# Defining Zero Trust:

Industry Approaches and Policy Frameworks
for Strong Wireless Network Security

# Table of Contents

# Introduction

Zero Trust ("ZT") is an important concept that has existed in security frameworks for decades. As the wireless industry continues evolving its networks with increasingly advanced technology, Zero Trust is receiving greater attention—particularly in policy discussions around cybersecurity, where "Zero Trust" has become a high-profile buzzword. Unfortunately, an incomplete understanding of the variations in Zero Trust terminology, the application of Zero Trust concepts, and the varied approaches required for Zero Trust implementation across different network builds, can complicate efforts.

To ensure Zero Trust is more than just a buzzword, this overview arms policymakers with the tools they need to understand the concept and the practical realities behind its implementation.

To help drive more robust discussions around Zero Trust, this paper will:

1. **Clarify how Zero Trust principles and their implementation advance network security;**
2. **Summarize Zero Trust's existing implementation** and continued evolution in the wireless ecosystem through proactive industry efforts and partnerships;
3. **Define and clarify the differences between the vocabulary primarily used in Zero Trust discussions,** including Zero Trust, Zero Trust Architecture ("ZTA"), and Zero Trust Network Access ("ZTNA");
4. **Identify variations in Zero Trust use cases,** including implementation in 5G networks;
5. **Outline the current Zero Trust regulatory landscape and where improvements should be made;** and
6. **Make policy recommendations to government** to maintain flexibility, encourage customization in organizations' migration to Zero Trust and development of Zero Trust Architectures, and avoid mandates or "one-size-fits-all" solutions.

# What Is Zero Trust?

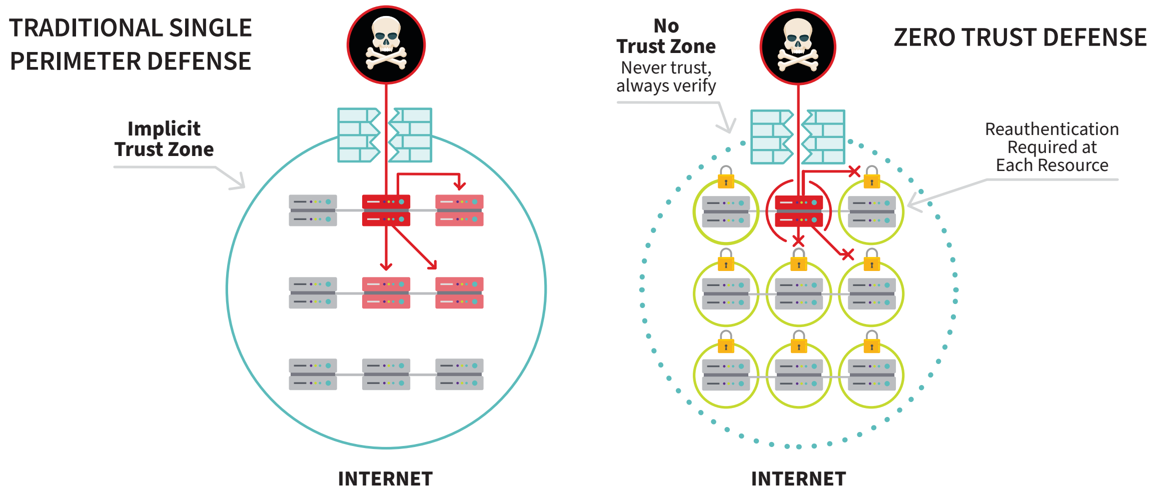
Zero Trust is an information security philosophy based on a set of concepts—it is not a single solution, architecture, or end state. Zero Trust is a set of core principles designed to address challenges in network security by requiring continuous verification for all users, applications, and any associated devices as they access different parts of a network and corresponding network functions.

Information or network security as we experience it every day relies on knowing whether a particular user, device, or application is authorized to access an information system or the information stored on that system. For most users, this means we have a username or other account to log into a network, or a profile on our laptop or mobile device.

From this single point of entry, networks or devices are usually configured to allow access to particular information, applications, or networks based on the known aspects of that user. Traditionally referred to as “single perimeter defense,” this method is sometimes colorfully termed a “castle-and-moat” network security model—because once the “moat” barrier is crossed, users or devices have full access to the “castle” within.

As we know, criminals or spies can steal account information and passwords, and use them to log into an information system while posing as an authorized user. Because so many networks are set up to “trust” users, devices, and applications that have presented satisfactory credentials—that is, to allow access throughout the system based on the initial gatekeeping function of the account or user information—compromised credentials or devices enable bad actors or malicious software to get around many of the security features of a network.

Zero Trust aims to address these risks through core principles that require continuous verification for all users, applications, and any associated devices as they access different parts of a network and corresponding network functions. For the average user, these verification processes run in the background through various authentication and authorization control protocols based on the risk and needs of the network.


