NIST SPECIAL PUBLICATION 1800-35E

Implementing a Zero Trust Architecture

Volume E:
Risk and Compliance Management

Alper Kerman
Murugiah Souppaya
National Institute of Standards and Technology
Gaithersburg, Maryland

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

Susan Symington
The MITRE Corporation
McLean, Virginia

William Barker
Dakota Consulting
Largo, Maryland

December 2022

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder's responsibility to fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise, and the impact should the threat be realized before adopting cybersecurity measures such as this recommendation.

National Institute of Standards and Technology Special Publication 1800-35E, Natl. Inst. Stand. Technol. Spec. Publ. 1800-3E, 65 pages, December 2022, CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: nccoe-zta-project@list.nist.gov.

Public comment period: December 21, 2022 through February 6, 2023

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

A zero trust architecture (ZTA) focuses on protecting data and resources. It enables secure authorized access to enterprise resources that are distributed across on-premises and multiple cloud environments, while enabling a hybrid workforce and partners to access resources from anywhere, at any time, from any device in support of the organization's mission. Each access request is evaluated by verifying the context available at access time, including criteria such as the requester's identity and role, the requesting device's health and credentials, the sensitivity of the resource, user location, and user behavior consistency. If the enterprise's defined access policy is met, a secure session is created to protect all information transferred to and from the resource. A real-time and continuous policy-driven,

risk-based assessment is performed to establish and maintain the access. In this project, the NCCoE and its collaborators use commercially available technology to build interoperable, open, standards-based ZTA implementations that align to the concepts and principles in NIST Special Publication (SP) 800-207, *Zero Trust Architecture*. This NIST Cybersecurity Practice Guide explains how commercially available technology can be integrated and used to build various ZTAs.

KEYWORDS

cybersecurity framework subcategories; identity credential and access management (ICAM); risk; security controls; zero trust; zero trust architecture (ZTA).

ACKNOWLEDGMENTS

We are grateful to the following individuals for reviewing the document.

Name	Organization
Timothy Jones	Forescout
Tim LeMaster	Lookout
Parisa Grayeli	MITRE
Kevin Stine	NIST
Wade Ellery	Radiant Logic
Deborah McGinn	Radiant Logic

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Collaborators

Appgate
AWS
Broadcom Software
Cisco
DigiCert
F5
IBM
Ivanti
Lookout
Mandiant
Microsoft
Okta
Ping Identity
Radiant Logic
SailPoint
Tenable
Trellix
VMware

Technology Collaborators		
Forescout	Palo Alto Networks	Zimperium
Google Cloud	PC Matic	Zscaler

Collaborators listed above who have already contributed technologies may also provide additional components for integration in future builds.

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: nccoe-zta-project@list.nist.gov

Contents

List of Tables

1 Introduction

In this project, the NCCoE and its collaborators use commercially available technology to build interoperable, open, standards-based zero trust architecture (ZTA) implementations that align to the concepts and principles in NIST Special Publication (SP) 800-207, *Zero Trust Architecture* [1]. This NIST Cybersecurity Practice Guide provides a risk assessment and maps ZTA security characteristics to cybersecurity standards and best practices. The mappings include both general ZTA logical component capabilities and specific ZTA example implementation capabilities.

1.1 How to Use this Guide

This NIST Cybersecurity Practice Guide will help users develop a plan for migrating to ZTA. It demonstrates a standards-based reference design for implementing a ZTA and describes various example implementations of this reference design. Each of these implementations, which are known as *builds,* are standards-based and align to the concepts and principles in NIST SP 800-207, *Zero Trust Architecture*. The reference design described in this practice guide is modular and can be deployed in whole or in part, enabling organizations to incorporate ZTA into their legacy environments gradually, in a process of continuous improvement that brings them closer and closer to achieving the ZTA goals that they have prioritized based on risk, cost, and resources.

NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on implementing the example solutions and developing other parts of the content. As a preliminary draft, we will publish at least one additional draft for public comment before it is finalized.

When complete, this guide will contain five volumes:

- NIST SP 1800-35A: *Executive Summary* – why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving this challenge
- NIST SP 1800-35B*: Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-35C: *How-To Guides* – instructions for building the example implementations, including all the security-relevant details that would allow you to replicate all or parts of this project
- NIST SP 1800-35D: *Functional Demonstrations* – use cases that have been defined to showcase ZTA security capabilities and the results of demonstrating them with each of the example implementations
- NIST SP 1800-35E*: Risk and Compliance Management* – risk analysis and mapping of ZTA security characteristics to cybersecurity standards and recommended practices **(you are here)**

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-35A*, which describes the following topics:

- challenges that enterprises face in migrating to the use of ZTA
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-35B*, which describes what we did and why.

Also, Section 3 of this guide, *NIST SP 1800-35E,* will be of particular interest. Section 3, ZTA Reference Architecture Security Mappings, maps logical components of the general ZTA reference design to security characteristics listed in various cybersecurity standards and recommended practices documents, including *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework), *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53), and *Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028*.

You might share the *Executive Summary, NIST SP 1800-35A*, with your leadership team members to help them understand the importance of migrating toward standards-based ZTA implementations that align to the concepts and principles in NIST SP 800-207, *Zero Trust Architecture*.

IT professionals who want to implement similar solutions will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-35C*, to replicate all or parts of the builds created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution. Also, you can use *Functional Demonstrations, NIST SP 1800-35D*, which provides the use cases that have been defined to showcase ZTA security capabilities and the results of demonstrating them with each of the example implementations.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a ZTA. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but example solutions. This is a preliminary draft guide. As the project progresses, the preliminary draft will be updated, and additional volumes will also be released for comment. We seek feedback on the publication's contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to nccoe-zta-project@list.nist.gov.

2 Risk Management

This section discusses the threats and vulnerabilities addressed by the ZTA reference architecture and the residual risk not addressed by ZTA.

2.1 Threats

Conventional network security has focused on perimeter defense. Historically, most corporate resources have been located within and protected by the enterprise's network perimeter, which tended to be large and static. Subjects that are inside the network perimeter are often assumed to be implicitly trusted and are given broad access to the corporate resources within the network perimeter. Attempts to access resources from outside the network perimeter, i.e., from the internet, are often subject to more scrutiny than those originating from within. However, a subject can be compromised regardless of whether it is inside or outside of the network perimeter. Once a subject is compromised, malicious actors—through impersonation and escalation—can gain access to the resources that the subject is authorized to access and move laterally within the network perimeter to access adjacent corporate resources.

By protecting each resource individually and employing extensive identity, authentication, and authorization measures to verify a subject's requirement to access each resource, zero trust can ensure that authorized users, applications, and systems have access to only those resources that they absolutely have a need to access in order to perform their duties, not to a broad set of resources that all happen to be within the network perimeter. This way, if a malicious actor does manage to gain unauthorized access to one resource, this access will not provide them with any advantage when trying to move laterally to other nearby resources. To compromise those other resources, the attacker would be required to figure out how to circumvent the mechanisms that are protecting those resources individually because it is not possible to reach those resources from nearby compromised resources. In this way, ZTA limits the insider threat because instead of having permission to access all resources within the network perimeter, malicious insiders would only be permitted to access those resources they require to perform their official roles.

In addition, once a subject is granted access to the resource, this access is often permitted to continue for a substantial period of time without being reevaluated based on a defined policy. The access session is often not monitored or subject to behavioral analysis, and the configuration and health of the devices being used to access resources may be subject to initial, but not ongoing, scrutiny. So, if a subject does manage to gain unauthorized access to a resource, the subject often has ample time to exfiltrate or modify valuable information or further compromise the resource and/or use it as a point from which to pivot and attack other corporate resources. ZTA limits these threats by performing continual verification of a subject’s identity and authorization to access a resource. It may also perform behavioral analysis and validation of each system’s health and configuration, and consider other factors such as day, time, and location of subject and resource. Based on the organization’s defined policy, ZTA makes dynamic ongoing assessments of the risk of each access request in real-time to ensure it poses an acceptable level of risk according to corporate policy.

A number of trends in how corporations conduct business have also introduced additional security threats. These trends include increased use of cloud computing and remote work.

The growth in cloud computing has meant that enterprises are now storing critical corporate resources (e.g., databases, applications, servers) in the cloud (i.e., outside of the traditional network perimeter) as well as on-premises. As a result, these resources cannot be protected by the network perimeter strategy. A new protection paradigm is needed that focuses on protecting resources individually, no matter where they are located, so that they are not at risk of being subjected to security policies that are not under corporate control or not enforced consistently across all enterprise resources. Often the clouds in which resources are hosted are multitenant, meaning that different corporate enterprises have authorized access to their own portions of the cloud infrastructure, with each tenant reliant on the cloud service provider to enforce this separation. If a malicious actor were to figure out how to subvert cloud security and move from one tenant’s account to the next, corporate resources would be at risk. Use of ZTA to protect each resource individually serves as further assurance that the resources will not be accessible to cloud users from other enterprises, nor will they be accessible to users from within the enterprise who do not have a need to access them.

The growth of the remote workforce, as well as collaboration with corporate partners and dependence on contractors are other trends that are also challenging the conventional security paradigm. The subjects requesting authorized access to corporate resources may not necessarily be within the network perimeter. They may be employees working from home or from a coffee shop’s public Wi-Fi via the internet, or a corporate partner, contractor, customer, or guest that requires access to some resources but must be restricted from accessing other resources. By relying on strong identity, authentication, and authorization services to determine precisely which resources a subject is authorized to access with respect to their role in or relationship to the corporation, ZTA can restrict subjects to accessing only those resources that they have a need to access and ensure that they are not permitted to access any other resources.

The use of cloud applications or other external components that need access to some corporate resources is another trend that is rendering the conventional security paradigm obsolete. Although an external component may need to access some corporate resources in order to perform a required function, if it is granted blanket access to all resources within the network perimeter, it becomes a dangerous potential attack vector. By focusing on the identity, credentials, and authorization of each subject making an access request, whether that subject be a human user or a non-human application, component, or other system, ZTA can help ensure that all subjects are permitted to access only those resources that they are required to access in order to fulfill their purpose. In a ZTA architecture, a component that becomes compromised is of limited usefulness to the attacker. It can be used to access only those resources that it is authorized to access rather than serving as a general attack vector.

