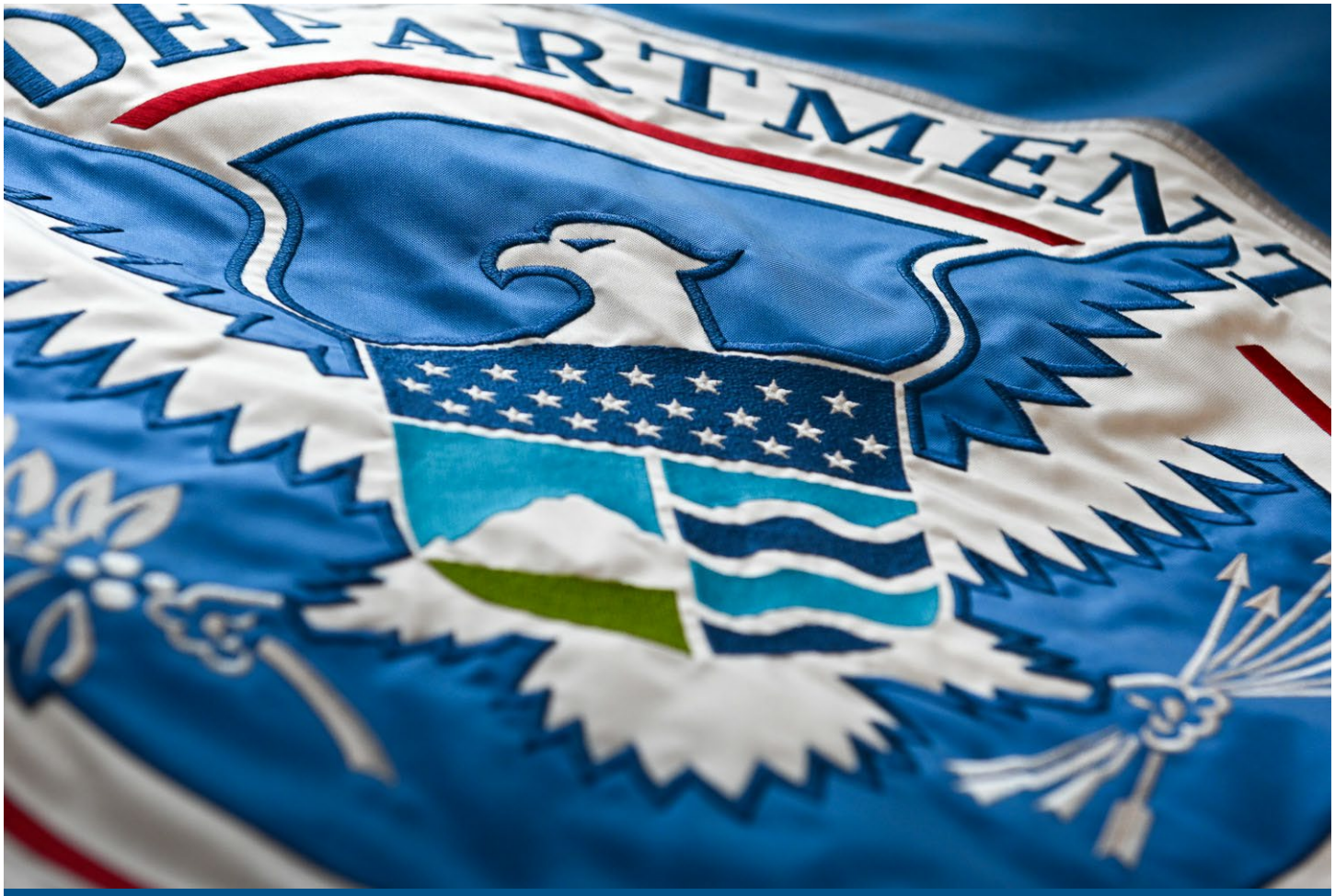


# Zero Trust Implementation Strategy

October 2023

Homeland Security

## Introduction

Like the rest of the Federal government, the Department of Homeland Security (DHS) has been implementing zero trust mandates for years. DHS leadership established a Zero Trust Action Group, and later a Zero Trust Integrated Product Team, incorporating technical leadership from across the Department—and together, these teams have made impressive progress. Notable achievements in the first several years of DHS' zero trust journey include establishing a cloud security gateway now used by most of the Department in lieu of virtual private networks, implementing multi-factor authentication and data encryption in-transit and at-rest across almost all DHS systems, and integrating identity and device management solutions that are essential for further zero trust implementation efforts.

While the work that lies behind us is commendable, the work that lies ahead of us is more challenging. As shown in the CISA Zero Trust Maturity Model, implementing zero trust becomes far more difficult as you progress toward higher levels of maturity. At this stage of the journey, we need a formal strategy to align and mutually reinforce further efforts.

This document presents a cohesive, formal strategy of the Department to advance, accelerate, and align zero trust implementation. This strategy establishes a shared vision that better protects resources, stabilizes cybersecurity budgets, and accelerates mission outcomes—all at the same time. This strategy will also allow the Department to pursue a shared zero trust vision while addressing shared challenges, including resource scarcity, legacy technology, and a nascent shared services environment.

This strategy was conceived and written by a coalition spanning DHS Headquarters and Components between July and October 2023, and formally adopted by the Chief Information Security Officer (CISO) Council in October 2023. By direction of the DHS Chief Information Officer, the DHS CISO will govern implementation and further refinement of this strategy through the CISO Council.