TRADITIONAL SINGLE PERIMETER DEFENSE
Implicit Trust Zone
INTERNET
No Trust Zone
Never trust, always verify
ZERO TRUST DEFENSE
Reauthentication Required at Each Resource
INTERNET

*Graphic based on NIST image, available at https://www.nist.gov/image/zero-trust.*

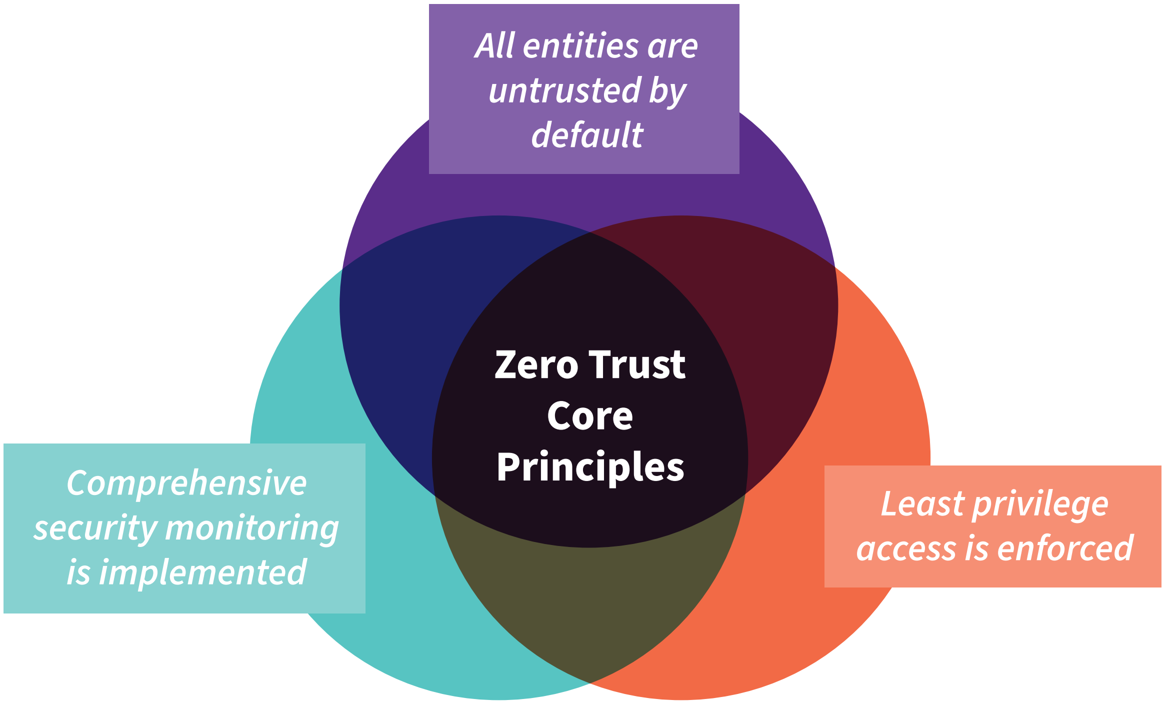
## Key Zero Trust Principles and Concepts to Enhance Network Security

As described by the National Institute of Standards and Technology ("NIST"), Zero Trust is best understood as a set of concepts and ideas that "assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location . . . or based on asset ownership. . ."[1]

In other words, when users are authorized to enter a network built around Zero Trust principles, they are not automatically granted permission to access the data, services, or other resources within the network. Rather than trust every user by default once they have been authorized for initial entry, ZT-based networks treat every user with suspicion at all points within—that is, they treat users with "zero trust"—and all users, applications, or devices require repeated authentication and authorization each time they attempt to access a new part of the network or its data, services, applications, or other assets.

Popularized by Forrester analyst John Kindervag,[2] there is general consensus that Zero Trust reflects three core principles:

1. **Assume Untrusted.** All entities on a network are untrusted by default, even if previously authorized.
2. **Minimize Access.** Least privilege access is enforced—that is, users, applications, and devices are given authorization for access at their correct level, never more.
3. **Constantly Monitor.** Comprehensive security monitoring is implemented to continuously validate users, applications, and devices.


All entities are untrusted by default
Comprehensive security monitoring is implemented
Zero Trust Core Principles
Least privilege access is enforced

[1] *See* NIST, *Zero Trust Architecture*, Special Publication 800-207 at *ii* (Aug. 2020) ("NIST 800-207").

[2] David Holmes and Jess Burn, "The Definition of Modern Zero Trust" (Jan. 24, 2022), https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/.

## Network Operators Design ‘Zero Trust Architectures’ Based on the Core Principles of Zero Trust

As further described in a later section, the systems that network operators implement around Zero Trust principles are called Zero Trust Architectures, or ZTAs. Because each network has different capabilities depending on its structure, equipment, and systems, ZTAs inherently differ to meet each network’s particular needs.

As Zero Trust continues to evolve, there is no single approach to designing ZTAs. However, NIST has identified seven basic tenets that help inform the design and deployment of an organization’s ZTA:

