Advancing Zero Trust Maturity Throughout the User Pillar

Executive Summary

According to the 2020 Verizon Data Breach Investigations Report, over 80% of breaches due to hacking involved credentials, whether lost or stolen, to impersonate users for further compromise[1].[1] Such cyber incidents are on the rise, creating economic disruption and impacting national security.

This cybersecurity information sheet (CSI) provides recommendations for maturing identity, credential and access management (ICAM) capabilities to effectively mitigate such cyberattacks. It further discusses how these capabilities integrate into a comprehensive Zero Trust (ZT) framework, as described in Embracing a Zero Trust Security Model. [2] National Security System owners and operators should take concrete steps to mature identity and access security controls and the operational practices related to establishing digital identities and authenticating and authorizing users to access critical resources. Doing so will provide system owners and operators the ability to identify, resist, and respond to many cyber intrusion techniques.

Adoption of ZT principles is not accomplished overnight. Implementation is achieved through careful and deliberate planning and continuous incremental improvements. Building capabilities aligned to a mature ZT framework requires integrating every system in the enterprise with the controls defined for each of seven pillars – User, Device, Data, Application/Workload, Network/Environment, Visibility & Analytics, and Automation & Orchestration, starting with the user pillar, which builds on existing ICAM capabilities.

[1] Version 1.1 corrects the quote to data directly from Verizon's 2020 Data Breach Investigations Report instead of the version 1.0 quote that was from GovTech.com's discussion on Verizon's 2020 report.

Introduction

Cybersecurity incidents leveraging gaps, or immature capabilities in identity, credential, and access management (ICAM) of national security, critical infrastructure, and defense industrial base systems are on the rise, impacting national security. In June 2015, the United States Office of Personnel Management (OPM) suffered a data breach of personnel records, including users with access to the nation's most critical systems. The breach occurred by leveraging compromised credentials. The agency had multifactor authentication in place, but it was not fully implemented until it was too late to prevent the earlier initial breach. On May 6, 2021, Colonial Pipeline, a major Southeast oil pipeline system, suffered a major ransomware cyberattack that caused financial and supply chain havoc across the United States, impacting economic stability. The attack exploited a legacy Virtual Private Network (VPN) system without multifactor authentication in place. Attackers were able to gain access into the system by compromising a complex password. These are just two of the many examples of publicly known cybersecurity incidents that exploit immature ICAM capabilities that are covered by the user pillar of the ZT framework. With similar exploits on the rise, it is crucial for organizations to adopt a mature Zero Trust (ZT) approach to defend critical national security systems (NSS) and other United States Government (USG) and private sector critical IT resources. [2] [3] [4] [5]

This CSI details increasingly mature capabilities in the user pillar, including recommendations and examples for achieving these maturity levels. The user (or identity) pillar highlights capabilities to establish the foundational authoritative identities of a system. Further, it describes the characteristics of authentication and authorization decisions. The user pillar maturity model builds on and matures the controls of the Federal Identity, Credential, and Access Management (FICAM) architecture. FICAM establishes five core user service practice areas: Identity Management, Credential Management, Access Management, Federation and Governance. [6] FICAM is the federal government's enterprise approach to design, plan, and execute common Identity, Credential, and Access Management (ICAM) processes. The FICAM framework was established in 2009 to provide a common ICAM segment architecture for federal agencies to use in ICAM program and solution roadmap planning. The FICAM capabilities, expanded and refined by ZT principles, create a solid foundation for NSS owners and operators alike. They outline ways to take concrete steps to mature ZT security practices relating to identity management, access security controls, and the

operational practices related to establishing identities for users and strong mechanisms for authenticating and authorizing users' access to critical resources.

Audience

This CSI provides guidance primarily intended for NSS owners and operators, but may be useful for owners and operators of other systems that might be targeted by sophisticated malicious actors. Guidance for other system owners and operators is also available via National Institute of Standards and Technology (NIST), [3] and Cybersecurity and Infrastructure Security Agency (CISA). [4] This guidance is compatible with Department of Defense (DoD) Zero Trust guidance [5] referenced at the end of this document.

Background

The President's Executive Order on Improving the Nation's Cybersecurity (EO 14028) and National Security Memorandum 8 (NSM-8) direct the Federal Civilian Executive Branch (FCEB) agencies and NSS owners and operators to develop plans to adopt a ZT cybersecurity framework. [7] [8]

In the NSA cybersecurity information sheet (CSI) Embracing a Zero Trust Security Model, the concept of ZT is defined and its seven pillars are identified. ZT implementation efforts are intended to continually mature cybersecurity protections, responses, and operations over time. Progression of capabilities in each of the seven pillars should be seen as a cycle of continuous improvement based on evaluation and monitoring of threats. [2]