The authors wish to acknowledge the active participation of dozens of practitioners and subject matter experts from across the entire DHS enterprise, without whose efforts this strategy would not exist.

## Approval

This strategy has been APPROVED for the Department by the Chief Information Security Officer Council as of October 2023.

KENNETH W BIBLE
Digitally signed by KENNETH W BIBLE
Date: 2024.01.29 11:44:33 -05'00'

Kenneth W. Bible, P. E.
Chief Information Security Officer
Department of Homeland Security

## Table of Contents

## Purpose and Audience

This **Zero Trust Implementation Strategy** establishes a strategic framework for the coordinated actions necessary to implement zero trust across the Department of Homeland Security (DHS).

This document is intended as a top-level reference for anyone with responsibility for implementing zero trust—executive leaders, program and project managers, team leaders, and individual team members—regardless of their technical background or level of expertise in cybersecurity.

## The Case for Change

DHS must shift its approach to cybersecurity because the current traditional, network-centric approaches prevalent across the Department are **unaffordable**, **unsustainable**, and **ineffective**. Spending more on cybersecurity without changing our approach will not yield better results.

### Traditional, network-centric cybersecurity

Traditional cybersecurity methods focus on defending networks. A traditional approach defines the role of cybersecurity as preventing, detecting, reacting to, responding to, and recovering from breaches (penetrations of the network by malign actors). Traditional network-centric cybersecurity divides cyber terrain into zones with varying degrees of trust, typically including an Intranet (which is implicitly trusted), a demilitarized zone that provides outward-facing services such as email and web servers (which is partially trusted), virtual private networks (which extend the Intranet to include trusted external endpoints), and external networks (which are untrusted). In such models, defenses and defenders focus mainly on the boundaries of these zones.

