ALLIANCE FOR DIGITAL INNOVATION

Trust Redefined:

A Roadmap for Zero Trust Cybersecurity in the Public Sector

Overview

This paper covers a number of topics related to understanding and adopting a Zero Trust Architecture. The focus is to help public sector organizations at the federal, state, and local levels develop a roadmap for zero trust by understanding the following:

The Alliance for Digital Innovation

What Is Zero Trust Architecture?

ZTA Empowers Digital Transformations

The Federal Approach to ZTA

State and Local Approaches to ZTA

Developing a ZTA Roadmap

How to Acquire ZTA Capabilities

Improve Government Workforces to Optimize the Benefits of ZTA

Introduction

There's an old Russian proverb used by Ronald Reagan while he negotiated the Intermediate-Range Nuclear Forces (INF) treaty with Mikhail Gorbachev in 1987, "Trust but Verify." While this phrase illustrated the relationship that became the cornerstone of our nuclear peace agreement with Russia, it does not meet the mark with our current approach to cyberspace. In fact, a few years ago the National Institute of Standards and Technology (NIST) updated the phrase to reflect the modern approach to cybersecurity: "Never Trust, Always Verify."[1] Then, in the wake of the Solar Winds cybersecurity incident in which a supply chain compromise impacted thousands of organizations including the U.S. federal government,[2] the federal government codified the movement to a zero trust approach in section 3 of Executive Order 14028, *Improving the Nation's Cybersecurity.*[3] This "zero trust" approach to enterprise cybersecurity highlights the unique nature of operating in a digital environment, where identities and interactions are much easier to fake or obfuscate.

Zero Trust Architecture (ZTA) has become the focus for public sector organizations as government services and work have increasingly moved online in recent years, at first out of necessity because of the pandemic, and then to improve the quality and ease of accessing services for citizens. Advancements in technological capabilities, including everything from Artificial Intelligence (AI) and natural language processing systems to cloud-based services, have made it easier and more efficient for states to offer online services. Additionally, remote work options have also become a norm and a necessity to bolster the workforce.

---

1 https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify
2 https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic
3 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cyber-security/

While these changes have been beneficial and necessary, the lack of the application of best practices and cyber hygiene have increased cybersecurity risks and widened the attack surfaces for adversaries and have put more Americans' data and critical infrastructure at risk. One powerful way to mitigate these threats and reduce the impact of a successful attack is through the adoption of Zero Trust Architecture.

Deploying ZTA is inherently collaborative and must involve all levels of government. A comprehensive approach will also need to focus not only on security, but also on acquisition processes and upskilling the work force to support the initiatives. Implementing a stronger and more defensible infrastructure will take time and effort but will mean greater cybersecurity and greater peace of mind.

The Alliance for Digital Innovation

The Alliance for Digital Innovation (ADI) is a nonprofit coalition of innovative, commercial companies whose mission is to bring IT modernization and emerging technologies to government. ADI member companies include a wide range of cloud service providers, small and midsize innovative integration companies, and other innovative technology companies, all supporting the public sector. Our members provide key critical technologies at all levels of the government's technology stack, including cloud infrastructure, digital identity, human resources software, quantum computing, digital services, and a range of sophisticated cybersecurity tools and services critical to public sector missions. Our goal is to break down institutional, systemic, and legal barriers to bring the technological advancements in commercial innovation to the public sector and help build a modern, 21st century digital government.

What Is Zero Trust Architecture?

Imagine a castle with high walls and a moat to repel invaders. This familiar concept of a strong perimeter defense protected government organizations for centuries, until advances in military technology made such strongholds antiquated. Similarly, early cybersecurity philosophies embraced the idea of establishing a strong perimeter defense to keep malicious actors from accessing sensitive information.

Zero Trust Architecture, on the other hand, assumes that there is no "safe zone." It is based on the concept that no device, application, or individual user should be assumed to be trustworthy, and that every user and system trying to access any resource within a secure network environment should be evaluated and validated, regardless of whether they originate from inside or outside the network.[4] Just as you would not assume someone is trustworthy because they made it inside the castle walls, organizations that have adopted ZTA do not trust any device, network, user, or service by default, even if they are inside the network. Organizations that have adopted ZTA continually verify and validate the identity of everyone and everything on their network.

Because there is no one solution to achieve ZTA, organizations implementing ZTA should focus on the five pillars of zero trust, which are identity, devices, networks, applications, workloads, and data. Implementing ZTA across government is a multi-step process that involves multiple teams, collaboration between public and private sector entities, and technologies.