2.2 Vulnerabilities

The vulnerability of resources to unauthorized access in an environment in which the network perimeter defense paradigm is in effect is a consequence of the implicit trust that is placed in all subjects within the perimeter. This situation is exacerbated by the fact that all resources within the perimeter tend to be reachable from one another, but none are individually protected beyond the blanket protections that the security perimeter provides from outside threats. Hence, the compromise of a single subject can result in the compromise of many resources that are reachable within the perimeter, regardless of whether the subject has a business need to access those resources. In addition, resource access sessions are not evaluated on a continuing basis, making resources vulnerable to attack by malicious actors that manage to compromise subjects or resources after an initial access request has been granted.

2.3 Risk

The reference architecture and the example ZTA solutions implemented are designed to ensure that authorized users, applications, systems, and other non-human entities have access to only those resources that they absolutely have a need to access in order to perform their duties, not to a broad set of resources that all happen to be within the network perimeter. A network protected by a ZTA will be vulnerable to exploitation if one or more of the core components of the ZTA itself (e.g., the policy engine [PE], policy administrator [PA], or a policy enforcement point [PEP]) or the functional components that provide crucial information to the core components (e.g., endpoint detection and response capabilities; identity, credential, and access management capabilities; data security capabilities; security analytics capabilities) become compromised. ZTA may help prevent malicious insiders and compromised subjects from accessing resources that they are not authorized to access, and it may help prevent an attacker from using a compromised resource as a landing place from which to pivot and attack additional corporate resources. ZTA may also help find and identify already-compromised subjects, systems, and resources through continuous, real-time monitoring and behavioral analysis. However, ZTA does not help owners correct compromised systems or resources.

3 ZTA Reference Architecture Security Mappings

This section provides mappings between cybersecurity functions performed by the ZTA reference design's logical components (see NIST SP 1800-35B Section 4.1) and security characteristics enumerated in a variety of relevant cybersecurity documents. These mappings are intended for any organization that is interested in implementing ZTA or that has begun or completed a ZTA implementation. They provide information on how ZTA cybersecurity functions from the NCCoE's ZTA project are related to:

- *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework—CSF) 1.1 [3] Subcategories,
- NIST SP 800-53r5 (*Security and Privacy Controls for Information Systems and Organizations*) [4] security controls, and
- Executive Order (EO) 14028 [5] security measures defined in *Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028* [6]

All of the elements in these mappings—the ZTA cybersecurity functions, CSF Subcategories, SP 800-53 controls, and EO 14028 security measures—are concepts involving ways to reduce cybersecurity risk and meet compliance requirements involving sectors' specific recommended practices. In future versions of this document, the NCCoE may perform additional mappings between ZTA cybersecurity functions and security characteristics enumerated in other cybersecurity standards, directives, recommended practices, memoranda, etc.

3.1 Use Cases

This mapping was developed to support these two primary use cases. They are not intended to be comprehensive.

1. **Why should organizations implement ZTA?** This use case identifies how implementing ZTA can support an organization with achieving CSF Subcategories, SP 800-53 controls, and EO 14028 security measures. This helps communicate to an organization's senior management that expending resources to implement ZTA can also aid in fulfilling other security requirements.
2. **How can organizations implement ZTA?** This use case identifies how an organization's existing implementations of CSF Subcategories, SP 800-53 controls, and EO 14028 security measures can help support a ZTA implementation. An organization wanting to implement ZTA might first assess its current security capabilities so that it can plan how to add missing capabilities and enhance existing capabilities in order to implement ZTA. Organizations can leverage their existing security investments and prioritize future security technology deployment to address the gaps.

3.2 Mapping Producers

The NCCoE ZTA project team performed the initial mapping with input and feedback from the collaborators who have contributed technology to demonstrate ZTA capabilities.

3.3 Mapping Approach

In addition to performing these general mappings between the ZTA reference design's cybersecurity functions and various sets of security characteristics, the NCCoE intends to also develop mappings that are specific to each ZTA example implementation. To develop these build-specific mappings, the NCCoE intends to ask each collaborator for each build to indicate the mapping between the cybersecurity functions its technology components provide in that build and the sets of security characteristics. These build-specific mappings will appear in future drafts of this document. Using the logical components in the ZTA reference design as the organizing principle for mapping cybersecurity functions to security characteristics is intended to make it easier for collaborators to map their build-specific technology contributions. Using this approach, the build-specific technology mappings will be instantiations of the project's general reference design mappings for each document.

3.3.1 Mapping Terminology

A mapping defines a relationship between two entities.

For this mapping, we have used the following relationship types to describe how the functions in our ZTA reference design are related to the NIST reference documents. Note that the *Supports* relationship applies to use case 1 only and the *Is Supported B*y relationship applies to use case 2 only.

- **Supports**: ZTA function X *supports* security control/subcategory/measure Y when X can be applied alone or in combination with one or more other functions to achieve Y in whole or in part.
- **Is Supported By**: ZTA function X *is supported by* security control/subcategory/measure Y when Y can be applied alone or in combination with one or more other security controls/subcategories/measures to achieve X in whole or in part.
- **No Relationship**: ZTA function X has *no relationship* to security control/subcategory/measure Y when X and Y are not directly related.

Each relationship of type *Supports* (A supports B) or *Is Supported By* (B is supported by A) has one of the following properties assigned to it:

- **Example of**: The supporting concept A is an *example of* how the supported concept B can be achieved in whole or in part. However, B could also be achieved without applying A.
- **Integral to**: The supporting concept A is *integral to* the supported concept B. A must be applied as part of achieving B.
- **Precedes**: The supporting concept A *precedes* the supported concept B when A must be achieved before applying B.

When determining whether a ZTA function's support for a given CSF Subcategory, SP 800-53 control, or EO 14028 security measure is integral to that support versus an example of that support, we do not consider how that function may in general be used to support the subcategory, control, security measure, or other item. Rather, we consider only how that function is intended to support that subcategory, control, security measure, or other item within the context of our ZTA reference design.

Also, when determining whether a ZTA function is supported by a CSF subcategory with the relationship property of *precedes*, we do not consider whether or not it is possible to apply the function without first achieving the subcategory. Rather, we consider whether or not, according to our ZTA reference design, the subcategory is to be achieved prior to applying that function.

3.3.2 Mapping Process

The process that the NCCoE used to create the mapping from the logical components of the ZTA reference design to the security characteristics of a given document was as follows:

1. Create a table that lists each of the logical components of the ZTA reference design in column 1.
2. Describe each logical component's cybersecurity function in column 2.
3. Map each cybersecurity function to each of the security characteristics in the document to which the function is most strongly related, and list each of these security characteristics on different sub-rows within column 3. Begin each security characteristic entry with an underlined keyword that describes the mapping's relationship type (e.g., *Supports*, *Is Supported By*, *or No Relationship).* After the keyword describing the relationship type, put in parentheses the underlined keyword(s) describing the relationship's property (e.g., *Example of*, *Integral to*, or *Precedes*).
4. In the fourth column, provide a brief explanation of why that relationship type and property apply to the mapping.
5. After completing the mapping table entries as described above for all the logical components in the reference design, examine the mapping in the other direction, i.e., starting with the security characteristics listed in the document and considering whether they have a relationship to the logical components' cybersecurity functions in the reference design. In other words, step through each of the security characteristics in the document and determine if there is some logical component in the reference design that has a relationship to that security characteristic. If so, add an entry for that security characteristic mapping to that logical component's row in the table. By examining the mapping in both directions in this manner, security characteristic mappings are less likely to be overlooked or omitted.

The NCCoE applied this mapping process separately for each reference document. None of the mappings are intended to be exhaustive; they all focus on the strongest relationships involving each cybersecurity function in order to help organizations prioritize their work. Mapping every possible relationship, no matter how tenuous, would create so many mappings that they would not have any value in prioritization.

3.3.3 Mapping Subsection Organization

The mappings are organized in the remainder of this document as follows:

- Section 3.4 – NIST CSF 1.1
- Section 3.5 – NIST SP 800-53r5
- Section 3.6 – EO 14028 Security Measures

In each section, the mapping from the logical components of the ZTA reference design is provided first, followed by each of the build-specific mappings that has been completed so far. Builds are denoted using the abbreviations defined in volume B, where *E1B1*, for example, refers to Build 1 of the example implementation in Enterprise 1, *E2B1* refers to Build 1 of the example implementation in Enterprise 2, and *E1B2* refers to Build 2 of the example implementation in Enterprise 1. The composition of each build is described in an appendix of volume B.

3.4 Mapping Between ZTA Functions and the CSF Subcategories

In Table 3-1 we provide a mapping between the logical components of the ZTA reference design and the NIST CSF subcategories. This table indicates how ZTA functions help support CSF subcategories and vice versa.