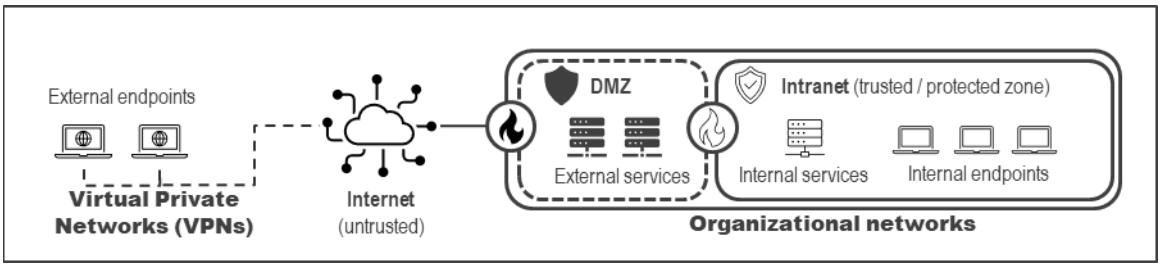


**Figure 1: A traditional, network-centric cybersecurity model**

### Problems with network-centric cybersecurity

Traditional, network-centric cybersecurity proceeds from false assumptions, including:

- That bad actors come from outside of the network, and cybersecurity keeps them out.
- That keeping the network perimeter secure keeps the data inside the network safe
- That access to the network should enable the discovery and use of most resources.

It is no longer possible for boundary-based defenses to stop all or even most breaches before they occur, or even to detect a breach quickly. Contemporary threat actors, from insider threats to cyber criminals to nation-state actors, have become more persistent, stealthier, and more subtle; they

penetrate network perimeter defenses with regularity. Because of this, it is no longer safe to assume that an entity with access to a network is trustworthy—in fact, we must assume the opposite.

## Zero Trust: A Different Approach

US Government agencies have been ordered to move toward zero trust architectures with urgency; see Executive Order 14028, Office of Management and Budget (OMB) Memoranda M-22-09 and M-21-31, and National Security Memorandum 8[1] as prominent and relevant examples. We can expect audits and budgets to hinge on questions of whether and how we've implemented zero trust for years to come.

More importantly: By carefully and deliberately implementing zero trust, we can better protect DHS resources, stabilize cybersecurity investments, and accelerate mission outcomes—all at the same time.

### What is Zero Trust?

National Institute of Standards and Technology (NIST) Special Publication 800-207 defines zero trust architecture[2]. What follows is a high-level summary for a non-technical audience.

At a high level, "zero trust"[3] is a shift in an organization's fundamental cybersecurity approach. Traditional approaches focus on protecting networks; zero trust focuses on **protecting resources**.

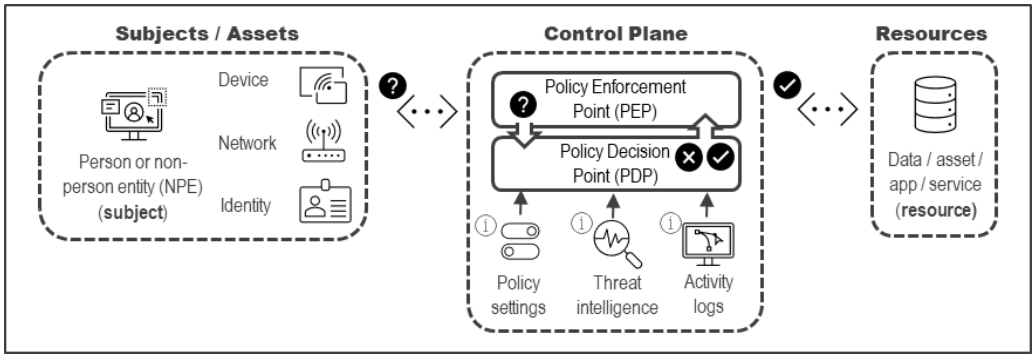


**Figure 2: A notional zero trust architecture (simplified)**

Zero trust architecture describes three essential elements: A **subject** (using assets to access resources), a **control plane** (mediating access to resources), and **resources** (data, assets, applications, and services). As the name implies, no element is implicitly trusted; a subject may be any person or non-person entity, using any device, on any network. The control plane decides whether to allow subjects to access resources based on ***context***.

- Policy might dictate that certain kinds of requests are explicitly allowed or denied.
- Threat intelligence may indicate that certain kinds of activity should not be allowed.
- Activity logs might also indicate patterns of malicious activity that should be interrupted.