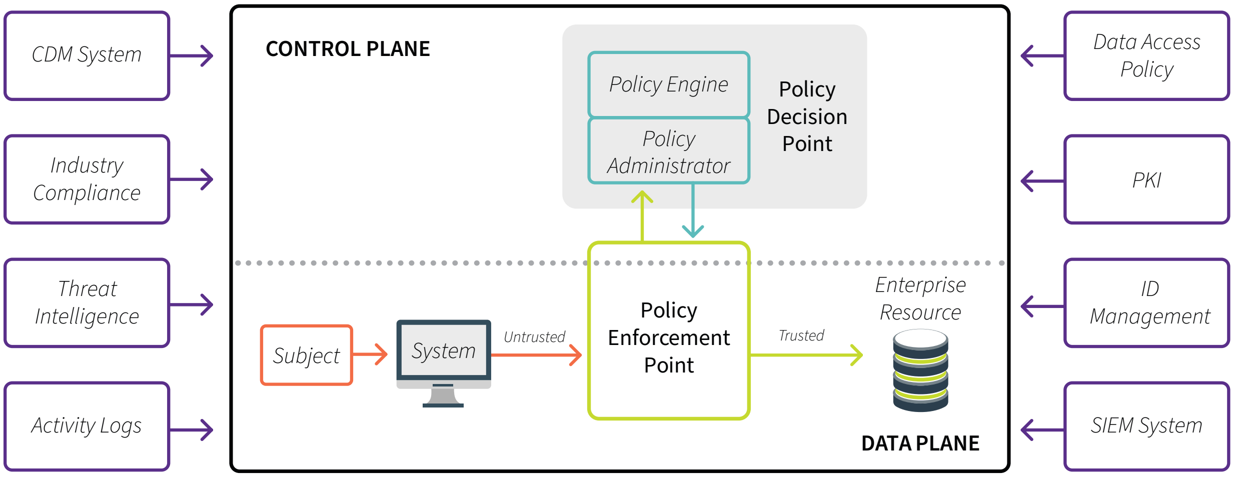
1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—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 communications and uses it to improve its security posture.[3]

As NIST describes, “Zero trust (ZT) 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. Zero trust architecture (ZTA) is an enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.”[4]

Put another way, a ZTA is how an organization applies the Zero Trust concepts to its own networks. The picture below shows the logical components of a Zero Trust Architecture, as defined by NIST.

[3] NIST 800-207 at 6-7.

[4] NIST 800-207 at 4.



*Graphic based on NIST image, available at https://www.nist.gov/image/zero-trust.*

Two key aspects of Zero Trust are critical.

***First, flexibility is a fundamental part of Zero Trust.*** Zero Trust principles guide and inform organizations as they develop and implement ZTAs that are appropriate for their risk profile and context. There is no single ZTA that policymakers can point to or that organizations can simply implement. Rather, "a [ZTA] uses [ZT] principles to plan industrial and enterprise infrastructure and workflows."[5]

As NIST describes, "ZT is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture."[6] Each organization's Zero Trust Architecture and implementation will be inherently unique.

***Second, Zero Trust is a process, not an end state.*** It is important to understand that "[a]chieving zero trust will not be a static achievement with a single finish line. Instead, zero trust will [. . .] evolve with changes to both the technology and threat landscape."[7]

For these reasons, it is not ideal to ask the binary question of whether an organization, agency, or system has achieved Zero Trust. The focus instead should be on the process the organization is using to adapt its infrastructure and policies to Zero Trust concepts, and the outcomes it is seeking to achieve through that work.

[5] NIST 800-207 at *ii*.
[6] NIST 800-207 at 1.
[7] *See* NSTAC, *Zero Trust and Trusted Identity Management*, Report to the President at 4 (Feb. 2022) ("NSTAC ZT Report").

# Zero Trust and the Wireless Industry

## Zero Trust Is Not New to the Wireless Sector.

As Zero Trust terms have become increasingly popular in government discourse around network security, vendors and service providers are emphasizing that their security offerings are consistent with Zero Trust or able to meet the government's or companies' Zero Trust needs. It is important for policymakers to understand that while the *emphasis* is new, zero trust *implementation* is not—in fact, the concept is nearly three decades old.

Zero Trust dates to the mid-1990s[8], and the wireless industry has long embraced evolving security approaches that are consistent with Zero Trust principles, even predating the current focus on Zero Trust implementation. For example, the wireless industry has supported the development of mutual authentication techniques, where the network must authenticate the device and the device must authenticate the network.

Today, the wireless industry is leading the way in exploring and evolving Zero Trust principles, both in industry standards bodies and in partnership with government. Specifically, the industry drives Zero Trust concepts and ZTA implementations in several contexts, including, for example, when providers embrace Zero Trust principles in their own networks, when the wireless industry develops and offers tools to assist enterprises in implementing Zero Trust principles, and when the industry collaborates with government and standards bodies to help drive ongoing innovation.

## The Wireless Industry Is Working in Partnership with Government and Standards Bodies to Advance Zero Trust.

The wireless industry, along with the broader private sector, has been advancing Zero Trust in various venues and through active involvement with numerous standards bodies and federal advisory groups.

***ATIS.*** An example of the wireless industry's ongoing work on Zero Trust is its involvement with the Alliance for Telecommunications Industry Solutions ("ATIS") and its Technology & Operations Council. The group is working on a project that, among other things, examines 5G Zero Trust solutions and how they can be integrated with other Zero Trust solutions that might be adopted throughout IT infrastructure, such as cloud deployments and enterprise IT.[9]

***The Alliance for Telecommunications Industry Solutions (ATIS) is a partnership of leading global telecommunications and information technology companies that develops standards and technical solutions.***

[8] Stackscale, "What is the Zero Trust security model?" (Dec. 2021), https://www.stackscale.com/blog/zero-trust-security/.

[9] ATIS, "Enhanced Zero Trust and 5G" (accessed Nov. 2022) ("ATIS Enhanced Zero Trust and 5G"), https://www.atis.org/tops-council/enhanced-zero-trust-and-5g/.