Table 3-1 Mapping between ZTA Reference Design Logical Components and CSF Subcategories

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	Decides whether to grant, deny, or revoke access to a resource, based on enterprise policy, information from functional components, and a trust algorithm	Supports (integral to) PR.AC-3: Remote access is managed	The PE makes remote access decisions based on policy. In a ZTA, the PE must be applied to help manage remote access. Note that in ZTA, the same policy applies to all access requests, regardless of whether they are remote or local. Although ZTA does not differentiate between local and remote access policy, however, compliance frameworks might.
Policy Administrator (PA)	Executes the PE's policy decision by sending commands to a PEP that establishes and shuts down the communication path between subject and resource	Supports (integral to) PR.AC-3: Remote access is managed	The PA supports the enforcement of remote access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced. In a ZTA, the PA must be applied to help manage remote access.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
Policy Enforcement Point (PEP)	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource; forwards requests to and receives commands from the PA	Supports (integral to) PR.AC-3: Remote access is managed	The PEP enforces remote access decisions. In a ZTA, the PEP must be applied in order to help manage remote access.
		Supports (example of) PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	The PEP can prevent unauthorized access to the portions of the enterprise that it guards. If it is used to protect a single resource, then it does not necessarily provide network segregation or network segmentation. However, it can be deployed to protect and segregate discrete network segments. Network segmentation may also be provided by other mechanisms besides a PEP.
		Supports (integral to) PR.DS-5: Protections against data leaks are implemented	The PEP prevents unauthorized transfer of information out of the portion of the enterprise that it guards. In a ZTA, the PEP must be applied to help protect against data leaks.
		Supports (integral to) PR.PT-4: Communications and control networks are protected	To support ZTA, the data plane and control plane (networks) must be logically separate. The PEP is the only component that can send and receive messages from both planes. It protects the planes from each other and ensures that the control plane is not directly accessible by enterprise assets and resources.
		Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	The PEP may be used to monitor connections between a subject and an enterprise resource to detect prohibited or suspicious activity. However, it must not necessarily be configured to do so. Network monitoring may also be provided by other mechanisms besides a PEP.
		Supports (integral to) RS.MI-1: Incidents are contained	In a ZTA, the PEP is central to containing incidents. If a resource is compromised, the PEPs protecting other resources prevent attackers from moving laterally from the compromised resource to the resources protected by those other PEPs.
Access Policies	Define the conditions that must be met to grant each subject	Is supported by (precedes) ID.AM-3: Organizational	In order to properly formulate policy regarding each subject's access to resources, the expected, permissible data

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	access to each resource	communication and data flows are mapped	flows between subjects and resources must be well-understood.
		Is supported by (precedes) ID.AM-4: External information systems are catalogued	In order to properly formulate policy regarding each subject's access to external information systems, the systems to which access is to be permitted must be catalogued.
		Is supported by (precedes) ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	The access policies that are formulated for the organization must be based in part on the classification, criticality, and business value of the resources to which access is being requested.
		Supports (example of) ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	The organization can define "confidence level" or similar access policies that calculate risk based on various factors such as detected threats and vulnerabilities, and then determine the ZTA's response to a given access request based on this calculated risk.
		Supports (example of) ID.RA-6: Risk responses are identified and prioritized	The organization can define "confidence level" or similar access policies that calculate risk based on various factors such as detected threats and vulnerabilities, user behavior, and user location, and then base the ZTA's response to a given access request based on this calculated risk. For example, if the risk is determined to be at or below a certain threshold, the request would be permitted. If the risk is above a certain threshold, the request would be denied.
		Supports (integral to) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least	Access policies are the mechanisms for ensuring that permissions and authorization to access any given resource conform with the principles of least privilege and separation of duties.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		privilege and separation of duties	
		Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Access policies are the mechanisms for ensuring that subjects are authenticated commensurate with the risk of the transaction.
		Is supported by (precedes) PR.IP-12: A vulnerability management plan is developed and implemented	The organization Is expected to develop a vulnerability management plan and to define and enforce its access policies based in part on this plan.
		Is supported by (precedes) DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Before defining access policies, a baseline of network operations and expected data flows for users and systems must be established so that the authorized data flows are well-understood and policies that enforce them can be defined.
		Supports (example of) DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Once established, access policies manage and enforce the desired data flows.
		Supports (example of) DE.AE-5: Incident alert thresholds are established	Policies that set incident alert thresholds can be defined such that when the threshold is reached, a specified action will be performed, e.g., alert generation.
Identity Management	Creates and manages enterprise user and device accounts, identity records, role	Is supported by (precedes) ID.AM-6: Cybersecurity roles and responsibilities for the	Identity Management supports the creation, storage, and management of digital representations of cybersecurity roles and their associated permissions and

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	information, and access attributes that form the basis of access decisions within an organization to ensure the correct subjects have the appropriate access to the correct resources at the appropriate time.	entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	responsibilities. It also supports the assignment of roles to user identities. To be able to create, store, and manage these representations of user roles and responsibilities, the roles and responsibilities themselves must have already been established.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Identity Management supports issuance, storage, management, and revocation of identities and their associated roles and credentials. It also supports the verification of credentials when performing user and device authentication.
		Supports (integral to) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Identity Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of least privilege and separation of duties, and it is used to assign users to roles that best match their responsibilities, based on the principle of least privilege and separation of duties, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	Identity Management stores and manages the association of identities with credentials.
Access & Credential Management	Manages access to resources by performing user and device authentication (e.g., SSO and MFA) and using identity, role, and access attributes to determine which	Is supported by (precedes) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	To determine whether an access request is authorized, the Access and Credential Management component authenticates the user or device that is requesting access by verifying the credentials that are bound to the user or device and asserted as part of the access request. The user and device identities must be asserted for this component to be able to authenticate them.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	access requests are authorized.	Supports (integral to) PR-AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The key function of the Access and Credential Management component is to perform user and device authentication.
		Supports (example of) RS.MI-1: Incidents are contained	If a legitimate user's credentials are stolen and an attacker uses them to gain unauthorized access to a resource, the Access and Credential Management component will limit the attacker to accessing only those resources that the legitimate user's role or attributes allow. This is one example of how incidents can be contained.
		Supports (example of) RS.MI-2: Incidents are mitigated	If a legitimate user's credentials are stolen and an attacker uses them to gain unauthorized access to a resource, the attacker will only be allowed to access that resource in the way that the legitimate user's role allows (e.g., read-only vs. read-write). This is one example of how incidents can be mitigated.
		Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	The Access and Credential Management component can perform ongoing, intermittent user authentication and authorization, thereby monitoring for unauthorized users and devices.
Federated Identity	Aggregates and correlates all attributes relating to an identity or object that is being authorized by a ZTA. It enables users of one domain to	Is supported by (precedes) ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g.,	The Federated Identity component enables enforcement of the cybersecurity roles and responsibilities that have been established and stored for many different groups—the enterprise workforce and third-party stakeholders (e.g., suppliers, customers, partners) to be managed and enforced. These roles and responsibilities

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Federated identity encompasses the traditional ICAM data, supports identities that may be part of a larger federated ICAM community, and may include non-enterprise employees.	suppliers, customers, partners) are established	must already be established before they can be enforced.
Identity Governance	Provides policy-based, centralized, automated processes to manage user identity and access control functions (e.g., ensuring segregation of duties, role management, logging, auditing, access reviews, analytics, and reporting) to ensure compliance with requirements and regulations.	Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	A key function of the Identity Governance component is to support the auditing of identities and credentials.
		Supports (integral to) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	The Identity Governance component manages access permissions and authorizations in a way that incorporates the principles of least privilege and separation of duties.
		Is supported by (precedes) ID.GV-1: Organizational cybersecurity policy is established and communicated	The Identity Governance component ensures that the organization's cybersecurity policy is enforced in such a way that it complies with regulatory, legal, and other governance-related requirements. This policy must already be established before it can be enforced by the Identity Governance component.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (integral to) ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	The Identity Governance component supports the coordination and alignment of cybersecurity roles and responsibilities with internal roles and external partners to ensure that the organization operates in accordance with regulatory, legal, and other governance-related requirements.
		Is supported by (precedes) ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	The processes that the Identity Governance component follows have been defined to ensure that the organization operates in conformance with all legal and regulatory requirements. These requirements must be well understood in order to define the Identity Governance processes. As these requirements change, they must be managed on an ongoing basis, and they may require changes to identity governance processes.
		Supports (integral to) ID.GV-4: Governance and risk management processes address cybersecurity risks	The processes that the Identity Governance component follows are defined and managed with the objective of addressing cybersecurity risks.
		Supports (integral to) PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	The Identity Governance component performs logging and audits all identity management activities in accordance with policy and regulations.
Multi-Factor Authentication (MFA)	Authenticates user identity by requiring the user to provide not only something they know (e.g., a password), but also something they have (e.g., a token).	Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks	The MFA component enables users to be authenticated using a second factor, which is required for higher-risk access requests.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		and other organizational risks)	
Unified Endpoint Management (UEM)/Mobile Device Management (MDM)	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities and threats; monitor for suspicious activity to prevent and detect intrusions; prevent, detect, and disable malware, viruses, and other malicious or unauthorized traffic; repair infected files when possible; provide alerts and recommend remediation actions; and encrypt data. Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data from devices if needed, tracks user	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	For a device to be enrolled into a UEM/MDM system, the device must be known to be part of the organization's inventory.
		Supports (integral to) ID.AM-2: Software platforms and applications within the organization are inventoried	The UEM/MDM installs, manages, configures, and updates applications on UEM/MDM-managed devices, so it provides inventory information regarding these applications.
		Supports (integral to) ID.RA-1: Asset vulnerabilities are identified and documented	The UEM/MDM may be able to identify and remediate device vulnerabilities by updating software on managed devices, for example.
		Supports (integral to) ID.RA-3: Threats, both internal and external, are identified and documented	The UEM/MDM may monitor for suspicious activity; detect and disable malware, viruses, and other malicious traffic; and repair infected files on managed devices.
		Supports (integral to) PR.AC-3: Remote access is managed	The UEM/MDM may prevent a remote device that it is managing from being able to access any resources until the device is brought into compliance.
		Supports (example of) PR.DS-1: Data-at-rest is protected	The UEM/MDM may encrypt data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
		Supports (example of) PR-DS-2: Data-in-transit is protected	The UEM/MDM may encrypt data sent from the device, but this data could also be encrypted via a different mechanism.
		Supports (example of) PR.DS-5: Protections against data leaks are implemented	The UEM/MDM may track user activity on the device and monitor for unauthorized traffic to help prevent, detect, and mitigate data leaks.
		Supports (example of) PR.DS-6: Integrity checking mechanisms	The UEM/MDM may use integrity checking to verify updates prior to installing them. It may also use integrity