Zero trust architecture proceeds from different assumptions than traditional cybersecurity, including:

- That bad actors may come from anywhere—within or outside of the network.
- That network perimeters have already been breached—or that a breach is inevitable.
- That subjects should be allowed to discover and use the resources they need—and no others.

## Zero Trust Vision

If DHS components carefully, deliberately, and cooperatively implement zero trust, we can expect to better protect DHS resources, stabilize cybersecurity investments, and accelerate mission outcomes.

### Better protect resources.

Modern, mature, and interoperable zero trust environments will afford component cyber defenders more opportunities to detect novel threats, and more response options that can quickly be deployed to address sophisticated threats. Adopting zero trust will sensitize cyber defenders to recognize ever more subtle threat indicators. Incident responses will still be necessary, but with the appropriate security model, ethos, and response tools, defenders can react effectively to increasingly sophisticated threats.

### Stabilize cybersecurity investments.

Rather than spending more every year to maintain outdated cybersecurity tools and compliance regimes at the expense of modernization, cybersecurity budgets will stabilize around efficient investments in modern, shared services that minimize total costs and maximize the effectiveness of cyber defenders. Rather than struggle to meet unfunded mandates to modernize cybersecurity tools and approaches, we will consistently invest in modern, secure environments and approaches that set the pace for all others.

### Accelerate mission outcomes.

New mission capabilities will be brought online within modern, secure, agile environments that allow for the evaluation and mitigation of cybersecurity risks in days or weeks, not months or years. Cybersecurity will go from being the longest task in development, to the shortest path to production. Legacy capabilities that cannot easily be replaced or rebuilt must be encapsulated in modern containers that can be better protected in modern, secure, agile environments at all levels of classification.

## Shared Challenges

This Zero Trust Implementation Strategy must seek to achieve the outcomes of our vision while also addressing shared challenges that would otherwise impede zero trust implementation, including:

- Increasingly hostile and complex threats (state and non-state cyber threat actors, insider threats, and an expanding malware economy present an unprecedented threat environment)
- Resource challenges (zero trust mandates often come without new or sufficient resources to enable adoption and wide-scale implementation)
- Legacy technology and architecture (whatever we do must be possible in the context of current environments and address current problems—such as technical debt and shadow IT)
- Nascent shared solutions environment (previous and current enterprise solutions are loosely defined and have not always been well-managed in an effective marketplace of ideas)
- Governance (maneuvering a large and complex bureaucracy to achieve an agile, modern end state requires the ability to make decisions and take actions quickly and decisively, unimpeded by policy)

## Strategic Approach

Achieving our shared vision, while addressing our shared challenges, will require coordinated and sustained execution across multiple, parallel lines of effort by DHS Headquarters and Components.

What follows is not a strategic plan—it is not intended to provide a comprehensive list of actions or to sequence all actions in time and space. Rather, it is a **strategic approach**—a list of shared focus areas requiring actions to be coordinated and aligned to achieve complementary effects. Lines of effort are loosely defined, allowing for detailed planning (e.g., Component- and program-specific plans) to occur later, without unnecessarily constraining methods or solutions or hampering innovative approaches.

### Foundational efforts

WE MUST BE BRILLIANT AT THE BASICS.

Much of the work of implementing Zero Trust, for any organization, is ***just work***. It does not involve procuring or installing new technology but may (and usually will) involve integrating and using existing technology in new ways, consistent with zero trust principles. More importantly, it usually involves prioritizing effort on the part of key people—mainly those who operate and defend existing systems, networks, and infrastructure—to set the conditions necessary to implement zero trust principles.