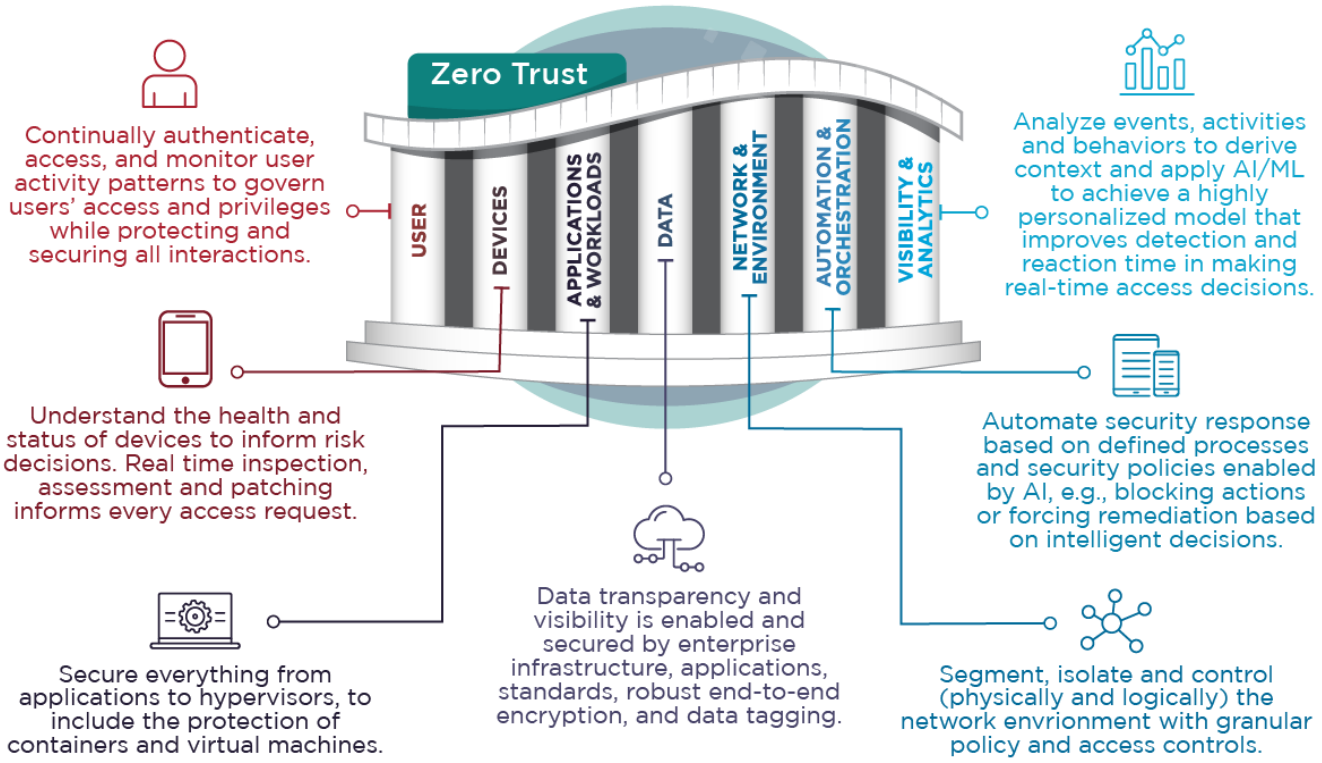

Figure 1: Description of the seven (7) pillars of Zero Trust

Figure 1 depicts the ZT pillars, including the user pillar. The capabilities and milestones for the user pillar component of the ZT maturity model will be described in detail throughout this document. The pillars are not independent; many capabilities in the user pillar depend on, or align with capabilities in other pillars as indicated.

The user pillar, which focuses on managing user access in a dynamic risk environment, depends on capabilities that will be the focus of other pillars. Based on the needed decision making speed and the amount of information that must be monitored, automation (part of the automation and orchestration pillar) may be necessary for a mature implementation. Continuous auditing (part of the visibility and analytics pillar) provides accountability for accesses, and can be used to analyze risk associate with a particular request. Network, data, and application segregation (part of the network/environment, data, and workstation applications pillar) impact the credentials associated with user accesses, and risk-based access controls also depend on the capabilities of different devices (part of the device pillar).

User Pillar

The user pillar expands and refines the capabilities associated with FICAM framework to address the enhanced threat to identity, credentials, and access management. This CSI identifies these capabilities and aligns them to Zero Trust maturity levels for the user pillar. The FICAM Framework and user pillar capabilities include:

- **Identity Management**: technical systems, policies, and processes that create, define, govern, and synchronize the ownership, utilization, and safeguarding of identity information to associate digital identities to an individual or logical entity.
- **Credential management**: technical systems, policies, and processes that establish and maintain a binding of an identity to an individual, physical, or logical entity, to include establishing the need for a credential, enrolling an entity, establishing and issuing the credential, and maintaining the credential throughout its life cycle.
- **Access Management:** management and control of the mechanisms used to grant or deny entities access to resources, including assurances that entities are properly validated, that entities are authorized to access the resources, that resources are protected from unauthorized creation, modification, or deletion, and that authorized entities are accountable for their activity.
- **Federation**: interoperability of ICAM with mission partners. This CSI only discusses the general complexity of identity federation.
- **Governance**: continuous improvement of systems and processes to assess and reduce risk associated with ICAM capabilities. This CSI addresses improvements for this category by defining maturity levels for each of the ICAM categories rather than discussing maturity of identity governance in general.