ZTA Empowers Digital Transformations

Government services have been migrating services online as part of their digital transformation and IT modernization initiatives. Services that previously may have been available only in person are being moved online by digital transformation. This enables residents to conduct transactions online rather than going somewhere in person and waiting in line. This involves moving on-premise applications and systems to the cloud to enable greater scalability and flexibility. All of these changes require a cybersecurity transformation, and Zero Trust should be built into the process of modernizing and replacing legacy systems.

---

4 In its Special Publication 800-207, the National Institute of Standards and Technology (NIST) defines zero trust as "a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decision in information systems and services in the face of a network viewed as compromised."

Digital transformation and IT modernization combined with the increase in attacks targeting state and local governments make clear that strong security solutions are necessary. ZTA takes a comprehensive approach to cybersecurity to help mitigate the impact of future breaches. Components of ZTA include:

	ZTA	Impact
Micro-segmentation	Micro-segmentation of networks ensures that users only have access to specific parts of the network that they need, known as the principle of least privilege, and restricting access between them.	Adversaries are less likely to be able to make lateral movements within the network, even if they gain access to parts of the network, thereby limiting the impact of unauthorized access.
Authentication and access controls	Strong authentication mechanisms, such as MFA, ensures that only authorized users with the proper credentials and additional verification factors are granted access to networks. Additionally, implementing fine-grained authorization will enable granular access control based on varied factors.	Reduces the likelihood that adversaries can use compromised credentials to access networks.
Third-party application security	Third-party applications and their updates are subject to greater control and oversight.	Reducing the chances that adversaries can take advantage of these applications.
Continuous monitoring and risk assessments	Systems continuously monitoring network activity and user behavior to detect and flag anomalous or suspicious activity quickly.	Allows for faster response times during a cyberattack or intrusion.

While there is no way to prevent all cyberattacks and intrusions, ZTA — which assumes that such an event has already occurred or will occur imminently — takes steps to mitigate the impact of adversarial activity within the network.

Furthermore, the different components of ZTA make it modular, and solutions need to be tailored to protect and empower different technologies, such as:

1. **Cloud-Delivered Applications.** As more government operations move to cloud services and rely on cloud applications, ZTA must be a foundational philosophy. It is important to ensure that communications between different cloud services are secure and to maintain more granular access control. Cloud-delivered applications are also more dynamic and modular than on-site solutions; thus ZTA is needed to ensure that security is easily maintained even in a changing environment. Authentication and authorization are particularly important for online services using citizens' identities to deliver services, online signatures, or other such factors.
2. **Secure Remote Access to Systems.** ZTA helps mitigate the risks associated with remote work and remote network access, which state and local governments are increasingly embracing to bolster workforces. Specifically, ZTA uses a "perimeterless" approach to security, treating every access request as potentially adversarial regardless of location. Additionally, ZTA relies on fine-grained authorization and continuously authorizing users, which is necessary when users are accessing the network from distinct locations or devices.
3. **Endpoint Detection and Response (EDR).** EDR is the cybersecurity approach to defending from malicious activity the physical devices that connect to a network such as desktops, laptops, and mobile devices. Given that organizations today have so many connected devices, EDR is a critical part of a zero trust journey. A robust EDR solution is key to identifying/preventing threats and enabling threat hunting activities if a malicious actor gains unauthorized access to systems.

4. **Mobile Applications and Digital Services.** As more services move online, the number of network access points for adversarial actors increases, requiring additional security measures. MFA and fine-grained authorization enable organizations to know who is accessing what information.
5. **Monitoring and Logging.** ZTA requires continuous monitoring and logging of users, access requests, and network traffic to detect anomalous activity. This improves the capacity to see which users are accessing the network, and where, how, and when access is happening.[5] Logging also enhances investigation and remediation during security incidents and events.

The Federal Approach to ZTA

President Biden's recent Executive Order on cybersecurity mandates ZTA for federal agencies and thus spurred the release of documents from different federal agencies.[6] Several federal guidelines provide details on implementing Zero Trust. The National Institute of Standards and Technology (NIST) outlines the core tenets of Zero Trust in Special Publication 800-207:[7]

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communication and uses it to improve its security posture.

These tenets are all technology-agnostic, and they can and should be incorporated into ZTA in a variety of ways. The specific tools used should be tailored to the needs of the specific network and information being protected.

