_Main_Phases_of_Developing_a_Maturity_Assessment_Model

Furnell, S. (2021). The cybersecurity workforce and Skills. *Computers & Security*, *100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Ge, Y., & Zhu, Q. (2023, December 5). *Chapter 1 zero-trust cyber resilience*. Zero-Trust Cyber Resilience. https://arxiv.org/html/2312.02882v1

Kindervag, J. (2010, September 17). *No more chewy centers: Introducing the zero trust model of Information Security*. Palo Alto Networks. https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

Peisert, S., Schneier, B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C., Mannan, M., Mirkovic, J., Prakash, A., & Michael, J. B. (2021). Perspectives on the Solarwinds incident. *IEEE Security & Privacy*, *19*(2), 7–13. https://doi.org/10.1109/msec.2021.3051235

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *NIST Special Publication*. https://doi.org/10.6028/nist.sp.800-207

Takabi, H., Joshi, J. B. D., & Ahn, G.-J. (2010). Security and privacy challenges in Cloud Computing Environments. *IEEE Security & Privacy Magazine*, *8*(6), 24–31. https://doi.org/10.1109/msp.2010.186

The White House. (1998, May 22). *Critical Infrastructure Protection (PDD 63)*. Clinton Library. https://www.clintonlibrary.gov/sites/default/files/documents/pdd-63.pdf

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero Trust Cybersecurity: Critical Success factors and a maturity assessment framework. *Computers & Security*, *133*, 103412. https://doi.org/10.1016/j.cose.2023.103412