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	activity on devices, and detects and addresses security issues on the device.	are used to verify software, firmware, and information integrity	checking to verify compliance of device software and firmware.
		Supports (example of) PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	The UEM/MDM may rely on device attestation or similar mechanisms that use integrity checking to verify the hardware integrity of the device before trusting the device.
		Supports (integral to) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	The UEM/MDM ensures that devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware. UEM/MDM enforces and maintains these baselines at endpoints.
		Is supported by (precedes) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	The baseline configuration on the endpoints that the UEM/MDM enforces must have been developed based on security principles, such as the concept of least functionality, in accordance with the organization's policies. UEM/MDM operation depends on the existence of such baselines.
		Supports (example of) PR.IP-6: Data is destroyed according to policy	The UEM/MDM can remotely delete applications and data from devices as needed according to policy. Other mechanisms are also capable of destroying data as needed.
		Is supported by (precedes) PR.IP-12: A vulnerability management plan is developed and implemented	The UEM/MDM can mitigate and remediate vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies. These policies must exist before the UEM/MDM can enforce them, and they constitute at least one portion of the

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			organization's vulnerability management plan.
		Supports (example of) PR.PT-2: Removable media is protected and its use restricted according to policy	The UEM/MDM can restrict the use of removable media as required by policy.
		Supports (example of) PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	The UEM/MDM can be used to configure devices to provide only essential capabilities.
		Supports (example of) DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	The UEM/MDM can monitor user activity for suspicious behavior.
		Supports (example of) DE.CM-4: Malicious code is detected	The UEM/MDM prevents, detects, and disables numerous types of malicious code.
		Supports (example of) DE.CM-5: Unauthorized mobile code is detected	The UEM/MDM may be able to detect unauthorized mobile code.
		Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	The UEM/MDM monitors the device for unauthorized software and connections.
		Supports (integral to) RS.MI-1: Incidents are contained	The UEM/MDM performs many activities that help to contain incidents, such as detecting and disabling malware and other malicious or unauthorized activity; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness to someone who steals a locked device.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (integral to) RS.MI-2: Incidents are mitigated	The UEM/MDM performs many activities that help to mitigate incidents, such as detecting and disabling malware and other malicious or unauthorized activity; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness to someone who steals a locked device.
Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP)	Detects and stops threats to endpoints through an integrated suite of endpoint protection technologies including antivirus, data encryption, intrusion prevention, EDR, and data loss prevention (DLP). May include mechanisms that are designed to protect applications and data; ensure device compliance with policies regarding hardware, firmware, software, and configuration; monitor endpoints for vulnerabilities, suspicious activity, intrusion, infection, and malware; block unauthorized traffic; disable malware and repair infections;	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	For a device to have EDR/EPP software installed on it, the device must be known to be part of the organization's inventory.
		Supports (integral to) ID.AM-2: Software platforms and applications within the organization are inventoried	The EDR/EPP can inventory software on the device.
		Supports (integral to) ID.RA-1: Asset vulnerabilities are identified and documented	The EDR/EPP scans the device to detect missing patches or outdated software and report them. It can also install patches if instructed to do so later.
		Supports (integral to) ID.RA-3: Threats, both internal and external, are identified and documented	The EDR/EPP detects and disable malware, viruses, and other signature-based threats.
		Supports (integral to) PR.AC-3: Remote access is managed	The EDR/EPP may include a firewall that blocks unauthorized connections to and from the device.
		Supports (example of) PR.DS-1: Data-at-rest is protected	The EDR/EPP may encrypt data stored on the device, but data stored on the device could also be encrypted via a different mechanism.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
	manage and administer software and updates; monitor behavior and critical data; and enable endpoints to be tracked, troubleshooted, and wiped, if necessary.	Supports (example of) PR-DS-2: Data-in-transit is protected	The EDR/EPP may encrypt data sent from the device, but this data could also be encrypted via a different mechanism.
		Supports (example of) PR.DS-5: Protections against data leaks are implemented	The EDR/EPP may include a firewall that blocks unauthorized traffic to and from the device.
		Supports (example of) PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	The EDR/EPP may use integrity checking to verify updates prior to installing them. It may also use integrity checking to verify compliance of device software and firmware.
		Supports (integral to) and Is supported by (precedes) PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	The EDR/EPP ensures that devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware. This baseline that the EDR/EPP enforces must have been developed based on security principles, such as the concept of least functionality, in accordance with the organization's policies. So EDR/EPP operation depends on the existence of such baselines, but it also enforces and maintains these baselines.
		Supports (example of) PR.IP-6: Data is destroyed according to policy	The EDR/EPP can remotely delete applications and data from devices as needed according to policy. Other mechanisms are also capable of destroying data as needed.
		Is supported by (precedes) PR.IP-12: A vulnerability management plan is developed and implemented	The EDR/EPP can mitigate and remediate vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies. These policies must exist before the EDR/EPP can enforce them, and they constitute at least one portion of the organization's vulnerability management plan.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (example of) PR.PT-2: Removable media is protected and its use restricted according to policy	The EDR/EPP can restrict the use of removable media as required by policy.
		Supports (example of) PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	The EDR/EPP can be used to configure devices to provide only essential capabilities.
		Supports (example of) DE.CM-4: Malicious code is detected	The EDR/EPP detects and disable malware, viruses, and other signature-based threats.
		Supports (example of) DE.CM-5: Unauthorized mobile code is detected	The EDR/EPP may be able to detect unauthorized mobile code.
		Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	The EDR/EPP monitors the device for unauthorized software and connections.
		Supports (example of) DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	The EDR/EPP can monitor user activity for suspicious behavior.
		Supports (integral to) RS.MI-1: Incidents are contained	The EDR/EPP performs many activities that help to contain incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (integral to) RS.MI-2: Incidents are mitigated	The EDR/EPP performs many activities that help to mitigate incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.
Security Information and Event Management (SIEM)	Collects and consolidates security information and security event data from many sources; correlates and analyzes the data to help detect anomalies and recognize potential threats and vulnerabilities; and logs the data to adhere to data compliance requirements.	Supports (example of) DE.AE-2: Detected events are analyzed to understand attack targets and methods	The SIEM collects security and event information from many components. This aggregated data may be analyzed to understand attack targets and methods.
		Supports (integral to) DE.AE-3: Event data are collected and correlated from multiple sources and sensors	A key function of the SIEM is to collect and correlate security event data from multiple sources.
		Supports (example of) DE.AE-4: Impact of events is determined	Security analysts may use SIEM data to help them determine the impact of events.
		Supports (example of) PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	The SIEM can aggregate logs of security information and event activity as required by policy.
		Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	SIEM logs can be examined as an indirect and non-real-time method of monitoring network activity to detect anomalous behavior and other indicators of potential cybersecurity events.
		Supports (example of) RS.AN-2: The impact of the incident is understood	The SIEM logs can provide data that helps security analysts to understand the impact of cybersecurity incidents.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		Supports (example of) RS.AN-3: Forensics are performed	The SIEM logs can provide data that can help security analysts to perform forensic analysis of cybersecurity incidents.
Vulnerability Scanning and Assessment	Scans and assesses the enterprise infrastructure and resources for security risks; identifies vulnerabilities and misconfigurations; and provides remediation guidance regarding investigating and prioritizing responses to incidents.	Supports (integral to) DE.CM-8: Vulnerability scans are performed	A key function of the Vulnerability Scanning and Assessment component is to perform vulnerability scans.
Security Integration Platform	Integrates the SIEM and other security tools into a single pane of glass to support generation of insights into threats and help track, manage, and resolve cybersecurity incidents. Executes predefined incident response workflows to automatically analyze information and orchestrate the operations required to respond.	Supports (example of) RS.RP-1: Response plan is executed during or after an incident	A Security Integration Platform can execute predefined incident response workflows.
		Supports (example of) RS.AN-2: The impact of the incident is understood	Security analysts can use a Security Integration Platform to visualize security events and their impacts, thereby enabling incidents to be better understood.
		Supports (example of) RS.AN-3: Forensics are performed	Security analysts can use a Security Integration Platform to help them perform forensic analysis of cybersecurity incidents.
Security Validation	Continuously monitor, measure, and validate the effectiveness of the ZTA's cybersecurity controls	Supports (integral to) DE.DP-3: Detection processes are tested	Security Validation is used to test and verify the effectiveness of detection processes and other ZTA cybersecurity controls.
		Supports (example of) DE.DP-5: Detection processes are continuously improved	The organization can use Security Validation to continuously monitor, measure, and validate the effectiveness of cybersecurity controls, thereby enabling

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
			the organization to continuously improve the detection processes.
Network Discovery	Discovers, classifies, and assesses the risk posed by devices and users on the network.	Supports (integral to) ID.RA-3: Threats, both internal and external, are identified and documented	A key function of Network Discovery is to monitor the network to find, identify, and document unknown and/or unexpected devices and activity that may pose a threat to the organization.
		Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	Network Discovery can help identify unknown and/or unexpected devices and activity that may be indicative of suspicious events, making it an example of how the network can be monitored to detect potential cybersecurity events.
		Supports (integral to) DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	A key function of the Network Discovery component is to discover unauthorized devices and connections on the network.
Virtual Private Network	Enables authorized remote users to securely access the inside of the enterprise. (Once inside, the ZTA manages the user's access to resources.)	Supports (example of) PR.AC-3: Remote access is managed	Requiring remote users to access the enterprise via VPN is one mechanism that can be used to manage remote access.
		Supports (example of) PR.DS-2: Data-in-transit is protected	VPNs are one method of encrypting data in transit.
		Supports (example of) DE.CM-1: The network is monitored to detect potential cybersecurity events	Traffic sent on the VPN can be monitored to detect prohibited or suspicious activity.
Certificate Management	Provides automated capabilities to issue, install, inspect, revoke, renew, and otherwise manage TLS certificates.	Is supported by (precedes) ID.AM-2: Software platforms and applications within the organization are inventoried	Servers and software must be identified and known to be within the organization's inventory in order for them to be issued certificates.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for	Verification (i.e., authentication) of the identity of servers depends on the issuance, use, and management of TLS certificates.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to CSF Subcategories (and Relationship Properties)	Relationship Explanation
		authorized devices, users, and processes	
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	Proofing (i.e., authenticating) server identities requires TLS certificates.
		Supports (integral to) PR.DS-2: Data-in-transit is protected	The setup of encrypted TLS transport connections depends on TLS certificates.
		Supports (integral to) PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	TLS transport connections provide integrity checking on their traffic, and the setup of TLS connections depends on TLS certificates. Any integrity mechanism that relies on public key cryptography is supported by TLS certificates.