As examples, critical foundational efforts, necessary for all stakeholders, include (but are not limited to):

- **Identification of Component Critical Data, Assets, and Resources.** Components must begin with identification and classification of critical data and resources. This process should identify asset and resource importance, data sensitivity, ownership, any regulatory requirements, business criticality, and potential impact in case of a security breach.
- Adopting **Identity Driven Access**, which involves a change of mindset and operational practices as it will require DHS components to regularly review and update entity access permissions, as well as to adopt robust identity and access management processes to ensure that access rights are aligned with specific job requirements.
- Adopting the **Principle of Least Privilege (PoLP)**[4]–predicated on the notion that person and non-person entities, including Application Program Interface (API) accounts[5], will be granted the minimum level of access and permissions required to perform specific tasks, and nothing more. PoLP seeks to limit potential security risks by ensuring that permissions are narrowly tailored to the essential requirement of each entity's function within the system.
- **Threat Surface Reduction (TSR)** is essential for implementing zero trust, as it focuses on safeguarding critical assets by identifying, compartmentalizing, and isolating potential threat vectors within an organization. It requires a thoughtful assessment of an organization's network architecture, the relationships between different components, and the flow of data. As it does not inherently involve procuring new tools or technologies, TSR will require DHS to leverage its existing network infrastructure and security solutions in new ways. By reducing our attack surface, DHS drives down risk to agency and component environments and enables the security modernization necessary to mitigate advanced threats.

## Standardization & Interoperability

WE MUST EMBRACE DIVERSITY WITHOUT SACRIFICING INTEROPERABILITY.

An organization as large and diverse as DHS cannot be expected to produce, procure, and use identical solutions in identical ways. No matter how mature our enterprise service offerings may be, we must expect a variety of approaches to zero trust, rather than treating variation as an exception to the rule. Varied solutions should be a source of strength—allowing DHS to draw from the best design patterns and implementations from within DHS agencies and offices, from our various external partners such as the Department of Defense (DoD) and the Intelligence Community (IC), and from the industrial base.

Embracing varied solutions means, by extension, that our strategic approach to implementing zero trust must also begin to steer the Department toward a comprehensive framework of **Standardization & Interoperability**. Pinpointing and reinforcing the most pertinent standards and open implementations will position DHS to establish a cohesive security fabric, while still allowing for innovation and tailoring.

Activities necessary to promote standardization and interoperability include, but are not limited to:

- **Identity and access control standardization**. Establishing standardized uniform protocols for authentication methods, authorization, and access control mechanisms allows the organization to enhance security, bolsters compliance efforts, and streamlines identity management practices across the organization. Relevant, mature standards along these lines include Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML).
- **Data and metadata standardization** entails establishing uniform data classification, encryption, and tagging protocols to ensure that data is consistently identified, protected, and monitored throughout its lifecycle. Standardizing metadata, such as information about data ownership, usage, and lineage, facilitates transparency and accountability in data handling processes throughout the organization. Trusted Data Format (TDF) is a relevant open standard here.
- **Standardizing operational metadata** across dissimilar implementations can promote more effective and comprehensive visibility and control over zero trust solutions. Emerging open standards such as the Open Cybersecurity Schema Framework (OCSF) enable vendor-neutral sharing of relevant security information and security automations across dissimilar platforms.
- **Establishing and sharing reference designs** enables components to accelerate implementations, avoid pitfalls, and more efficiently maintain design elements that underpin zero trust solutions. Efforts along these lines may be as simple as posting documents and architecture artifacts in a shared repository for others to use, or as complex and interwoven as sharing a code base for solutions across multiple DHS components working in similar environments.
- **Designing and testing for interoperability** between the multiple facets of the Zero Trust security elements to work seamlessly together. Whether data classification and security mechanisms to enforce access control, endpoint security solutions and network access control systems, security analytics platforms and threat detection mechanisms to provide a unified view of threats, API security solutions and identity and access management systems, a focus on interoperability furthers the strategy of the Zero Trust model.

## Enterprise Services

WE MUST IDENTIFY AND SHARE THE BEST SOLUTIONS FOR SHARED PROBLEMS.