ATIS also has released publications related to Zero Trust that make important contributions and should be incorporated into future federal government Zero Trust guidance documents.[10]

***The Communications Security, Reliability, and Interoperability Council (CSRIC) is a federal advisory committee that brings together private sector and government experts to provide advice to the FCC on the security, reliability, and resiliency of the nation's communications systems.***

***CSRIC.*** Through its involvement with the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council ("CSRIC"), the broader telecommunications industry has developed valuable best practices that should be leveraged by the federal government in its transition to ZTA, as well as by policymakers considering Zero Trust principles more generally. The industry's work on Zero Trust in CSRIC has also included discussing the importance of Zero Trust principles in implementation guidance for cybersecurity risk management through NIST's Cybersecurity Framework ("CSF").[11]

***NSTAC.*** Similarly, the National Security Telecommunications Advisory Committee's ("NSTAC") Report to the President on Zero Trust and Trusted Identity Management ("NSTAC ZT Report"), guided by industry input, is intended to provide agency-level recommendations to "help catalyze cybersecurity transformation through zero trust adoption,"[12] it can also serve as a general resource to policymakers, as it compiles industry standards and best practices for Zero Trust implementation.[13]

***ESF.*** The Enduring Security Framework ("ESF"), "a cross-sector, public-private working group which provides cybersecurity guidance that addresses high priority cyber-based threats to the nation's critical infrastructure," has developed a four-part series that provides cybersecurity guidance to support the deployment of 5G cloud infrastructures.[14] This series generally aligns with NIST's Zero Trust work and addresses four principles related to 5G cloud security: (1) prevent and detect lateral movement; (2) securely isolate network resources; (3) protect data in transit, in-use, and at rest; and (4) ensure integrity of infrastructure.[15] Further, these publications "document best practices that strive to bring a Zero Trust mindset into 5G cloud endpoints and growing multi-cloud environments."[16]

[10] E.g., ATIS, *ATIS Standard: 5G Network Assured Supply Chain* at 82 (June 2022), https://access.atis.org/apps/group_public/download.php/66150/ATIS-I-0000090.pdf (identifying 5G core architectural and security enhancements that "provide micro-segmentation using various zero-trust techniques to provide authentication, integrity, and confidentiality protection between functions of the system to further limit lateral movement of compromised software"); *see also* ATIS, *Collaborative DevSecOps in a Service Provider Environment*, at 4 (Mar. 2021), https://access.atis.org/apps/group_public/download.php/58287/ATIS-I-0000082.pdf ; ATIS, *Multi-Network Enterprise Solutions*, at 28 (July 2021), https://access.atis.org/apps/group_public/download.php/60538/ATIS-I-0000086.pdf.

[11] *See, e.g.*, CSRIC IV Working Group 4, Final Report: Cybersecurity Risk Management and Best Practices, at 263, 266, 268, 280, 295 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[12] NSTAC ZT Report at ES-1-2.

[13] NSTAC ZT Report at 4-9

[14] CISA, "NSA and CISA Provide Cybersecurity Guidance for 5G Cloud Infrastructures," (October 28, 2021) https://www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures

[15] ESF, Security Guidance for 5G Cloud Infrastructures, Part 1: Prevent and Detect Lateral Movement (2021) at 1-2, https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_I_508_Compliant.pdf.

[16] CISA and NSA, "Security Guidance for 5G Cloud Infrastructures Part III: Data Protection," (2021) at 3 https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_III_508_Compliant.pdf

***3GPP.*** Likewise, the 3rd Generational Partnership Project ("3GPP"), which unites several telecommunications standard development organizations, advances 5G work that utilizes security models that take a new and different approach to individual, endpoint, and core security, using the core concepts underlying Zero Trust.[17]

***NCCoE.*** As discussed further below, numerous industry experts from the cloud and security vendor community are partnering with the NIST National Cybersecurity Center of Excellence ("NCCoE") on an "Implementing a Zero Trust Architecture" project to develop how-to guides and functional demonstrations that provide example ZTA solutions using common enterprise IT infrastructure.[18] Draft NIST Special Publication ("SP") 1800-35C, *Implementing a Zero Trust Architecture: How-To Guides*, shows how to integrate a set of existing products into a ZTA and includes identity, credential, and access management capabilities.[19]

NCCoE plans to add capabilities as the project continues.[20] Draft NIST SP 1800-35D, *Implementing a Zero Trust Architecture: Functional Demonstrations*, summarizes the use cases applying the solutions in SP 1800-35C.[21] Use cases tested include stolen credentials in an enterprise endpoint or "bring your own device" scenario, and reauthentication failures during active sessions.[22] The draft demonstrations show how a ZTA can work and what it can do, and they provide optional guidelines for security professionals to adopt or tailor to their organizations' enterprises.[23]

[17] *See generally* Prasad et. al., "3GPP 5G Security" (Aug. 2018) https://www.3gpp.org/news-events/3gpp-news/sec-5g.

[18] NIST, "Implementing a Zero Trust Architecture," Fact Sheet (June 2022) https://www.nccoe.nist.gov/sites/default/files/2022-06/NCCoE-Zero-Trust-Fact-Sheet-June10-2022.pdf

[19] *See* NIST, 1800-35C, *Implementing a Zero Trust Architecture, Volume C: How-To Guides*, Preliminary Draft, (Aug. 2022) ("NIST 1800-35C").