3.4.1 Mapping between E1B1 and the CSF Subcategories

This mapping will be provided in a future version of this document.

3.4.2 Mapping between E2B1 and the CSF Subcategories

This mapping will be provided in a future version of this document.

3.4.3 Mapping between E3B1 and the CSF Subcategories

This mapping will be provided in a future version of this document.

3.4.4 Mapping between E1B2 and the CSF Subcategories

This mapping will be provided in a future version of this document.

3.4.5 Mapping between E3B2 and the CSF Subcategories

This mapping will be provided in a future version of this document.

3.5 Mapping Between ZTA Functions and NIST SP 800-53 Controls

In Table 3-2 we provide a mapping between the logical components of the ZTA reference design and NIST SP 800-53 security controls. This table indicates how ZTA functions help support NIST SP 800-53 controls. Because hundreds of NIST SP 800-53 controls can help support ZTA functions, we have omitted use case 2 (see Section 3.1), identifying how existing SP 800-53 controls can help support a ZTA implementation. Readers needing to determine how their SP 800-53 implementations apply to a ZTA implementation can follow the Risk Management Framework.

Table 3-2 Mapping between ZTA Reference Design Logical Components and NIST SP 800-53 Controls

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	Decides whether to grant, deny, or revoke access to a resource, based on enterprise policy, information from functional components, and a trust algorithm	Supports (integral to) AC-17: Remote Access	The PE authorizes each type of remote access to the system prior to allowing such connections.
		Supports (integral to) AC-19: Access Control for Mobile Devices	The PE authorizes the connection of mobile devices to organizational systems.
		Supports (integral to) AC-20: External Systems	The PE authorizes or denies access to systems that are used by but are not part of on-premises systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness.
		Supports (integral to) AC-24: Access Control Decisions	The key function of the PE is to make access control decisions based on policy.
		Supports (integral to) SC-15: Collaborative Computing Devices and Applications	The PE permits or prohibits remote activation of collaborative computing devices and applications.
Policy Administrator (PA)	Executes the PE's policy decision by sending commands to a PEP that establishes and shuts down the communication path between subject and resource	Supports (integral to) AC-3: Access Enforcement	The PA supports the enforcement of access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
		Supports (integral to) AC-17: Remote Access	The PA supports the enforcement of remote access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
		Supports (integral to) AC-19: Access Control for Mobile Devices	The PA conveys mobile device access decision information from the PE to the PEP, where the decision can be enforced.
		Supports (integral to) AC-20: External Systems	The PA conveys external system access decision information from the PE to the PEP, where the decision can be enforced.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) SC-15: Collaborative Computing Devices and Applications	The PA conveys collaborative computing device activation decision information from the PE to the PEP, where the decision can be enforced.
Policy Enforcement Point (PEP)	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource; forwards requests to and receives commands from the PA	Supports (integral to) AC-2: Account Management	The PEP enforces authorized access to the system based on valid access authorization or intended system usage.
		Supports (integral to) AC-3: Access Enforcement	The PEP enforces access decisions.
		Supports (integral to) AC-4: Information Flow Enforcement	The PEP enforces approved authorizations for controlling the flow of information within the system and between connected systems. The data plane and control plane (networks) are logically separate. The PEP is the only component that can send and receive messages from both planes. It can protect the planes from each other and ensure that the control plane is not directly accessible by enterprise assets and resources.
		Supports (integral to) AC-12: Session Termination	The PEP can terminate connections to enforce compliance with policies.
		Supports (integral to) AC-17: Remote Access	The PEP can enforce remote access decisions.
		Supports (integral to) AC-18: Wireless Access	The PEP can enforce wireless access decisions.
		Supports (integral to) AC-19: Access Control for Mobile Devices	The PEP can enforce access decisions regarding connection to mobile devices.
		Supports (integral to) AC-20: External Systems	The PEP can enforce access decisions regarding connection to external systems.
		Supports (integral to) CA-7: Continuous Monitoring	The PEP monitors connections between a subject and an enterprise resource to detect prohibited or suspicious activity.
		Supports (integral to) IR-4: Incident Handling	If a resource is compromised, incidents are contained because attackers cannot move laterally from the compromised resource to any resources that are not also in that part of the enterprise guarded by the compromised resource's PEP.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (example of) SC-7: Boundary Protection	The PEP can enforce access decisions to key internal managed interfaces within the system including publicly accessible system components that are separated from internal organizational networks. It can prevent unauthorized access to the portions of the enterprise that it guards. If it is used to protect a single resource, then it does not necessarily provide network segregation or network segmentation. However, it can be deployed to protect and segregate discrete network segments.
		Supports (integral to) SC-15: Collaborative Computing Devices and Applications	The PEP can enforce access decisions regarding activation of collaborative computing devices.
		Supports (integral to) SC-23: Session Authenticity	The PEP is the only component that can send and receive messages from both the data and control planes. It can protect the planes from each other and ensure that the control plane is not directly accessible by enterprise assets and resources.
		Supports (integral to) SC-32: System Partitioning	The PEP can enforce approved authorizations for controlling the flow of information within the system.
		Supports (integral to) SC-41: Port and I/O Device Access	The PEP can enforce authorizations for access to I/O ports and devices.
		Supports (integral to) SC-43: Usage Restrictions	The PEP can enforce authorization and control of usage restrictions for system components.
		Supports (example of) SI-4: System Monitoring	The PEP monitors connections between a subject and an enterprise resource to detect prohibited or suspicious activity.
Access Policies	Define the conditions that must be met to grant each subject access to each resource	Supports (integral to) AC-3: Access Enforcement	Enforcement of approved authorizations for logical access to information and system resources is accomplished in accordance with applicable access control policies.
		Supports (precedes) AC-4: Information Flow Enforcement	Access policies are the basis for enforcement of approved authorizations for controlling the flow of information

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			within the system and between connected systems.
		Supports (integral to) AC-5: Separation of Duties	Access policies are the mechanisms for ensuring that permissions and authorization to access any given resource conform with the principle of separation of duties.
		Supports (integral to) AC-6: Least Privilege	Access policies are the mechanisms for ensuring that permissions and authorization to access any given resource conform with the principle of least privilege.
		Supports (example of) AC-14: Permitted Actions Without Identification or Authentication	Access policies must identify any user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and document and provide supporting rationales for user actions not requiring identification or authentication.
		Supports (integral to) AC-20: Use of External Systems	Access policies determine what connections to external systems by each subject are authorized.
		Supports (precedes) CA-3: Information Exchange	Access policies determine approval and management of the exchange of information between the system and other systems.
		Supports (precedes) CA-9: Internal System Connections	Access policies determine which system connections are authorized.
		Supports (example of) IA-1: Policy and Procedures	Access policies enforce identification and authentication policies and their associated controls.
		Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	Access policies are the mechanisms for ensuring that subjects are authenticated commensurate with the risk of the transaction.
		Supports (integral to) IA-3: Device Identification and Authentication	Access policies derive from organizational policies and determine the requirements for identification and authentication of organization-defined device types,

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			including devices that are not owned by the organization.
		Supports (integral to) IA-4: Identifier Management	Access policies derive from organizational policies and determine how authorization is received from where/whom for assigning individual, group, role, service, or device identifiers; selecting the identifier; assigning the identifier; and preventing reuse of identifiers for a defined time period.
		Supports (integral to) IA-5: Authenticator Management	Access policies determine requirements for strength of authentication mechanisms and for authenticator management procedures.
		Supports (integral to) IA-8: Identification and Authentication (For Non-Organizational Users)	Access policies determine requirements to uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.
		Supports (integral to) IA-9: Service Identification and Authentication	Access policies determine requirements to uniquely identify and authenticate organization-defined system services and applications before establishing communications with devices, users, or other services or applications.
		Supports (precedes) SA-9: External System Services	Access policies determine organizational security and privacy requirements to be met by external systems to permit connection to their services.
Identity Management	Creates and manages enterprise user and device accounts, identity records, role information, and access attributes that form the basis of access decisions within an organization to ensure the correct subjects have the appropriate access to	Supports (integral to) AC-2: Account Management	The Identity Management function includes account management such as definition of the types of accounts allowed and specifically prohibited for use within the system, authorized users of the system, group and role membership, access authorizations (i.e., privileges), and assignment of organization-defined attributes for each account.
		Supports (integral to) AC-3: Access Enforcement	The Identity Management function enforces approved authorizations associated with logical access to information and system resources in