These capabilities provide a starting point for a user pillar maturity model. A generic assessment of current capabilities for NSS and employee access to U.S. Government systems in these areas is included in the ZT preparation phase. These foundational capabilities are recommended for other high value systems in preparation for their ZT migration. As additional capabilities are deployed, enterprises advance through the

basic, intermediate, and advanced maturity phases and are more able to operate according to ZT principles.

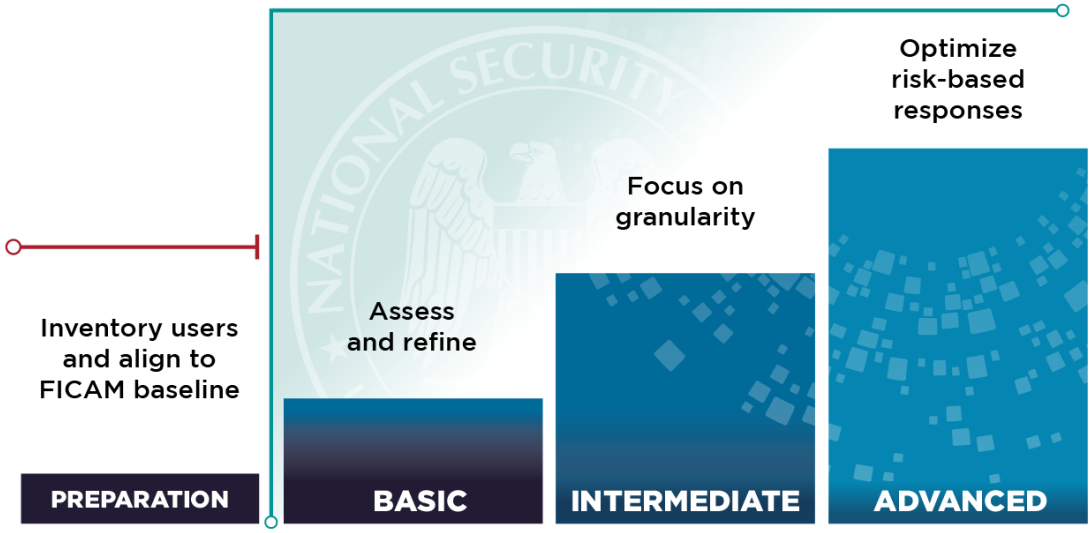

Figure 2: Zero Trust user pillar maturity

Identity Management

Identity management includes the processes and procedures to collect, verify, and manage attributes to establish and maintain enterprise identities for users. Robust identity management requires a comprehensive approach for proving that people and systems are who they say they are. This means establishing authoritative processes and sources for digital identities (and associated attributes) to verify a user's identity. Identity management encompasses the human resources, security, and technical systems and processes used to establish authoritative identities. Identity management begins with establishing a current and accurate inventory of all users, including person and non-person entities, ensuring those with access to critical resources are vetted and registered. The inventory includes identity attributes required by FICAM identity governance practices.

Identity Management Capabilities

- **Inventory users (including privileged users)** – Identify all users with access to critical resources and review their privileges. Reduce the risk of untrusted users with access to resources by removing users who no longer have a need for access.

- **Utilize standard, centralized identity stores** – Only use trusted, standardized inventories. Make them centrally accessible and usable so unsynchronized, out-of-date, or contradictory identity information is not used.

Maturity phases

- **Preparation for ZT**: FICAM requirements focus on person-entities. Enterprise repositories maintain entities for individuals. Enterprise identity vetting for persons and non-person entities (NPE) sponsors are in-person using methods commensurate with NIST FIPS 201. [9] Identity management for NPEs, however, is locally defined using ad-hoc procedures and local systems. Significant numbers of individuals who cannot use enterprise identity management systems are only registered locally.

  To prepare for more mature phases, organizations should ensure all users are registered and user information is accurate. Organizations should begin to standardize processes to identify and maintain records for NPE and other locally registered users.

- **Basic ZT maturity**: enterprise attribute standards are defined, and all local attributes are documented. All user attribute claims are validated during enterprise identity vetting or via approved remote vetting methods. All standard attributes can be integrated directly into access control mechanisms.

- **Intermediate ZT maturity**: enterprise user attributes are standardized for use in access mechanisms and authoritative sources are identified for each attribute. System owners can define additional user attributes as necessary to manage access to highly sensitive information, and processes to issue these attributes are standardized. Enterprise and locally defined attributes can be directly integrated into access control mechanisms.

- **Advanced ZT maturity**: Risk-based attributes are defined and standardized to alert resource managers of risk indicators associated with (NPE or person) entities. Authoritative sources for risk-based attributes have access to required system activity logs and are able to assess the associated risk and assert user values in support of risk-based responses. Note that risk-based responses can be manual or automated, to include enhanced monitoring, out-of-band investigation, conditional approval, or in extreme cases, denial of

access, and the responses may be resource specific. All user attributes relevant to a resource are integrated directly into the access mechanisms for that resource.