An executable strategy to implement zero trust must recognize and begin to solve resource challenges. Components consistently indicate that zero trust mandates arrived without additional resources to retool and reimplement cybersecurity and network operating models in parallel with current operations. Neither DHS Headquarters nor any individual Component has sufficient independent resources to drive zero trust implementations on their own, at the pace directed by higher authorities, and as things stand are left to develop and support zero trust solutions and operating models independently.

Widely adopted enterprise IT services can function as a significant force multiplier by promoting 'create once, use often' practices, leveraging economies of scale, driving continuous improvement through learning and automation, and enabling agility for DHS components. Shared solutions present some risks, but also offer the promise of much greater efficiency by avoiding the nonrecurring costs associated with creating, testing, and initially approving platforms and services aligned with zero trust principles.

For a strategy that hinges on shared solutions to be successful, enterprise IT services cannot be a lowest-common-denominator solution, but need to be lean (efficient), learning (responsive), and enabling (teams do not need to be coerced into adoption). Additionally, requirements and budgets for cybersecurity and network operations are distributed among DHS components, and accordingly, we should expect that innovative solutions to zero trust mandates may come from any quarter within DHS.

While can expect and may seek a wide variety of shared solutions that implement zero trust principles, the following types of shared solutions should be prioritized:

- **Shared platforms aligned with zero trust principles.** By collaboratively working with each component and gaining insight and feedback on their current zero trust solutions, DHS can begin to architect shared platforms and enable centralized procurement and cross-component deployment and use. This will enable closer collaboration among the components, establish standard design patterns and practices, and drive cost savings for the Department as a whole.
- Shared solutions enabling **Visibility and Analytics** and **Automation and Orchestration** to support the interoperability, integration, and automation of existing capabilities across the **Identity**, **Devices**, **Networks**, **Applications and Workloads**, and **Data** pillars. The actions directed under OMB M-22-09 broadly exclude cross-cutting functions and focus on the five pillars recognized in the CISA Zero Trust Maturity Model; as a result, components have done less to enable cross-cutting functions than they have done to date to position themselves to enable zero trust for identities, devices, networks, applications, and data.
- **Shared, federated identity services** that are suitable for use within DHS environments and across component-specific enclaves—to include on-premises, cloud-based, and disconnected environments—supporting DHS entities, external mission partners, and members of the public.
- **Enterprise licensing and procurement vehicles for commonly used solutions** where there are already common technology solutions in place across multiple components.

## Accelerators

WE MUST GO FASTER AND THINK DIFFERENTLY.

Speed is imperative to implementing zero trust for two equally important reasons.

First: We must implement zero trust principles and approaches as quickly as possible to create and maintain competitive advantages against persistent and increasingly potent cyber adversaries.

Second: Resources are limited. Making best use of scarce resources necessary to implement zero trust—people, money, and time—means failing fast, learning quickly, and avoiding costly mistakes.

Accelerators are innovative approaches to implementing zero trust, leveraging a minimum of resources (people, money, and time) to quickly determine whether an approach is successful, may show promise, or should be abandoned. Ideally, accelerators should leverage others' resources in place of our own—whether that is the resources of other government agencies who have already demonstrated success, or the resources of industry partners seeking to prove the viability of a particular technology or approach. Where we must invest our own scarce resources, we must make targeted, quick, and ruthless decisions.

While we cannot presume to know or hope to list every opportunity for acceleration here, the following are already-known areas in which acceleration may be possible:

- **Existing, cloud-based, zero trust aligned platforms** have been built and rigorously tested by other agencies, including but not limited to DoD and IC components, and have been shown to broadly meet the same requirements we would expect to apply to DHS components. Given that most cybersecurity controls can be implemented at the platform level and inherited by systems, the use of existing platforms offers the greatest potential benefits at the lowest probable costs. Administrative barriers that may otherwise prevent direct reuse, such as contracts and accreditation concerns, can be overcome; and if direct reuse of solutions proves impossible or undesirable, then at a minimum, we would expect to accelerate by leveraging existing designs.
- Given at least one cloud-based, zero trust aligned platform, further acceleration becomes possible by leveraging the platform in multiple ways. For example:
    - **Adversarial emulation** (particularly where it can be supported by automated toolsets) can quickly demonstrate and validate the cybersecurity posture of new systems or capabilities hosted in the platform. Presuming that adversarial emulation techniques demonstrate acceptable risks, authorizing officials can make higher-confidence risk-based decisions, potentially bringing new systems and capabilities online more quickly.
    - **Encapsulation of legacy systems** that cannot be easily refactored or rebuilt is a technique that can allow those systems to still benefit from enhanced cybersecurity tools and techniques through a platform aligned with zero trust principles.
- **Novel, software-based approaches to providing highly secure environments** exist as both government-off-the-shelf solutions and commercialized technologies once used to solve for challenging, government-specific cybersecurity scenarios. The DHS Zero Trust Team has already met with several vendors whose products match this description and are worthy of evaluation.

## Governance

WE MUST BE ABLE TO MAKE FIRM DECISIONS AND TAKE DECISIVE ACTIONS.

"Governance" is the enduring capacity of an institution to make decisions and take actions. Using that definition, it is easy to determine whether governance exists in any given organization or function. Implementing zero trust requires decisions to be made, and actions to be taken, at an institutional scale. If we lack effective governance of the organizations and functions necessary to implement zero trust, then we cannot implement zero trust as an institution.

Everything discussed in this implementation strategy requires effective governance. As examples, consider the following:

- Identifying and listing critical data, assets, applications, and services (see Foundational efforts).
- Setting and enforcing standards for data access (see Standardization & Interoperability).
- Designating federated identity services for use across components (see Enterprise Services).
- Deciding whether to invest in, further evaluate, or abandon a novel product (see Accelerators).

For governance to be effective, decisions must be firm. Components have consistently reported that past institutional decisions, when first made or when later changed, created unforeseen challenges. Decisions contemplated in this strategy can have vast implications, positive and negative, for all parties. These decisions must therefore be reached in inclusive ways, made unequivocally, and changed rarely.

By direction of the DHS Chief Information Officer, the Chief Information Security Officer (CISO) Council is the governing body for this strategy. The strategy is adopted when the CISO Council accepts it, and any changes to this strategy are subject to the approval of the CISO Council.

The authors note that effective governance over various matters is needed to support implementation, most notably including but not limited to decisions regarding:

- Designation and deprecation of enterprise services necessary to implement zero trust.
- Identification of, investment in, evaluation of, and abandonment of zero trust accelerators.
- Identification and enforcement of technical standards relevant to zero trust implementation.
- Approval of reference designs and standard configurations for zero trust implementations.
- Allocation of scarce resources among competing investments in zero trust implementations.

Where there are no other authorities in place to make decisions needed to implement zero trust, those authorities are reserved for the CISO Council, consistent with this strategic approach. Decisions regarding zero trust implementation that impact systems under other Authorizing Officials will be made either in coordination with, or by, the CISO Council going forward.

## Measuring Success

Metrics drive behavior and predict outcomes. To drive desired behavior and predict zero trust outcomes, authorities should monitor two key metrics relative to any current or proposed zero trust solution: Customer Experience and Operational Resilience.

In principle, these metrics should never be in conflict. Successful zero trust solutions and implementations should increase both customer experience and operational resilience in tandem. Solutions that sacrifice one metric for the other should be questioned. Solutions that harm both metrics should be subjected to harsh scrutiny, and very likely abandoned.

### Customer Experience

Components must be able to measure and report customer experience (CX) for zero trust solutions. Relevant authorities should ask:

1) What are your measures for CX and who approved them?
2) What is your CX performance and how do you know?