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	the correct resources at the appropriate time.		accordance with applicable access control policies.
		Supports (precedes) AC-4: Information Flow Enforcement	The Identity Management function is a necessary component of access authorizations on which information flow enforcement depends.
		Supports (integral to) AC-5: Separation of Duties	Identity Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of separation of duties, and it is used to assign users to roles that best match their responsibilities, based on the principle of separation of duties, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
		Supports (integral to) AC-6: Least Privilege	Identity Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of least privilege, and it is used to assign users to roles that best match their responsibilities, based on the principle of least privilege, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
		Supports (integral to) AC-17: Remote Access, including enhancement #1	The Identity Management function authorizes each type of remote access to the system prior to allowing such connections.
		Supports (integral to) AC-24: Access Control Decisions	The Identity Management function is a mechanism for ensuring that organization-defined access control decisions are applied to access requests prior to access enforcement.
		Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	The Identity Management function is necessary for unique identification and authentication of organizational users.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) IA-5: Authentication Management	The Identity Management function permits verification, as part of the initial authenticator distribution, of the identity of the individual receiving the authenticator.
		Supports (integral to) IA-8: Identification and Authentication (Non-organizational Users)	The Identity Management function is necessary for unique identification and authentication of non-organizational users.
		Supports (integral to) PE-2: Physical Access Authorizations	The Identity Management function is the basis for authorization of credentials for facility access, including physical access to security-critical devices.
Access & Credential Management	Manages access to resources by performing user and device authentication (e.g., SSO and MFA) and using identity, role, and access attributes to determine which access requests are authorized.	Supports (integral to) AC-2: Account Management	The Access and Credential Management function includes account management such as definition of the types of accounts allowed and specifically prohibited for use within the system, authorized users of the system, group and role membership, access authorizations (i.e., privileges), and assignment of organization-defined attributes for each account by performing user authentication.
		Supports (integral to) AC-3: Access Enforcement	The Access and Credential Management function enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
		Supports (precedes) AC-4: Information Flow Enforcement	The Access and Credential Management function is a necessary component of access authorizations on which information flow enforcement depends.
		Supports (integral to) AC-5: Separation of Duties	Access and Credential Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of separation of duties, and it is used to assign users to roles that best match their responsibilities, based on the principle of separation of duties, and to manage each user's roles as their

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			responsibilities in the enterprise change, or as they leave employment.
		Supports (integral to) AC-6: Least Privilege	Access and Credential Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of least privilege, and it is used to assign users to roles that best match their responsibilities, based on the principle of least privilege, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
		Supports (integral to) AC-24: Access Control Decisions	The Access and Credential Management function is a mechanism for ensuring that organization-defined access control decisions are applied to access requests prior to access enforcement using authentication.
		Supports (integral to) IA-1: Policy and Procedures	The Access and Credential Management function is integral to implementation of the organization's identification and authentication policies and procedures.
		Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	Access and Credential Management is a necessary element of uniquely identifying and authenticating organizational users. To determine whether an access is authorized, the Access and Credential Management component authenticates the user or device that is requesting access by verifying the credentials that are bound to the user or device and asserted as part of the access request. These credentials must be asserted for this IDAM component to be able to authenticate the user request.
		Supports (precedes) IA-3: Device Identification and Authentication	The Access and Credential Management function is prerequisite to uniquely identifying and authenticating organization-defined devices and/or types of devices before establishing a local, remote, or network connection.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) IA-5: Authentication Management	The Access and Credential Management function permits verification, as part of the initial authenticator distribution, of the identity of the individual receiving the authenticator.
		Supports (integral to) IA-8: Identification and Authentication (Non-Organizational Users)	The Access and Credential Management function is necessary for unique identification and authentication of non-organizational users.
		Supports (integral to) IA-9: Service Identification and Authentication	The Access and Credential Management function is necessary for authorization of user/system connections to services employing identification and authentication mechanisms.
		Supports (example of) IR-4: Incident Handling	If a legitimate user's credentials are stolen and an attacker uses them to gain unauthorized access to a resource, the Access and Credential Management component will limit the attacker to accessing only those resources that the legitimate user's role allows.
Federated Identity	Aggregates and correlates all attributes relating to an identity or object that is being authorized by a ZTA. It enables users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Federated identity encompasses the traditional ICAM data, supports identities that may	Supports (example of) IA-5: Authentication Management	An extension of IA-5 (9) requires acceptance and verification of federated or PKI credentials.
		Supports (example of) IA-8: Identification and Authentication (Non-Organizational Users)	Extensions of IA-8 (5 and 6) require acceptance and verification of federated or PKI credentials.
		Supports (example of) IA-12: Identity Proofing	An extension of IA-12 (6) calls for accepting externally proofed identities, a fundamental component of managing federated identities across agencies and organizations.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	be part of a larger federated ICAM community, and may include non-enterprise employees.		
Identity Governance	Provides policy-based, centralized, automated processes to manage user identity and access control functions (e.g., ensuring segregation of duties, role management, logging, auditing, access reviews, analytics, and reporting) to ensure compliance with requirements and regulations.	Supports (integral to) AC-2: Account Management	The Identity Governance function includes account management such as authorized users of the system, access authorizations (i.e., privileges), and assignment of organization-defined attributes.
		Supports (integral to) AC-3: Access Enforcement	The Identity Governance function enforces approved authorizations for logical access to information and system resources by identified users in accordance with applicable access control policies.
		Supports (precedes) AC-4: Information Flow Enforcement	The Identity Governance function is a necessary component of the identity component of access authorizations on which information flow enforcement depends.
		Supports (integral to) AC-5: Separation of Duties	The Identity Governance component can manage access permissions and authorizations in a way that incorporates the separation of duties principle.
		Supports (integral to) AC-6: Least Privilege	The Identity Governance component can manage access permissions and authorizations in a way that incorporates the least privilege principle.
		Supports (integral to) AC-24: Access Control Decisions	The Identity Governance function is a mechanism for ensuring that organization-defined access control decisions are applied to access requests prior to access enforcement and that organization-defined access control decisions are applied to access requests prior to access enforcement using authentication.
		Supports (integral to) AU-2: Event Logging	The Identity Governance component logs all identity management activities in accordance with policy and regulations.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) AU-12: Audit Record Generation	The Identity Governance component audits all identity management activities in accordance with policy and regulations.
Unified Endpoint Management (UEM)/Mobile Device Management (MDM)	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities and threats; monitor for suspicious activity to prevent and detect intrusions; prevent, detect, and disable malware, viruses, and other malicious or unauthorized traffic; repair infected files when possible; provide alerts and recommend remediation actions; and encrypt data.	Supports (integral to) AC-1: Policy and Procedures	UEM/MDM devices enforce access control policies and procedures and associated access controls.
		Supports (integral to) AC-2: Account Management	The UEM/MDM can monitor the use of accounts user activity for prohibited use.
		Supports (integral to) AC-6: Least Privilege	The UEM/MDM can be used to configure devices to provide only essential capabilities.
		Supports (integral to) AC-17: Remote Access	The UEM/MDM enforces usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorizes each type of remote access to the system prior to allowing such connections. May use encrypted VPNs to enhance confidentiality and integrity for remote connections.
		Supports (integral to) AC-18: Access Control for Wireless Access	The UEM/MDM enforces configuration requirements, connection requirements, and implementation guidance for each type of wireless access and authorizes each type of wireless access to the system prior to allowing such connections. An AC-18 extension (1) requires protection of wireless access to the system using authentication of users and devices and encryption.
	Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data	Supports (integral to) AC-19: Access Control for Mobile Devices	The UDM/MDM enforces configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas and authorizes the connection of mobile devices to organizational systems.
		Supports (integral to) AC-20: Use of External Systems	The UDM/MDM enforces organization-defined controls asserted to be implemented on external systems