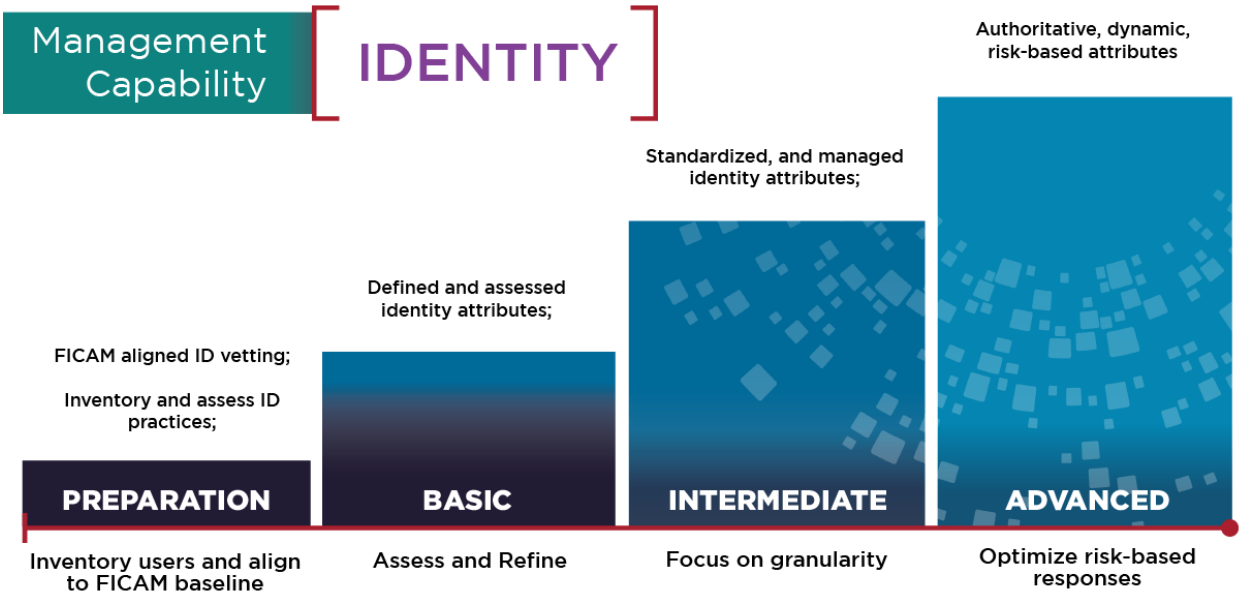

Figure 3: Zero Trust identity management maturity

Credential Management

Credential Management includes issuance, usage, and revocation of credentials bound to enterprise identities. Once identities are established, they must be issued secure credentials to prove to systems they are who they say they are. Each identity may be associated with multiple credentials, depending on the different roles or personas the entity may perform for the organization. It is strongly recommended that highly privileged users have separate credentials for their privileged and non-privileged roles. Each stage in the credential lifecycle — establishing, issuing, maintaining, and revoking credentials — is managed to ensure digital credentials are clearly bound to the physical or logical entity described by the identifier. Note that assertions made by single sign-on or identity federation servers, such as Kerberos or Active Directory, are also referred to as credentials. Here the logon and remote authentication credentials are distinguished from assertions made by single-sign-on or federation servers. The latter are covered under access management and federation capabilities.

Credential Management Capabilities

Credential management capabilities are well established for public-key credentials and are captured in certificate policies and various Federal, DoD, and NSS policy documents. They are less mature in use cases where alternate credentials are used. Credential management generally includes documenting the need for a credential, associating the entity with verified identity information, generation and issuance of the credential to the entity, and maintenance of the credential over its lifecycle, to include revocation, re-issuance or replacement, re-enrollment, and expiration. The systems, processes, and procedures for credential management are specific to the type of credential. NIST Special Publication (SP) 800-63 provides guidance for credentials used in federal systems. [10] Zero Trust principles depend on protecting access to resources using strong credentials.

Multi-factor authentication (MFA) is based on at least two of the three types of authentication factors: something you know, something you have, and something you are. The strength of authentication systems is described in NIST's SP 800-63 part B in terms of authenticator assurance levels (AAL) ranging from AAL 1 to AAL 3. Strongly assured methods are recommended for all person users with access to critical resources. **NSA recommends strong multi-factor authentication for person users.**

There are multiple authenticator methods that can be used individually or in combination to achieve the desired AAL. Software options include applications that generate time-based authentication codes or out-of-band prompts to authorize a login attempt. Some devices allow for leveraging a hardware root of trust on a computer or smartphone to enhance protection of secret or private keys used by software authenticators. Multi-factor hardware devices require activation using one or more factors (PIN alone, or supplemented with a biometric) and provide a one-time password or cryptographic authenticator. [11] Hardware one-time password devices can display a one-time password for user entry, isolating the user's private information from network access, or can connect directly to the user's device via a controlled interface. Certain cryptographic authenticators, known as phishing-resistant MFA, can provide phishing resistance by establishing a cryptographically verifiable connection between the user's device and the server. [12]

Compliance with EO 14028 requires MFA techniques for all users. Organizations should select strong MFA products that are validated to meet the desired AAL. Multifactor cryptographic device authenticators, like the common access card (CAC) and personal identity verification (PIV) card, as well as multifactor hardware tokens implementing FIDO2 mechanisms, are the most robust mechanisms commercially available, providing AAL 3 with phishing resistance.