Additionally, CISA's Zero Trust Maturity Model[8] refers to these NIST guidelines and the EO mandates that federal agencies adopt or bolster their ZTA. There's also White House Office of Management and Budget Memorandum 22-09 that details Zero Trust principles.[9] While these publications were written for federal agencies, the guidance is also beneficial to state and local governments. Moreover, a more robust and mature ZTA may lead to easier cooperation with the federal government as well as a stronger case when seeking federal funding for IT projects.

State and Local Approaches to ZTA

Public sector organizations around the world are at the forefront of implementing zero trust, according to a recent report from Okta.[10] The U.S. government has rolled out guidance and best practices for using zero trust across federal agencies and in recent years, and states have begun adopting zero trust mandates through legislation and executive action.

ADI has supported zero trust legislation and collaborating with policymakers to ensure that states are adopting best practices around the country. In 2023, Utah became the first state in the nation to codify ZTA as a strategic technology priority, and agencies must now consider giving preference to third-party cloud providers and other vendors that meet industry standards promulgated by organizations such as the Federal Risk and

5 https://www.nccoe.nist.gov/sites/default/files/2022-07/zta-nist-sp-1800-35b-preliminary-draft.pdf
6 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
7 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
8 https://www.cisa.gov/zero-trust-maturity-model
9 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
10 https://www.okta.com/sites/default/files/2022-09/OKta_WhitePaper_ZeroTrust_H2_Campaign_.pdf

Authorization Management Program (FedRAMP) management office and NIST.[11] Maryland adopted similar legislation for its public utilities,[12] with other states likely to follow suit in 2024.

Fig. 1 – States with Recent Zero Trust Legislation

State	Bill	Summary	Status
California	AB 749 (2023)	Requires state agencies to implement ZTA; must achieve "Initial" maturity by 2024 and "Optimal" maturity by 2030	Passed Assembly*
Maryland	HB 969 (2023)	Critical infrastructure would require public service companies to implement ZTA; mandates incident reporting and coordination of remediation plans	Signed by Governor
Utah	HB 545 (2023)	Requires the state CIO to develop uniform standards for state agencies to implement ZTA, including at a minimum multi-factor authentication, cloud-based enterprise endpoint detection and response solutions, and robust logging practices	Signed by Governor

*https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=202320240AB749

This increased focus by states on ZTA is not limited to state agencies; there have also been efforts to extend the mandates to critical infrastructure. In Maryland, public service companies such as water and energy utilities must now adopt ZTA, meet minimum standards, report cybersecurity incidents to the Maryland Public Service Commission, and work with state officials to address vulnerabilities through remediation plans. ADI supported this legislation because mitigating cyber risk for public utilities represents a critical step in achieving a "whole of government" approach to cybersecurity.

It's also important to promote collaboration across an entire state. Last year, Virginia became one of the first states to mandate that all public bodies—including entities from state government, local government, K-12, and higher education—report cybersecurity incidents to a single point of contact at the state level to improve awareness and coordination of resources.[13]

Other states have adopted legislation creating new entities to promote a collaborative approach to cybersecurity. Oregon's House Bill 2049, while not mentioning ZTA specifically, presents a holistic approach to a "whole of state" cybersecurity that includes solutions for workforce, public partnerships with state agencies, higher education, and the private sector.[14] In Washington, the recently passed Senate Bill 5518 establishes a new cross-functional advisory body for public sector cybersecurity that will provide recommendations on how to improve cybersecurity across the public sector, private industry, and critical infrastructure.[15] Although these bills do not mention ZTA explicitly, the improved collaboration will facilitate their efforts to implement ZTA in the future.

From an operations standpoint, California has taken steps to create an enterprise-wide approach to ZTA. In May, the California Department of Technology (CDT) issued Technology Letter 23-01,[16] which established new requirements for identity and access management, including multi-factor authentication (MFA). Going forward, CDT will require state agencies to meet the "Initial" ZTA maturity stage as defined by the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model Version 2.0 by spring 2024, with a formal

11 https://le.utah.gov/~2023/bills/static/HB0545.html
12 https://mgaleg.maryland.gov/2023RS/bills/hb/hb0969E.pdf
13 https://lis.virginia.gov/cgi-bin/legp604.exe?221+sum+SB764#
14 https://olis.oregonlegislature.gov/liz/2023R1/Measures/Overview/HB2049
15 https://app.leg.wa.gov/billsummary?BillNumber=5518&Year=2023&Initiative=false
16 https://cdt.ca.gov/technology-letter-23-01/

timeline for state agencies to achieve "Optimal" maturity by the end of the decade.[17] It is excellent news that California prioritizes solutions that meet robust cybersecurity standards.