[20] *Id.* at 3.

[21] *See* NIST, SP 1800-35D, *Implementing a Zero Trust Architecture, Volume D: Functional Demonstration*, Preliminary Draft (Aug. 2022), https://www.nccoe.nist.gov/sites/default/files/2022-08/zta-nist-sp-1800-35d-preliminary-draft.pdf.

[22] *Id.* at xi.

[23] *Id.* at 2.

# 5G Networks Use and Support Zero Trust, Building on Existing Standards

## Network Security Standards Continue to Evolve with the Changing Landscape

Today's 5G technology is an impressive case study in Zero Trust use. The development of 5G is closely connected with Zero Trust principles, building upon manifestations of Zero Trust found in earlier networks, such as in the mutual authentication protocols between devices and networks that have been in place since the introduction of 4G. Many aspects of 5G security—both the network design itself, and the functions it enables—are consistent with Zero Trust principles and help advance security that prioritizes Zero Trust. This is evident in numerous industry-led standards and guidance development efforts.

For example, 3GPP continues to develop specifications that support security and privacy, and that reflect the changing wireless network landscape. Specifically, in the decentralized and virtualized networks that will make up 5G, security measures beyond simple perimeter-oriented "castle-and-moat" approaches should be considered in order to support ongoing security enhancements.

3GPP has produced technical specifications[24] for authentication and other 5G network features covering:

- Network access security
- Network domain security
- User domain security
- Application domain security
- SBA domain security

Each of these specifications can be implemented throughout 5G networks to support Zero Trust Architectures.

***The 3rd Generation Partnership Project (3GPP) unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organizational Partners" providing their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies.***

***3GPP specifications cover cellular telecommunications technologies, including radio access, core network, and service capabilities.***

[24] *See* 3GPP, TS 33.501 V16.11.0, *Security architecture and procedures for 5G System*, (June 2022) (Release 16), https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.11.00_60/ts_133501v161100p.pdf.

## 5G Network Standards Are Already Aligned with Zero Trust Tenets

The latest 3GPP standards reflect and support Zero Trust principles as new standards like 4G and 5G move away from traditional approaches to security, such as perimeter-based frameworks where entities are deemed trustworthy after they have entered the network. As Ericsson explains, this is important because "[t]he heterogeneous nature of modern telecommunications infrastructure is making it increasingly difficult to protect network resources with conventional perimeter-oriented approaches to network security."[25]

***Example implementation: Unique identification***

*One Zero Trust element embraced by the wireless industry is unique identification. Each SIM card in a cellphone is allocated a unique identifier—in 5G, it is known as the Subscription Permanent Identifier ("SUPI"). Each SUPI is encrypted and concealed as the Subscription Concealed Identifier (SUCI), thereby serving as the key to authenticating a device as it travels from base station to base station through the network.*

Innovations in telecommunications network design solve this challenge by using a Zero Trust model where assumptions of trustworthiness are abandoned.

As Ericsson notes, "One of the technology aspects that is of growing significance in the telecom security sphere today is the zero trust security model. The 5G specifications are now aligned with the zero trust tenets. This means that the telecommunications industry is in a strong position to create a 5G zero trust architecture."[26]

Ericsson further explains, "The 3GPP 5G standards define relevant network security features supporting a zero trust approach in the three domains: network access security, network domain security and service-based architecture (SBA) domain security."[27] There are "four key security features in 5G that are of most significance in terms of enabling zero trust architectures: secure digital identities, secure transport, policy frameworks and security monitoring."[28]

Each network operator and deployment may have its own specific ZTA as it deploys solutions that meet the 3GPP standards. As AT&T has explained, "[ZTA] means different things to different people because many organizations already have certain aspects of [ZT] in place."[29]

Regardless of the various implementation methods, Zero Trust is being baked in as a foundation of modern wireless networks.

[25] *See* Jonathan Olsson at. al., Ericsson, *Zero trust and 5G – Realizing zero trust in networks*, (May 2021) ("Ericsson Zero Trust"), https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g.

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] Bindu Sundaresan, AT&T, "Securing the edge with Zero Trust" (Oct. 2021), https://cybersecurity.att.com/blogs/security-essentials/securing-the-edge-with-zero-trust.

# Government Implementation of Zero Trust: Current Landscape and Challenges

## The Federal Government Wants to Move Rapidly Toward Zero Trust.

The federal government is now working to implement Zero Trust principles as it moves to rapidly improve cybersecurity across its departments and agencies. The May 12, 2021, Executive Order 14028, *Improving the Nation's Cybersecurity* ("EO 14028"),[30] requires federal agencies to modernize their cybersecurity, including by developing a plan to implement ZTA.[31] The White House Office of Management and Budget ("OMB") subsequently provided implementation guidance for federal agencies in a January 2022 memorandum.[32]

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") has also published Zero Trust guidance, including a draft Zero Trust Maturity Model intended to assist federal agencies' ZTA implementation as required by EO 14028,[33] and a separate guidance document that informs federal agencies about how Zero Trust principles can be applied to currently available mobile security technologies that are likely already part of a federal enterprise's mobility program.[34]

The Department of Defense ("DoD") has also published its first version of a Zero Trust reference architecture for the DoD information network,[35] while the National Security Agency has offered a short guidance document describing the benefits and challenges of moving toward Zero Trust.[36]

## Existing Federal Guidance to Advance Zero Trust Implementation.

Much of the federal guidance focuses on federal agency Zero Trust implementation. However, several federal initiatives could help both the private sector and government in their evolving Zero Trust implementations. NIST, including NCCoE, has multiple Zero Trust workstreams under way:

[30] Executive Order 14028, Improving the Nation's Cybersecurity, 86 FR 26633 (May 2021) ("EO 14028").