For detailed MFA guidance, read more in Transition to Multifactor Authentication [11] and Selecting Secure Multi-factor Authentication Solutions. [13]

Non-person entity authenticators should be protected via hardware-based mechanisms. An NPE would ideally be represented by a public key certificate whose associated private key is under the strict control of the entity it represents, whether that entity is a physical device, a process, or other logical entity. Those entities that do not support public key authentication typically use passwords. Any such entities should use long, randomly generated passwords, stored as necessary in a hardware-protected password vault or isolated environment. All default passwords must be changed and system accounts that are not necessary should be disabled.

NPEs that support public-key credentials are sponsored and managed by authorized individuals who are responsible for ensuring the entity is accurately identified, either in a public-key certificate or in account records. The sponsor is also responsible for installing the private key associated with the credential to ensure it is protected from potential compromise, and prompt reporting of any suspected compromise. Hardware root-of-trust using trusted platform modules and execution isolation techniques are recommended to provide assurance that only the authorized entity associated with the credential has access to the private key.

Each authenticator must be managed by and only issued to authorized and vetted identities. Person users are responsible for reporting if their authenticator is no longer in their control (lost or compromised) or no longer needed. Sponsors for NPE entities are responsible for requesting revocation of a credential if the entity associated with the credential is compromised, or no longer active. All relying parties will need to be informed and disassociate the authenticator from user accounts or privileges in a timely manner when a credential is so reported. Users with multiple authenticators can leverage an enterprise lifecycle management system associated with one of the

authenticators, using methods described in NIST's Derived PIV guidance. [14]

Of special concern is the use of cryptographically obsolete methods. An enterprise must be able to replace user credentials if the methods used become obsolete. Without proper planning, this could have significant disruptive impacts to the enterprise. Even with careful planning, it is possible that a particular authentication method becomes weak. Enterprises should be able to respond to such a discovery by rapidly revoking obsolete or compromised mechanisms and deploying new credentials using secure methods, potentially to large numbers of users in a short period of time.

- **Issue authorized strong credentials** – according to each user's role/persona.
- **Inventory the type of credentials users utilize to log in for each account** – each credential is associated with the entity representing a persona and each persona is associated to the unique person. Each NPE credential is associated with the logical entity or to the process(es) and device(s) that can act as the logical entity, and to its sponsor.
- **Establish infrastructure, tools, and processes to enable reporting and dissemination of credential status information** – establish efficient processes and procedures to revoke all credentials associated with each user. For people users, establish efficient processes and procedures to revoke all credentials associated with a user device protecting software credentials, and to revoke all credentials associated with a hardware multifactor authenticator device. For NPE users, establish efficient processes and procedures to revoke all credentials associated with a sponsor, with a device, or associated with software or operating systems that can be compromised.

Maturity phases

- **Preparation for ZT**: FICAM requires person users to be assigned credentials issued by an enterprise-approved Public Key Infrastructure (PKI). Approved certificate policies governing such PKI include issuance during face-to-face interactions between the user or sponsor and an authorized registration officer or trusted agent, as well as efficient reporting and revocation processes. Users in defined exceptional use cases may use alternative MFA

credentials. To prepare for higher maturity levels, inventory all credentials associated with each user.

- **Basic ZT maturity**: All users, including those in authorized exceptional use cases, use enterprise-approved, highly assured authenticators that are compliant with NIST SP 800-63 guidance, where the credential lifecycle is managed using defined methods or via association with enterprise PKI credentials.
- **Intermediate ZT maturity**: Enterprises have established plans to update user credentials to ensure authenticators are compliant with NSS standards within the stated timelines (e.g., in accordance with NSM-10 [15] and CNSSP 15 [16]). All credentials are independently managed throughout their lifecycle and can be revoked rapidly in response to notification of compromise of the user, the user's device, or processes on the user's device.
- **Advanced ZT maturity**: Enterprises have established and effective processes and procedures to rapidly revoke and replace credentials when needed, including unanticipated compromise of cryptographic implementations. Authoritative sources of risk-based attributes can interface directly with credential revocation systems.