Similarly, the state of New York has incorporated ZTA into its New York State Cybersecurity Strategy released by Governor Kathy Hochul in August 2023.[18] In addition to the modernization of its networks, state leaders will pursue ZTA maturity by "updating legacy software, hardware, and operational paradigms with new systems that offer better performance and security."[19]

Illinois faced an all-too-familiar challenge during the pandemic when it needed secure but simple means for employees to access systems.[20] This required them to begin their zero trust journey and adopt a new approach to securing its systems. For example, the state deployed a single sign-on solution that supported Illinois's zero trust environment by authenticating every user who seeks access to the state's closed network. It worked so well for employees that the state rolled it out for its 13 million residents.

The City of Los Angeles and the State of Oklahoma are other examples of governments that quickly adapted to work from home needs during the pandemic by deploying new services that improved their Zero Trust maturity. These new cyber capabilities enabled greater control over who has access to various parts of the government networks.[21] Additionally, Matt Singleton, CISO for the Office of Management and Enterprise Services in Oklahoma, stated that, "The integration of the different platforms is giving us unprecedented visibility into the environment. We can respond faster. In some cases, we can forecast where we may have issues, and address those things before they become a problem."[22]

North Dakota Information Technology (NDIT) is another government enterprise that has begun to transform their cybersecurity profile to increase their visibility and security throughout their network.[23] To that end, NDIT has implemented tools for detecting threats through behavioral analytics and tools that abide by the principles of Zero Trust, such as least-privileged access controls, across their networks. "We've learned that Zero Trust is even more than a technology. It's also about personnel. It's ideation that people have to adopt. As much as a technology shift, it's meant a culture shift for our team, our vendors, and our users," said Ryan Kramer, Enterprise Infrastructure Architect with NDIT.

Themes and lessons learned have emerged from these early approaches to state cybersecurity, and more will continue to emerge as more states join the ranks and legislation comes into full effect. ZTA adoption cannot be optional or aspirational, and legislation must mandate best practices such as MFA and Endpoint Detection and Response (EDR) to be effective. Legislation must also include "whole of state" solutions, such as emphasizing collaboration, eliminating arbitrary local/state government silos, information sharing, and pooling resources through shared services. Last, states must develop funding models to give cyber leaders the resources to implement necessary changes and to be able to prioritize vendors that meet ZTA standards.

Developing a ZTA Roadmap

These are examples illustrating that one solution will not fit all needs; therefore public sector organizations need to approach Zero Trust piece by piece. To fully appreciate the benefits of Zero Trust, it can be helpful to develop a roadmap for implementation.

---

17 https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
18 https://www.governor.ny.gov/sites/default/files/2023-08/2023-NewYork-CybersecurityStrategy.pdf
19 https://www.governor.ny.gov/sites/default/files/2023-08/2023-NewYork-CybersecurityStrategy.pdf at p. 8
20 https://statetechmagazine.com/article/2023/04/single-sign-applications-support-zero-trust-state-agencies
21 https://www.zscaler.com/customers/city-of-los-angeles
22 https://www.zscaler.com/customers/state-oklahoma
23 https://www.paloaltonetworks.com/customers/northdakota

A roadmap is necessary to provide clear direction for all stakeholders and ease the transition. Zero Trust implementation will not happen at the push of a button and requires careful consideration to allow it to effectively protect networks. In the initial stages of implementation, the roadmap should emphasize:

1. Inventory of existing hardware, networks, and available tools and prioritization of needs to understand which networks require most immediate attention based on vulnerabilities. Prioritize any connected applications, services, and devices that access internal network resources.
2. Building in Zero Trust throughout IT modernization processes to ensure that the transition is smooth and modern technology receives necessary security protections. Avoid more variable funding sources such as General Funds and instead establish dedicated funding resources to facilitate long-term modernization projects and securing the latest technologies.
3. Coordination and collaboration across IT systems to ensure that all stakeholders are involved, particularly focusing on integration between state and local governments. This will help ensure a more integrated approach to identifying existing resources and gaps in developing the roadmap.
4. Creating a phased approach to Zero Trust implementation because it will break the rollout into manageable steps and provide appropriate times to measure success and readjust the roadmap if necessary.
5. Engaging in training for employees who are tasked with deploying and maintaining ZTA. Training will also be necessary for employees who will use new features.