[31] EO 14028, 86 FR 26633, 26636.

[32] OMB, Memorandum M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (Jan. 2022),. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[33] CISA, Zero Trust Maturity Model Version 1.0 (Draft) (June 2021), https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

[34] CISA, Applying Zero Trust Principles to Enterprise Mobility (Draft) (Mar. 2022), https://www.cisa.gov/sites/default/files/publications/Zero_Trust_Principles_Enterprise_Mobility_For_Public_Comment_508C.pdf

[35] DOD, Zero Trust Reference Architecture Version 1.0 (Feb. 2021), https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf.

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

*NIST's National Cybersecurity Center of Excellence (NCCoE) bring together experts from industry, government, and academia to address real-world needs for securing complex IT systems and protecting the nation's critical infrastructure.*

***Cybersecurity Practice Guide.*** As part of its "Implementing a Zero Trust Architecture" project, NCCoE is developing a cybersecurity practice guide that will demonstrate how to use commercially available technology to build interoperable, open standards-based ZTA implementations that align to the concepts and principles in NIST SP 800-207, Zero Trust Architecture.

***Zero Trust Implementation Approaches.*** In addition to Draft NIST SP 1800-35C and Draft NIST SP 1800-35D described above, NCCoE has released preliminary drafts of NIST SP 1800-35A, *Implementing a Zero Trust Architecture: Executive Summary*, and NIST SP 1800-35B, *Implementing a Zero Trust Architecture: Volume B: Approach, Architecture, and Security Characteristics*.[37] Draft SP 1800-35B provides examples of building, demonstrating, and documenting several example ZTAs using products and technologies from a variety of different vendors.[38]

***Applying Risk Management Frameworks in ZTAs.*** Cybersecurity White Paper 20, *Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators*, provides a federal government-focused overview of the NIST Risk Management Framework ("RMF") and how the RMF can be applied when developing and implementing a ZTA.[39]

These projects show that Zero Trust is maturing, but that applications and guidance are relatively new and will continue to evolve as technology and threats change.

## Current Zero Trust Discussions Need Clarity and Consistency Around Concepts, Terms, And Use Cases

### *ZT, ZTA, and ZTNA are not the same.*

Now that Zero Trust has become a key focus of government, federal contractors and other solutions providers are touting their approaches and characterizing many tools and techniques as "zero trust." However, government documents variably refer to ZT, ZTA, and ZTNA, risking confusion about government goals and in specific obligations for contracting officers.

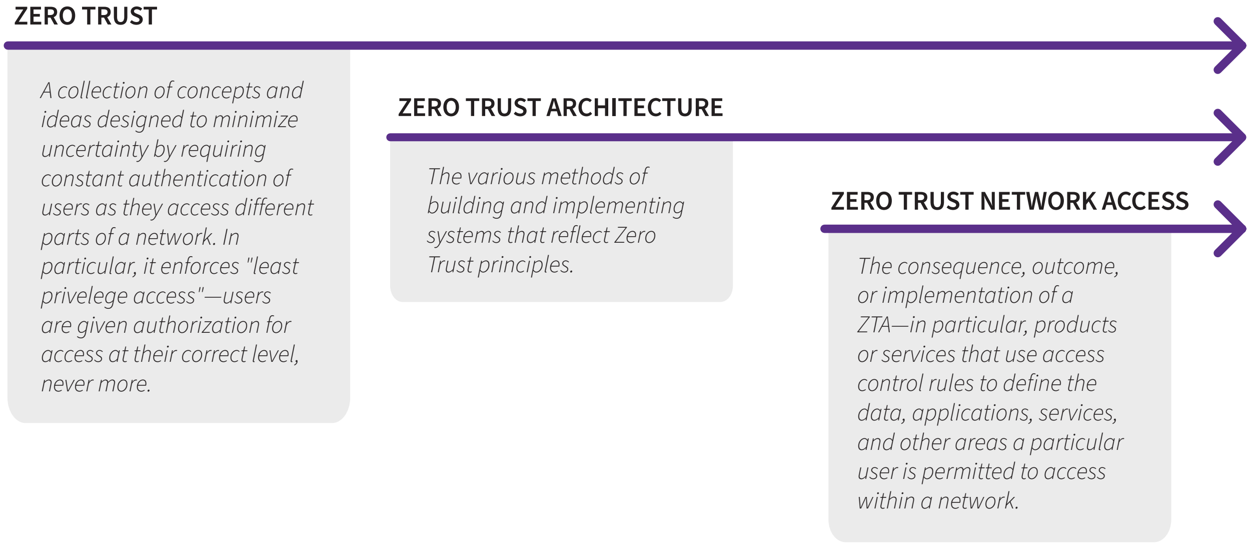
> *"Part of the reason why there is a lot of confusion about what zero trust is, is because it takes what the cybersecurity world has known about for many years and applies it in a different way." Zero Trust "is a paradigm shift in terms of how to think about security, but holistically it takes a lot of things that we already know how to do—such as multi-factor authentication, encryption, and software-defined networking¬—and combines them in different ways."*
>
> **— *Jeffrey Gottschalk, MIT***

[37] NIST, NIST SP 1800-35A: Implementing a Zero Trust Architecture (June 2022), https://www.nccoe.nist.gov/sites/default/files/2022-06/zta-nist-sp-1800-35a-preliminary-draft.pdf ("Draft SP 1800-35A"); Draft SP 1800-35B, Implementing a Zero Trust Architecture, Volume B: Approach, Architecture, and Security Characteristics (July 2022), https://www.nccoe.nist.gov/sites/default/files/2022-07/zta-nist-sp-1800-35b-preliminary-draft.pdf ("Draft SP 1800-35B").