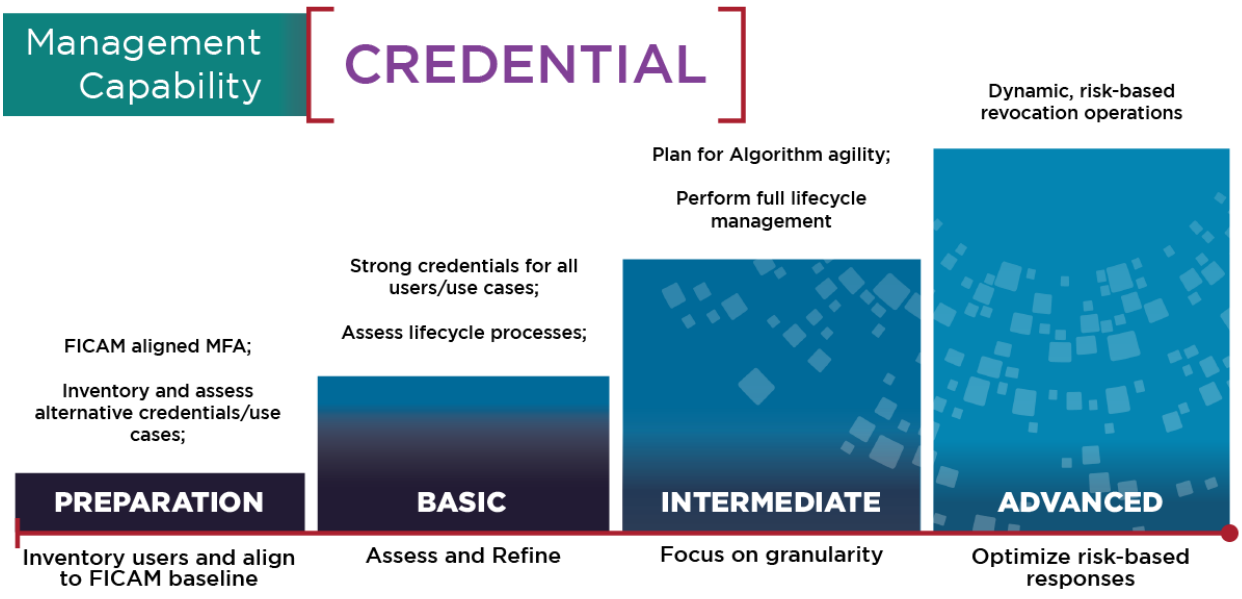

Figure 4: Zero Trust credential management maturity

Access Management

Access management includes management of the policies and mechanisms that ensure only authenticated users authorized for access to protected resources are able to gain access. FICAM recommendations include having mechanisms that ensure entities accessing resources are authenticated and authorized and held accountable for their activities, that provide confidentiality to protected resources, that preserve resource integrity, and that enable resources to be reliably available and properly maintained.

Access control frameworks provide access decisions at various levels of granularity, with mechanisms that support granular access rules generally representing a higher level of maturity. The recommendations here are stated in terms of an attribute-based access control model (ABAC). There are many ways of implementing these access controls, to include layered mechanisms that each consider different aspects of an access policy (See NIST SP 800-162 Guide to Attribute Based Access Control (ABAC) Definitions and Considerations). [17] Many implementations utilize single sign-on mechanisms that validate the user's credentials, verify attributes assigned to the authenticated identity, and issue access assertions to resources regarding the privileges conveyed in those attributes. These mechanisms tend to use broad, static, role-based access rules governing access to all resources on a system. Mechanisms to enforce dynamic, granular accesses to critical resources can be used directly, or as a supplement to these systems to achieve a balance of granularity and practicality.

Access control mechanisms should consider granularity, reliability, availability, and the potential risks to the resource. Attribute-based access control (ABAC) models provide the flexibility required to meet these goals. Assess the features of available access control systems against the ABAC model and consider enhancements to facilitate the desired features. Automated access denial decisions in response to probabilistic indicators (e.g., provided by behavior analytics) have the potential to disrupt mission and should be used sparingly. However, strong indicators of an active threat should be acted on quickly to minimize loss.

To determine what user and resource attributes are required for a given enterprise requires a comprehensive inventory and characterization of users, resources, and the users' ability to protect the data. At a minimum, mandatory access controls required by law should be supported by access mechanisms that are able to process dynamic

resource and user attributes for each access request. For National Security Systems, such attributes include classification, clearance, releasability, and citizenship attributes, along with community of interest restrictions and membership attributes. Additional role-based and need-to-know attributes specific to each sensitive resource are recommended. Attribute based mechanisms require an authoritative source for attributes and processes for users to be provisioned with attributes. In addition, resources need to be labeled with enterprise labels, and digital policies need to be established that reflect the access policies depending on the attributes.

Access Management Capabilities

- **Minimize privileges to specific roles necessary to accomplish mission functions** – Perform regular periodic reviews to remove unnecessary privileges. Automate removal of privileges (or attributes) based on lifecycle events (retirement/removal, change of position, etc.)
- **Least Privilege** – implementing least privilege access policies minimizes the damage a malicious actor can cause if they gain access to a limited set of credentials. It also limits the damage a user can cause through neglect, an accident, or malicious intent. Least privilege is most important for access to highly privileged functions, such as enterprise or domain administration. Least privilege concepts ensure that users can access the information they need while limiting gratuitous access. Current recommendations for highly privileged users include isolation – using separate devices, credentials, and accounts that are tailored to the highly privileged functions, but also isolated from high-risk activities. Current recommendations also include consideration of specialized tools that enforce role separations and workflow restrictions for highly privileged users.
- **Just in Time (JIT) / Just Enough Access (JEA)** – in addition to granular access rules, just in time / just enough access policies are a type of least privilege access that grants privileges to controlled resources only for predetermined periods of time on an as-needed basis. Access policies that apply JIT/JEA to highly sensitive resources, including highly privileged management functions or roles that govern ICAM functions, are recommended as highly effective at reducing abuses and containing adversary access.