The answers to these questions matter because they predict whether end users will use solutions as provided or seek alternatives. Components have consistently reported "shadow IT" (unmanaged and unsanctioned technology solutions, often procured outside of official channels) as a significant barrier to zero trust implementation. The primary cause of shadow IT is dissatisfaction with available solutions.

### Operational Resilience

Components must be able to measure and report the operational resilience (OR) of zero trust solutions. Relevant authorities should ask:

1) What are your measures for OR and who approved them?
2) What is your OR performance and how do you know?

The answers to these questions matter because they predict whether solutions, as provided, are reliable (particularly under suboptimal operating conditions). Solutions that are not consistently operationally resilient cannot be sustained as enterprise services over the long term, cannot be expected to accelerate DHS zero trust implementations, and are more likely to negatively affect other solutions with which they must integrate and interoperate.

## Closing Notes

This strategy provides a coordinated framework for planning, execution, and measurement of zero trust implementation across DHS. It is intended to guide the decisions and actions of DHS headquarters and components to achieve reinforcing effects, accelerate implementations, and help assure success.

Updates to this strategy, along with further guidance and direction aligned with this strategy, will be issued as needed through the CISO Council and other governing bodies.

## References

See the following links for further information and resources pertaining to this strategy.

### Links from text

**Executive Order 14028**
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity

**Office of Management and Budget (OMB) Memorandum M-22-09**
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

**OMB Memorandum M-21-31**
https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

**National Security Memorandum 8**
https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems

**National Institute of Standards and Technology (NIST) Special Publication 800-207**
https://csrc.nist.gov/pubs/sp/800/207/final

**Security Assertion Markup Language (SAML)**
https://www.oasis-open.org/standard/saml/

**eXtensible Access Control Markup Language (XACML)**
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

**Trusted Data Format (TDF)**
https://www.dni.gov/index.php/who-we-are/organizations/ic-cio/ic-cio-related-menus/ic-cio-related-links/ic-technical-specifications/trusted-data-format

**Open Cybersecurity Schema Framework (OCSF)**
https://github.com/ocsf/

**Department of Defense (DoD) Zero Trust Reference Architecture**
https://dodcio.defense.gov/Portals/0/Documents/Library/%28U%29ZT_RA_v2.0%28U%29_Sep22.pdf

### Additional resources

**Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model**
https://www.cisa.gov/zero-trust-maturity-model

**Department of Defense (DoD) Zero Trust Strategy**
https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

## End notes

[1] The scope of zero trust mandates is holistic—it includes all systems, all networks, and all capabilities, hosted by all DHS components and activities, at all classification levels. No part of DHS is exempt or excepted from zero trust.

[2] The Department of Defense (DoD) has also published a Zero Trust Reference Architecture that is relevant to DHS components that directly interoperate with DoD. The Intelligence Community (IC) also adopted DoD's architecture.

[3] Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgment that threats exist regardless of traditional network boundaries. A Zero Trust security model eliminates implicit trust in any one asset, person entity (PE) or non-person entity (NPE), node, or service and instead requires continuous verification of the operational transaction via real-time information fed from multiple sources to determine access and other system responses.

[4] Embracing the Least Privilege Access principle, components can significantly enhance their security posture within the Zero Trust framework, ensuring that entities only have access to the resources and data necessary for their functions while reducing the potential for unauthorized access and data breaches. When Least Privilege Access becomes habitual, risk-aware access decisions and automated detection and response actions become easier to implement which reduces network defender fatigue by allowing those resources to focus on sophisticated adversaries and their tactics for gaining access to sensitive data.

[5] Specifically focusing on API accounts, excessive access rights can pose significant security threats as they may provide attackers with broader attack surfaces and potential for unauthorized data exposure and larger system compromise. DHS must effectively apply PoLP to API accounts and employ comprehensive identify and access management (IAM) practices. This involves regularly reviewing and adjusting permissions based on job and task roles and requirements, regularly auditing access permissions, and employing automated tools for access control and continuous monitoring.