Recommendations

- Develop a Zero Trust Implementation Roadmap
- Involve a diverse set of stakeholders
- Incorporate a Zero Trust philosophy into any new technology deployment
- Establish dedicated funding resources

How to Acquire ZTA Capabilities

Procurement is a crucial factor when developing and maintaining ZTA, and trust in the process is paramount.

States must build mature, integrated contracting practices where cybersecurity governance and expertise are included from the outset rather than tacked on at the back end, which can lead to delays.

Considerations should include:

1. Evaluating a vendor's approach to appropriate aspects of ZTA, including identity access management, network security, and data protections, and how much custom control the government would be able to have.
2. Assessing whether IT solutions align with established Zero Trust principles and integrate into broader ZTA.
3. Collaborating with vendors efficiently during acquisition processes to align their solutions with the government's ZTA through security assessments or other means. Custom solutions may be necessary and become more cost effective through whole-of-state approaches.
4. Requiring that any new IT system is interoperable within multi-vendor ecosystems to ensure the ability to appropriately share information and provide effective digital services.

Taking these factors into account when acquiring new IT solutions will lead to a smoother and quicker transition to Zero Trust. However, it is time-consuming and expensive to start from scratch with every procurement, so governments should strongly consider utilizing cooperative efforts, such as StateRAMP, to shorten their acquisition cycle and reduce costs.

StateRAMP, much like FedRAMP for federal agencies, enables vendors to demonstrate that they meet certain security, cloud compliance, and risk management criteria to participating government agencies, allowing for a more efficient procurement process. This is also why a whole-of-state approach is important; it reduces the number of procurement processes that state and local governments must undergo and allows them to leverage their joint powers in these processes.

Finally, Zero Trust is also important to incorporate into future acquisitions. ZTA-enabling tools can be used to ensure that any new systems or tools that are purchased are not compromised or cannot be used to compromise a network. This can be vital in the acquisition processes because it may be harder to assess new systems where vulnerabilities are unknown.

Recommendations

- Utilize cooperative efforts and a whole-of-state approach to shorten acquisition cycles and reduce costs
- Require that new applications be interoperable with existing systems

Improve Government Workforces to Optimize the Benefits of ZTA

A strong workforce is paramount to realizing the full potential of ZTA. First, the proper IT and cybersecurity teams are needed to design and plan Zero Trust systems, define internal policies that govern ZTA implementation, ensure that they meet specific standards, and engage in the technical implementation. Once the implementation is complete, there's maintenance, where teams are then needed to respond to flagged incidents, audit the system to ensure everything is working properly, and update ZTA systems.

The public sector, however, is facing a deficit in qualified IT and cybersecurity employees. A federal report published in April 2022 found that the public sector deficit was 40,000 jobs and the overall deficit throughout the country was 700,000 jobs.[24] These numbers have increased since the report was published, as new and increasing technological needs arise. This also means that governments already lack a qualified workforce and are competing with private sector employers.

To address this deficit, governments should engage in reskilling the existing workforce to fill the growing need for IT and cybersecurity experts and ensure that the existing workforce has sufficient support. There are several ways to achieve these goals:

1. Offer opportunities for reskilling and learning through certifications, apprenticeship programs, workshops, or participation in industry conferences.
2. Encourage cross-functional collaboration with other stakeholders to develop more holistic understandings and for knowledge sharing.
3. Define clear roles and responsibilities to identify skill and workforce gaps.
4. When appropriate, engage in testing and training simulations to ensure a ready workforce.
5. Develop platforms or other methods to share information and best practices across an ecosystem and various levels of government, which is particularly necessary for a whole-of-state approach.

These steps and other efforts can and should be taken to mitigate the impact of workforce gaps to ensure that ZTA is properly implemented and maintained throughout ecosystems.

---

24 https://niccs.cisa.gov/

Recommendation

- Engage current workforce in reskilling and knowledge sharing opportunities to mitigate workforce gaps.

Conclusion

Malicious actors are not going anywhere. It's critical that public sector entities take steps to enhance their cybersecurity. Implementing ZTA can go a long way toward improving government security. As more services move online and adversaries become more advanced, public-sector organizations need to take the necessary steps to ensure that systems and applications are protected while also ensuring secure access for users.

Organizations should invest the time and resources to implement ZTA. The journey to a fully implemented ZTA will take time to achieve. The good news is that everything does not need to be done at once and every incremental step toward ZTA will benefit policymakers, public employees, and residents by improving cybersecurity across the jurisdiction.

The steps in the journey include developing a roadmap, leveraging the acquisitions process, and focusing on bolstering the workforce.