- **Privileged Access Management (PAM) Tools** – privileged access management (PAM) tools provide a centralized management interface for assigning fine-grained privileges based on risk exposure and least privilege access, only allowing as much access as required. PAM tools can also proxy privileged user access to resources (especially administrative functions) that do not support verification of strong authenticators, support workflow constraints, and enforce role separation. Privileged accounts and services must be controlled because threat actors continue to target administrator credentials for access to high-value assets and to move laterally through the network. As with other policy enforcement mechanisms, PAM implementations should be tightly controlled and monitored, since they control the highly privileged functions that shape the environment, making them an attractive target, as many incident response operations have revealed.

- **Privileged Access Devices** – providing a designated and dedicated device, sometimes called privileged access workstations, for all administration functions and accounts further supports isolation from unauthorized disclosure or unauthorized use of privileged accounts. This can be via a virtual workstation or a physical workstation. It is important that administrative workstations only have access to essential applications required to perform administrative actions and do not allow high-risk activities, such as email or web browsing.

- **Fine-grained, risk adaptive access policies** – a risk adaptive access framework ensures that organizations can balance reliability, availability, and mission performance against adversary threats. Access policies that include fine-grained access decisions are better suited to address threats while maintaining mission critical operations. In general, resources should be categorized using enterprise attributes that correlate to organizational mission sensitivities and security needs. To protect resources from adversary compromise, controls must be manageable, used, and enforced.

Maturity phases

- **Preparation for ZT**: Access control mechanisms are largely identity based, with manually managed groups and roles, and separate access control lists

must be maintained on disparate systems that support a variety of access methods. Some administrative accesses are segregated onto subnets and some highly privileged users may have separate administrator credentials. To prepare to mature these practices, inventory user entitlements and access policies, and understand the user and resource attributes that are implicit in those policies and entitlements. Remove entitlements that are outdated, inappropriate for the user's role, or no longer needed for mission. Identify those attributes which could be used directly in an attribute-based mechanism and determine if enterprise managed attributes can be used or whether locally defined attributes are appropriate. Applications that depend only on legacy account management mechanisms are identified and updated to use modern methods, allowing the weak legacy mechanisms to be disabled.

- **Basic ZT maturity**: Review current access policies against least privilege principles. Implement PAM for all users having access to highly privileged functions, especially for management of resources that do not support verification of strong authenticators. Identify authoritative sources for user attributes and implement data tagging for all critical resources to support more granular access models. Ensure accesses are logged to support forensics. Authentication assertions are limited in time and scope.
- **Intermediate ZT maturity**: Refined access policies enable segregation of resources. Access to highly privileged functions are segregated both logically and chronologically, using dedicated workstations and PAM tools that support JIT/JEA policies. Access policies begin to reflect the strength of authentication by minimizing access for weaker authentication methods (e.g., passwords.) Further they distinguish access for users of alternative MFA to specific instances that require them. General users have limited access based on the totality of attributes relevant to the access policy. Specifically, to the requested resource, which mean they are re-authenticated and re-validated for access to different resources as work responsibilities change. Access decisions depend on both the user requesting access and the device/systems used to make the request. Single sign-on assertions are time-bound and specific to classes of resources having identical access rules or are supplemented with dynamic attribute-based access rules.

- **Advanced ZT maturity**: User accesses are granular to the specific resource being requested, considering the user and their device, as well as the sensitivity of the application and specific data associated with the request. Person and NPE user attributes include risk-based indicators provided by authoritative sources. Access policies for sensitive resources are able to use risk-based attributes of the user and device to minimize risk. User activity information is assessed against user roles and behavior patterns to identify increased risk. Appropriate risk responses are triggered (via manual or automated processes) based on risk attributes. Analytic capabilities that support user risk-based attributes, such as continuous authentication, can be used to trigger re-authentication or other responses to determine potential compromise of user credentials.