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
	from devices if needed, tracks user activity on devices, and detects and addresses security issues on the device.		consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing only authorized individuals to access the system from external systems and processing, storing, or transmitting organization-controlled information using external systems.
		Supports (integral to) CA-7: Least Functionality	The UEM/MDM enforces configuration of the system to provide only organization-defined mission essential capabilities. The UEM/MDM can monitor user activity.
		Supports (integral to) CM-2: Baseline Configuration	The UEM/MDM ensures that the devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software and firmware.
		Supports (integral to) CM-4: Impact Analysis	The UEM/MDM ensures that the devices are compliant with organizational policy regarding analysis of changes to the system to determine potential security and privacy impacts prior to change implementation.
		Supports (integral to) CM-5: Access Restrictions for Change	The UEM/MDM enforces physical and logical access restrictions associated with changes to the system.
		Supports (integral to) CM-6: Configuration Settings	The UEM/MDM enforces configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organization-defined common secure configurations and implements the configuration settings.
		Supports (integral to) CM-10: Software Usage Restrictions	The UEM/MDM can monitor user activity for violation of usage restrictions.
		Supports (example of) CM-11: User Installed Software	The UEM/MDM can monitor user activity to enforce software installation policies.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (example of) CM-14: Signed Components	The UEM/MDM may use integrity checking to verify updates prior to installing them. It may also use integrity checking to verify compliance of device software and firmware.
		Supports (integral to) IR-4: Incident Handling	The UEM/MDM performs many activities that help to contain and mitigate incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.
		Supports (example of) MP-6: Media Sanitization	The UEM/MDM can remotely delete applications and data from devices as needed according to policy (not complete sanitization).
		Supports (example of) MP-7: Media Use	The UEM/MDM can restrict the use of removable media as required by policy.
		Supports (integral to) PM-5: System Inventory	The UEM/MDM installs, manages, configures, and updates applications on UEM/MDM managed devices, so it provides inventory information regarding these applications.
		Supports (example of) RA-3: Risk Assessment	The UEM/MDM may be able to identify device vulnerabilities by updating software, for example. The UEM/MDM may monitor for suspicious activity; detect and disable malware, viruses, and other malicious traffic; and repair infected files. The UEM/MDM can mitigate and remediate vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) RA-5: Vulnerability Monitoring and Scanning	The UEM/MDM can monitor device software, firmware, and configurations for vulnerabilities and threats.
		Supports (integral to) SA-18: Mobile Code	The UEM/MDM may be able to detect unauthorized mobile code.
		Supports (example of) SC-3: Security Function Isolation	The UEM/MDM can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities.
		Supports (example of) SC-8: Transmission Confidentiality and Integrity	The UEM/MDM can provide cryptographic protection for transmitted information.
		Supports (integral to) SC-13: Cryptographic Protection	The UEM/MDM may provide cryptographic protection to support a variety of security solutions.
		Supports (example of) SC-28: Protection of Data at Rest	The UEM/MDM can provide cryptographic protection for data that is stored onsite.
		Supports (integral to) SI-2: Flaw Remediation	The UEM/MDM mitigates and remediates vulnerabilities that it detects in device software, firmware, and configuration.
		Supports (integral to) SI-3: Malicious Code Protection	The UEM/MDM prevents, detects, and disables malware, viruses, and other malicious traffic. It also repairs infected files when possible. When malicious code is detected, it provides alerts and may recommend remediation action.
		Supports (integral to) SI-4: System Monitoring	The UEM/MDM monitors the device for unauthorized software and connections. The UEM/MDM monitors the system to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives and unauthorized local, network, and remote connections to identify unauthorized use of the system.
Endpoint Detection and Response	Detects and stops threats to endpoints	Supports (integral to) AC-2: Account Management	The EDR/EPP can monitor the use of accounts.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
(EDR)/ Endpoint Protection Platform (EPP)	through an integrated suite of endpoint protection technologies including antivirus, data encryption, intrusion prevention, EDR, and data loss prevention (DLP). May include mechanisms that are designed to protect applications and data; ensure device compliance with policies regarding hardware, firmware, software, and configuration; monitor endpoints for vulnerabilities, suspicious activity, intrusion, infection, and malware; block unauthorized traffic; disable malware and repair infections; manage and administer software and updates; monitor behavior and critical data; and enable endpoints to be tracked, troubleshooted, and wiped, if necessary.	Supports (integral to) AC-4: Information Flow Enforcement	The EDR/EPP may include a firewall that blocks unauthorized connections to and from the device.
		Supports (integral to) AC-17: Remote Access	The EDR/EPP may include a firewall that blocks unauthorized connections to and from the device.
		Supports (integral to) AC-19: Access Control for Mobile Devices	The EDR/EPP may include a firewall that blocks unauthorized connections to and from the device.
		Supports (integral to) AC-20: Use of External Systems	The EDR/EPP may include a firewall that blocks unauthorized connections to and from the device.
		Supports (integral to) CA-7: Continuous Monitoring	The EDR/EPP scans the device to detect missing patches or outdated software and report them.
		Supports (integral to) CM-2: Baseline Configuration	The EDR/EPP ensures that the devices are compliant with organizational policy in terms of having the expected baseline installation and configuration of software. It is a prerequisite that the compliance policies incorporate appropriate security principles.
		Supports (integral to) CM-7: Least Functionality	The EDR/EPP can be used to configure devices to provide only essential capabilities.
		Supports (integral to) CM-8: System Component Inventory	For a device to have EDR/EPP software installed on it, the device must be known to be part of the organization's inventory.
		Supports (integral to) IR-4: Incident Handling	The EDR/EPP performs many activities that help to contain incidents, such as detecting and disabling malware, viruses, and other malicious or unauthorized traffic; repairing infected files when possible; and providing alerts and recommending remediation actions when suspicious activity or malicious activity is detected on a device. It also encrypts data stored on the device, which limits the data's usefulness if it is exfiltrated.
		Supports (example of) MP-2: Media Access	The EDR/EPP can restrict the use of removable media as required by policy.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (example of) MP-6: Media Sanitization	The EDR/EPP can remotely delete applications and data from devices as needed according to policy (not full sanitization).
		Supports (example of) MP-7: Media Use	The EDR/EPP can restrict the use of organization-defined types of system media on organization-defined systems or system.
		Supports (example of) PM-5: System Inventory	The EDR/EPP can inventory software on the device.
		Supports (integral to) RA-3: Risk Assessment	The EDR/EPP supports Identification of threats to and vulnerabilities in the system by scanning the device to detect missing patches or outdated software and reporting them. The EDR/EPP also detects malware, viruses, and other signature-based threats.
		Supports (integral to) SC-7: Boundary Protection	The EDR/EPP may include a firewall that blocks unauthorized traffic to and from the device.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The EDR/EPP may encrypt data sent from the device and may include a firewall that blocks unauthorized traffic to and from the device.
		Supports (example of) SC-10: Software Usage Restrictions	The EDR/EPP can monitor user activity to enforce usage restrictions.
		Supports (example of) SC-11: User-Installed Software	The EDR/EPP can monitor activity to enforce software installation policies.
		Supports (integral to) SC-13: Cryptographic Protection	The EDR/EPP may encrypt data sent from the device or stored on the device.
		Supports (integral to) SC-15: Collaborative Computing Devices and Applications	The EDR/EPP may include a firewall that blocks unauthorized remote activation of collaborative computing devices and applications.
		Supports (integral to) SC-18: Mobile Code	The EDR/EPP may be able to detect unauthorized mobile code.
		Supports (integral to) SC-28: Protection of Information at Rest	The EDR/EPP may encrypt data stored on the device.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (example of) SI-2: Flaw Remediation	The EDR/EPP can mitigate and remediate vulnerabilities and threats that it detects in device software, firmware, and configuration by enforcing the organization's vulnerability management policies.
		Supports (integral to) SI-3: Malicious Code Protection	The EDR/EPP detects and disable malware, viruses, and other signature-based threats.
		Supports (integral to) SI-4: System Monitoring	The EDR/EPP monitors the device for unauthorized software and connections.
		Supports (example of) SI-7: Software, Firmware, and Information Integrity	The EDR/EPP may use integrity checking to verify updates prior to installing them. It may also use integrity checking to verify compliance of device software and firmware.
Security Information and Event Management (SIEM)	Collects and consolidates security information and security event data from many sources; correlates and analyzes the data to help detect anomalies and recognize potential threats and vulnerabilities; and logs the data to adhere to data compliance requirements.	Supports (integral to) AU-2: Event Logging	The SIEM logs security information and event activity as required by policy.
		Supports (integral to) AU-6: Audit Record Review, Analysis, and Reporting	The SIEM collects security and event information from many components. This data may be analyzed to understand attack targets and methods. Security analysts rely at least in part on SIEM data to help them determine the impact of events.
		Supports (example of) AU-7: Audit Record Reduction and Report Generation	The SIEM logs can provide helpful data that can help with forensic analysis of cybersecurity incidents.
		Supports (integral to) CA-7: Continuous Monitoring	The SIEM collects security and event information from many components.
		Supports (integral to) IR-4: Incident Handling	The SIEM collects security and event information from many components. This data may be analyzed to understand attack targets and methods and the impact of cybersecurity incidents.
		Supports (integral to) IR-5: Incident Monitoring	The SIEM collects security and event information from many components to support tracking and documentation of events. The SIEM logs can be examined as an indirect and non-real-time method of

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
			monitoring network activity to detect anomalous behavior and other indicators of potential cybersecurity events.
		Supports (integral to) RA-3: Risk Assessment	Security analysts rely at least in part on SIEM data to help them determine the impact of events.
		Supports (integral to) RA-5: Vulnerability Monitoring and Scanning	The SIEM acts as a vulnerability scanning and assessment tool.
		Supports (integral to) SC-7: Boundary Protection	The SIEM collects and correlates event information. The SIEM logs can be examined as an indirect and non-real-time method of monitoring network activity to detect anomalous behavior and other indicators of potential cybersecurity events.
Virtual Private Network (VPN)	Enables authorized remote users to securely access the inside of the enterprise. (Once inside, the ZTA manages the user's access to resources.)	Supports (integral to) AC-17: Remote Access	Requiring remote users to access the enterprise via VPN is one mechanism that helps manage remote access.
		Supports (integral to) AC-20: Use of External Systems	Limiting external users to access the enterprise via VPN is one mechanism that helps manage remote access.
		Supports (example of) CA-7: Continuous Monitoring	Traffic sent on the VPN can be monitored to detect prohibited or suspicious activity.
		Supports (example of) SC-8: Transmission Confidentiality and Integrity	VPNs encrypt data in transit.
		Supports (integral to) SC-13: Cryptographic Protection	VPNs encrypt data in transit.
Certificate Management	Provides automated capabilities to issue, install, inspect, revoke, renew, and otherwise manage TLS certificates.	Supports (integral to) AC-16: Security and Privacy Attributes	Proofing server identities requires TLS certificates.
		Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	Verification of the identity of servers depends on the issuance, use, and management of TLS certificates.

ZTA Project Component	ZTA Project Function	Function's Relationships with SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The setup of encrypted TLS transport connections depends on TLS certificates.
		Supports (integral to) SC-16: Transmission of Security and Privacy Attributes	TLS transport connections provide integrity checking on their traffic, and the setup of TLS connections depends on TLS certificates.
		Supports (integral to) SI-7: Software, Firmware, and Information Integrity	TLS transport connections provide integrity checking on their traffic, and the setup of TLS connections depends on TLS certificates.

3.5.1 Mapping between E1B1 and NIST SP 800-53 Controls

This mapping will be provided in a future version of this document.

3.5.2 Mapping between E2B1 and NIST SP 800-53 Controls

This mapping will be provided in a future version of this document.

3.5.3 Mapping between E3B1 and NIST SP 800-53 Controls

This mapping will be provided in a future version of this document.

3.5.4 Mapping between E1B2 and NIST SP 800-53 Controls

This mapping will be provided in a future version of this document.

3.5.5 Mapping between E3B2 and NIST SP 800-53 Controls

This mapping will be provided in a future version of this document.

3.6 Mapping Between ZTA Functions and EO 14028 Security Measures

In Table 3-3 we provide a mapping between the logical components of the ZTA reference design and the EO 14028 security measures. This table indicates how ZTA functions help support EO 14028 security measures for EO-critical software and EO-critical software platforms, and vice versa.