[38] *Id.*

[39] NIST, Cybersecurity White Paper 20, Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators (May 2022), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.20.pdf.

These terms refer to related but different concepts, and it is important that government guidance is informed by clear definitions.



**ZERO TRUST**

*A collection of concepts and ideas designed to minimize uncertainty by requiring constant authentication of users as they access different parts of a network. In particular, it enforces "least privelege access"—users are given authorization for access at their correct level, never more.*

**ZERO TRUST ARCHITECTURE**

*The various methods of building and implementing systems that reflect Zero Trust principles.*

**ZERO TRUST NETWORK ACCESS**

*The consequence, outcome, or implementation of a ZTA—in particular, products or services that use access control rules to define the data, applications, services, and other areas a particular user is permitted to access within a network.*

***Zero Trust, or ZT,*** refers to a network security approach based on core concepts that organizations look to in adopting a more secure approach to network protection. Zero Trust reflects three core principles that (1) all entities are untrusted by default; (2) least privilege access, as defined earlier, is enforced; and (3) comprehensive security monitoring is implemented. To align with these principles, networks must continuously authenticate all users, applications, and any associated devices as they access different parts of a network and corresponding network functions.

As described by NIST, 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."[40]

***Zero Trust Architecture, or ZTA,*** refers to the implementation of systems that are informed by Zero Trust's core principles. A notable description of ZTA can be found in EO 14028, which describes ZTA as "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."[41]

[40] NIST 800-207 at 4.

[41] EO 14028, 86 FR 26633, 26646 (May 2021).

NIST also defines ZTA as "an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies."[42] The NSTAC ZT Report[43] identifies tenets and pillars of ZTA, including:

— Never trust, always verify;

— Assume breach; and

— Verify explicitly.

There is no single model or reference architecture for a ZTA. Rather, organizations will create their own customized ZTAs based on the tenets of Zero Trust, a risk assessment, and their particular security goals and needs.

***Zero Trust Network Access, or ZTNA,*** is a term of art long used in the telecommunications sector. In general, it refers to products or services that use access control rules for applications on a network. When ZTNA is implemented, users, their associated devices, or applications can only access a subset of other points on the network that they need to execute their tasks, and that access is granted based on a combination of factors.

***The President's National Security Telecommunications Advisory Committee (NSTAC) consists of senior industry executives who advise the president on a wide range of issues related to telecommunications, information systems, information assurance, infrastructure protection, national security, and emergency preparedness.***

ZTNA also prevents connected devices from seeing all of the other applications or devices on a network. Together, these features can limit lateral movement by an unauthorized entity.[44] Federal guidance has not yet fully defined or adopted the term "ZTNA"—NIST notes merely that "ZTNA is the consequence of a zero trust architecture."[45]

## Government Policy to Promote a Transition to ZT Requires Flexibility.

The federal government is urging agencies and the private sector to move to Zero Trust, creating expectations for agencies and previewing possible procurement requirements. By doing so with an incomplete understanding of how Zero Trust principles are defined and applied to network security, policymakers risk injecting uncertainty and stringent requirements into a cybersecurity landscape whose strength lies in its flexibility.

As organizations and stakeholders move toward Zero Trust, it is important that federal policy does not depart from the longstanding risk-informed, flexible approaches outlined in NIST's Cybersecurity Framework and Risk Management Framework described earlier. Zero Trust principles should be flexibly applied, based on an organization's risk profile and context. Indeed, the CSF can be used by an

[42] NIST 800-207 at 4.

[43] *See* NSTAC ZT Report at 3-4.

[44] *See*, *e.g.*, Gartner, "Zero Trust Network Access (ZTNA)" (accessed Nov. 2022), https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-; *see also* Cloudflare, "What is Zero Trust Network Access (ZTNA)?"(accessed Nov. 2022), https://www.cloudflare.com/learning/access-management/what-is-ztna/.

[45] NIST, Special Publication 800-215 (initial public draft), Guide to a Secure Network Enterprise Landscape at 21 (Aug. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.ipd.pdf.

organization to implement Zero Trust principles. Essentially, Zero Trust is the philosophy, and the CSF can provide the overarching framework and roadmap for how to achieve it.