Table 3-3 Mapping between ZTA Reference Design Logical Components and EO 14028 Security Measures

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Policy Engine (PE)	Decides whether to grant, deny, or revoke access to a resource, based on enterprise policy, information from functional components, and a trust algorithm	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	The PE makes access decisions based on policy.
		Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	The PE makes access decisions based on policy.
Policy Administrator (PA)	Executes the PE's policy decision by sending commands to a PEP that establishes and shuts down the communication path between subject and resource	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	The PA supports the enforcement of access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.
		Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least	The PA supports the enforcement of access decisions by conveying the access decision information from the PE to the PEP, where the decision can be enforced.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		privilege to the extent possible.	
Policy Enforcement Point (PEP)	Guards the trust zone that hosts an enterprise resource; enables, monitors, and terminates the connection between subject and resource; forwards requests to and receives commands from the PA	Supports (integral to) SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data.	The PEP prevents unauthorized access to the portions of the enterprise that it guards.
		Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	The PEP enforces access decisions. The PEP can be placed in front of a single or multiple resources, making access control as fine-grained as desired.
		Supports (example of) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	The PEP can monitor connections between a subject and an EO-critical software platform to detect prohibited or suspicious activity.
Access Policies	Define the conditions that must be met to grant each subject access to each resource	Is supported by (precedes) SM 2.1: Establish and maintain a data inventory for EO-critical software and EO-critical platforms.	In order to properly formulate policy regarding each subject's access to data, the data for EO-critical software and EO-critical platforms must be catalogued.
		Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by	Access policies are the mechanisms for ensuring that permissions and authorization to access any given data and

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
		EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	resource conform with the principle of least privilege.
		Is supported by (precedes) SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	In order to properly formulate policy regarding each subject's access to resources, the software resources deployed to each platform running EO-critical software must be catalogued.
Identity Management	Creates and manages enterprise user and device accounts, identity records, role information, and access attributes that form the basis of access decisions within an organization to ensure the correct subjects have the appropriate access to the correct resources at the appropriate time.	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	Identity Management is used to create and manage the identities that are verified using multi-factor authentication.
		Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	Identity Management is used to define and manage digital representations of roles and associated access authorizations that are based on the principle of least privilege, and to manage each user's roles as their responsibilities in the enterprise change, or as they leave employment.
Access & Credential Management	Manages access to resources by performing user and device authentication (e.g., SSO and MFA) and using identity, role,	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and	Access & Credential Management is used to perform multi-factor authentication.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	and access attributes to determine which access requests are authorized.	EO-critical software platforms.	
		Supports (integral to) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	Performing user and device authentication is necessary for mutual authentication.
Federated Identity	Aggregates and correlates all attributes relating to an identity or object that is being authorized by a ZTA. It enables users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Federated identity encompasses the traditional ICAM data, supports identities that may be part of a larger federated ICAM community, and may	Supports (example of) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	Federated identities can be verified using multi-factor authentication.
		Supports (example of) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	Federated identities can be used with digital representations of roles and associated access authorizations.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	include non-enterprise employees.		
Identity Governance	Provides policy-based, centralized, automated processes to manage user identity and access control functions (e.g., ensuring segregation of duties, role management, logging, auditing, access reviews, analytics, and reporting) to ensure compliance with requirements and regulations.	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	The Identity Governance component manages user identity functions.
		Supports (integral to) SM 2.2: Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	The Identity Governance component manages access control functions.
		Supports (integral to) SM 4.1: Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	The Identity Governance component performs logging and audits all identity management activities in accordance with policy and regulations.
MFA	Authenticates user identity by requiring the user to provide not only something they know (e.g., a password), but also something they have (e.g., a token).	Supports (integral to) SM 1.1: Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	The MFA component enables users to be authenticated using a second factor.
Unified Endpoint		Supports (example of) SM 2.3: Protect data at	The UEM/MDM may encrypt data stored on the device, but data stored on the

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Management (UEM)/Mobile Device Management (MDM)	Manages and secures enterprise desktop computers, laptops, and/or mobile devices in accordance with enterprise policy to protect applications and data; ensure device compliance; mitigate and remediate vulnerabilities and threats; monitor for suspicious activity to prevent and detect intrusions; prevent, detect, and disable malware, viruses, and other malicious or unauthorized traffic; repair infected files when possible; provide alerts and recommend remediation actions; and encrypt data. Pushes enterprise applications and updates to devices, enables users to download enterprise applications that they are authorized to access, remotely deletes all applications and data from devices if needed, tracks user activity on devices, and detects and	rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	device could also be encrypted via a different mechanism.
		Supports (integral to) SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	The UEM/MDM installs, manages, configures, and updates software on UEM/MDM-managed devices, so it provides inventory information regarding this software.
		Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	The UEM/MDM installs, manages, configures, and updates software on UEM/MDM-managed devices.
		Supports (integral to) SM 4.1: Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	The UEM/MDM component performs security event logging on UEM/MDM-managed devices.
		Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	The UEM/MDM component provides several forms of endpoint security protection on UEM/MDM-managed devices.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	addresses security issues on the device.		
Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP)	Detects and stops threats to endpoints through an integrated suite of endpoint protection technologies including antivirus, data encryption, intrusion prevention, EDR, and data loss prevention (DLP). May include mechanisms that are designed to protect applications and data; ensure device compliance with policies regarding hardware, firmware, software, and configuration; monitor endpoints for vulnerabilities, suspicious activity, intrusion, infection, and malware; block unauthorized traffic; disable malware and repair infections; manage and administer software and updates; monitor behavior	Supports (example of) SM 2.3: Protect data at rest by encrypting the sensitive data used by EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	The EDR/EPP may encrypt data stored on the device, but data stored on the device could also be encrypted via a different mechanism.
		Supports (integral to) SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	The EDR/EPP inventories software on the device.
		Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	The EDR/EPP installs, manages, configures, and updates software on EDR/EPP-managed devices.
		Supports (integral to) SM 3.3: Use configuration management practices to maintain EO-critical software platforms and all software deployed to those platforms.	The EDR/EPP ensures that devices are compliant with organizational policy in terms of having the expected software configurations.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	and critical data; and enable endpoints to be tracked, troubleshooted, and wiped, if necessary.	Supports (integral to) SM 4.3: Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.	The EDR/EPP provides several forms of endpoint security protection on EDR/EPP-managed devices.
		Supports (example of) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	The EDR/EPP can monitor the device for unauthorized network connections. Other network monitoring technologies can be used instead of EDR/EPP to do this.
Security Information and Event Management (SIEM)	Collects and consolidates security information and security event data from many sources; correlates and analyzes the data to help detect anomalies and recognize potential threats and vulnerabilities; and logs the data to adhere to data compliance requirements.	Is supported by (precedes) SM 4.1: Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	The SIEM aggregates logs of security information and security event activity generated by EO-critical software platforms.
		Supports (example of) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	The SIEM can collect, analyze, and correlate security information and security event data from many platforms.
Vulnerability Scanning and Assessment	Scans and assesses the enterprise infrastructure and resources for security risks; identifies vulnerabilities and	Supports (integral to) SM 3.2: Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms.	A key function of the Vulnerability Scanning and Assessment component is to perform vulnerability scans for missing patches.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
	misconfigurations; and provides remediation guidance regarding investigating and prioritizing responses to incidents.	Supports (integral to) SM 3.3: Use configuration management practices to maintain EO-critical software platforms and all software deployed to those platforms.	A key function of the Vulnerability Scanning and Assessment component is to perform vulnerability scans for misconfigurations.
Security Integration Platform	Integrates the SIEM and other security tools into a single pane of glass to support generation of insights into threats and help track, manage, and resolve cybersecurity incidents. Executes predefined incident response workflows to automatically analyze information and orchestrate the operations required to respond.	Supports (example of) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	The Security Integration Platform component can support monitoring of security data from many platforms.
Security Validation	Continuously monitor, measure, and validate the effectiveness of the ZTA's cybersecurity controls	Supports (integral to) SM 4.2: Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	The ZTA's cybersecurity controls are a subset of the EO-critical software platforms' controls, so continuous monitoring of the ZTA's cybersecurity controls achieves a part of continuous monitoring for EO-critical software platforms.
Network Discovery	Discovers, classifies, and assesses the risk posed by devices and users on the network.	Supports (integral to) SM 4.4: Employ network security protection to monitor the network traffic to and from EO-critical software platforms to protect the platforms and their software using networks.	Discovering, classifying, and assessing the risk posed by devices on the network is vital for monitoring and analyzing network traffic to and from devices.

ZTA Logical Architecture Component	ZTA Component's Function	Function's Relationships to EO 14028 Security Measures (and Relationship Properties)	Relationship Explanation
Virtual Private Network	Enables authorized remote users to securely access the inside of the enterprise. (Once inside, the ZTA manages the user's access to resources.)	Supports (example of) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	VPNs are one method of encrypting data in transit.
Certificate Management	Provides automated capabilities to issue, install, inspect, revoke, renew, and otherwise manage TLS certificates.	Supports (example of) SM 1.2: Uniquely identify and authenticate each service attempting to access EO-critical software or EO-critical software platforms.	Services can be identified and authenticated through the use of TLS certificates.
		Supports (integral to) SM 2.4: Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications for EO-critical software and EO-critical software platforms consistent with NIST's cryptographic standards.	TLS certificates are widely used for mutual authentication and communications encryption—for example, in HTTPS.

3.6.1 Mapping between E1B1 and the EO 14028 Security Measures

This mapping will be provided in a future version of this document.

3.6.2 Mapping between E2B1 and the EO 14028 Security Measures

This mapping will be provided in a future version of this document.

3.6.3 Mapping between E3B1 and the EO 14028 Security Measures

This mapping will be provided in a future version of this document.

3.6.4 Mapping between E1B2 and the EO 14028 Security Measures

This mapping will be provided in a future version of this document.

3.6.5 Mapping between E3B2 and the EO 14028 Security Measures

This mapping will be provided in a future version of this document.

Appendix A References

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Gaithersburg, Md., August 2020, 50 pp. Available: https://csrc.nist.gov/publications/detail/sp/800-207/final

[2] S. Rose, Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators, National Institute of Standards and Technology (NIST) Cybersecurity White Paper (CSWP) 20, Gaithersburg, Md., May 2022, 14 pp. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.20.pdf

[3] NIST. *Cybersecurity Framework*. Available: https://www.nist.gov/cyberframework/

[4] Joint Task Force, Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Gaithersburg, Md., September 2020, 465 pp. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[5] Executive Order no. 14028, *Improving the Nation's Cybersecurity*, Federal Register Vol. 86, No.93, May 17, 2021. Available: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[6] Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028, National Institute of Standards and Technology (NIST). Available: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2