An organization's transition toward Zero Trust principles or building of a ZTA will not occur with a simple flip of a switch—network transitions are lengthy and complex, and a ZTA presents its own risks and costs that organizations need to assess and customize based on numerous factors. Because each network has different capabilities depending on its structure, equipment, and systems, ZTAs inherently differ to meet each network's particular needs. Designing a ZTA presents tradeoffs in implementation, and the benefits and risks will vary across diverse sectors, organizations, and use cases.[46]

NIST has repeatedly made clear that implementing a ZTA not "a wholesale replacement of infrastructure or processes."[47] NIST further advises that "[a]n organization should seek to incrementally implement zero trust principles, process changes, and technology solutions that protect its highest value data assets. Most enterprises will continue to operate in a hybrid zero-trust/perimeter-based mode for an indefinite period while continuing to invest in ongoing IT modernization initiatives.[48]

Given the gradual and variable nature of Zero Trust migrations, the federal government must ensure that its guidance is risk-based and incorporates the flexibility necessary to allow diverse organizations to reach their desired Zero Trust goals and to dynamically approach cybersecurity to meet ever-changing threats and challenges.

[46] *See* NIST 800-207 at 28-31 (detailing threats associated with ZTA); *see also* Deirdre Doherty & Brian McKenney, "Zero Trust Architectures: Are We There Yet?" at 12 (June 2021) (noting that "[w]hile ZTA holds promise for improving security, potential vulnerabilities also exist with this new approach, which must be studied and considered before migration and on an ongoing basis"), https://www.mitre.org/news-insights/publication/zero-trust-architectures-are-we-there-yet.

[47] NIST 800-207 at 36.

[48] *Id.*

# Recommendations for Sound Zero Trust Policy: A Collaborative, Flexible, and Risk-Based Approach

To achieve the most desirable outcomes, any federal guidance efforts should consider the following recommendations:

1. ***Government should leverage the wireless industry's experience and expertise in developing and implementing Zero Trust solutions.***

   — The wireless industry has valuable experience and expertise with Zero Trust principles in practice, and it has long embraced security approaches that are consistent with those principles.

   — Through industry groups such as ATIS, NSTAC, CSRIC, and ESF, the wireless industry is continuing to explore and evolve Zero Trust principles.

   — As the government continues its work to promote Zero Trust principles and facilitate ZTA implementations, it should coordinate closely with the wireless sector and leverage its unique experience and expertise on this issue.

2. ***Government should defer efforts to develop additional reference architectures to allow agencies and critical infrastructure sectors to develop and mature their own architectures.***

   — Government guidance should not move to additional reference architectures until more industry work has been completed. There is no one ZTA that will be applicable to entire sectors; they are necessarily going to be customized and iterative, making any prescriptive expectations or granular frameworks premature at best, and potentially counterproductive at worst.

   — It is vital that different industries and sectors have time to develop and implement ZTAs. For example, as noted previously, ATIS has a working group focused on applications of Zero Trust in the 5G wireless context.[49] This project will provide important insights for the wireless, telecommunications, and IT sectors on how to develop ZTAs using existing and forthcoming enterprise products. Until such critical work can be completed, further federal guidance informing or defining ZTAs run the risk of limiting the development and utility of industry-specific efforts.

[49] ATIS Enhanced Zero Trust and 5G.

3. ***Because no two ZTA adoptions will be the same, it is important that government guidance make clear that there is no single fixed approach.***

    — Different applications across organizations and sectors will drive innovation. Products and configurations developed to serve specific use cases may find customers in unexpected places, or be adapted further to meet the individual needs and use cases of other organizations.

    — A failure to make clear and promote the unique nature of each organization's ZTA adoptions will both limit the effectiveness of those adoptions and reduce the speed and success of innovative approaches.

4. ***Government should not pursue any private sector mandates related to the use of Zero Trust or Zero Trust Architecture.***

    — Because Zero Trust and Zero Trust Architectures are inherently variable and iterative, they do not logically support mandates or directives. This means there is neither a checklist approach nor other uniformly-applicable standards that could serve as a reliable and universal baseline.

    — Zero Trust and Zero Trust Architectures are still being developed. As considerable work continues at NIST, DHS, and in the private sector, any mandates or requirements would be premature, risking to stifle experimentation and impede innovation.

5. ***Any expectations for government contractors whose products or services may be part of the government's own transition to Zero Trust should be developed with care.***

    — Procurement requirements should not embrace a "one-size-fits-all" approach. They must recognize that ZTA adoption will look very different across missions and sectors, and that a one-size-fits-all ZTA approach is not appropriate for all ICT services.

    — OMB, the Federal Acquisition Regulatory (FAR) Council, and interested agencies should work with private sector stakeholders, who support many government missions with IT, telecom, and other services, to develop approaches that can support agencies' implementation of Zero Trust principles and their development of ZTAs.

# Conclusion

Zero Trust and its implementations are important and promising tools in enhancing cybersecurity and enterprise risk management for information and communications technologies. Zero Trust and Zero Trust Architectures encompass a significant change in how ICT systems are built and managed.

The wireless industry has already anticipated and implemented many of the tools and capabilities that are part of Zero Trust Architectures, and it has made significant progress in embracing the evolving landscape as it works with standards bodies and in partnership with government to drive continued innovation and enhanced security.

As conversations around Zero Trust continue among policymakers, and as government programs and guidance promote Zero Trust adoption, it is important that policymakers understand the key terms, allow for flexibility and variability across sectors, and encourage innovation.

By embracing the recommendations outlined in this paper, recognizing the existing and ongoing progress in Zero Trust adoption and evolution, and working with industry to leverage their experience and expertise in implementing Zero Trust solutions, government can develop reasonable pathways to implementing Zero Trust and strengthening network security.

ctia™