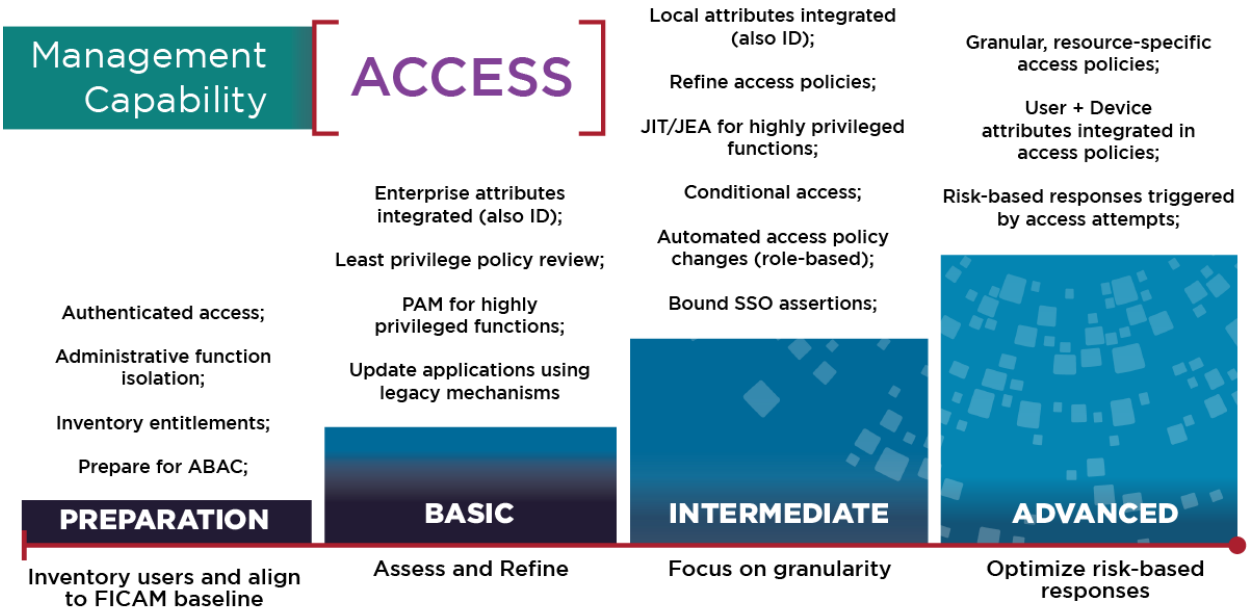

Figure 5: Zero Trust access management maturity

Identity Federation

Identity federation includes the technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by partners to securely share information in accordance with the access policies of multiple partners. Often, partners will have identity, credential, and access management implementations of varying maturity, and will almost certainly have distinct implementations that complicate sharing. Zero Trust mechanisms do not remove

requirements for cross-domain solutions, especially when information sensitivity differences create excessive risk or when maturity levels vary widely.

FICAM requirements for federation apply to all maturity levels. Further, they include establishing confidence in each partner's identity/credential management credential management practices, and addressing validation requirements for different authenticators. Also, mapping authentication assertions from multiple sources, sharing and aligning the attributes issued by each partner, and reconciling access policy differences are key FICAM requirements needed for mature ZT approaches. In addition to high-level agreements about sensitive information that will be shared; the formatting, equivalency, and interfaces of shared information will need to be negotiated by IT security leadership.

To ensure federation does not create an unacceptable risk, mitigating controls need to be established to address interoperability or capability gaps, as well as differences in maturity levels.

At higher maturity levels, organizations and their partners may be required to share sensitive risk-based attributes, access to back-end credential and inventory repositories, and detailed system access logs. Access policies should reflect access restrictions for partner requests. In general, federation between partner organizations is complicated, and will depend on the partner agreements, the capabilities and maturity of each partner's system, and the assessed risk associated with each system.

Guidance to follow when implementing Identity Federation

- Establish an inventory of partner identities your systems need to support, and what you know about those identities (user attributes), including PEs and NPEs
- Map partner identity and credential assurance levels and map partner-issued attributes to local equivalents.
- Map access policies to reflect partner sharing agreements, and to account for partner identities and attributes.
- Establish levels of trust for federated identities, and adapt access decisions to those trust levels. See NISTIR 8336. [10] [18]

Summary of Guidance

Expanding and refining the FICAM roadmap under the principles of a Zero Trust security model, according to the maturity model developed here, will provide an organization with tools and processes for resisting, detecting, and responding to ever increasing threats that exploit weaknesses or gaps in their ICAM programs. The tools and processes support an operational mindset that threats exist within the nominal boundaries of their systems. Vigilance is required to ensure that risks are continually assessed and appropriate responses are enacted in a timely manner, with follow-up investigations and damage control as necessary. National Security System owners and operators are strongly recommended to mature their Identity Management, Credential Management, Access Management, and operational practices of their enterprise, working through the capabilities outlined towards advanced maturity.

Identity Management begins with establishing a current and accurate inventory of all users, including person and non-person entities, ensuring those with access to critical resources are vetted and registered. Credential Management includes enforcing multi-factor authentication and the issuance, usage, and revocation of credentials bound to enterprise identities. Access Management includes implementing concepts of least privilege, working towards the goal of fine-grained access control. Identity federation will depend on partner agreements, the capabilities and maturity of each partner's system, and the assessed risk associated with each system. Organizations and their partners should work towards advancing each of these areas through the FICAM roadmap to mature their Zero Trust implementations.

Common Exceptions

While all systems should consider improvements based on the Zero Trust security model, certain types of systems may not be amenable to the specific constraints of particular Zero Trust designs. In certain scenarios, especially for safety and effectiveness purposes, such users may not be able to be individually authenticated. For example, facilities and industrial control centers where personnel must be able to take actions at a moment's notice or certain weapons platforms where constant re-authentication may be impractical. Other mechanisms, sometimes even non-technical ones, may be necessary for access control in these cases.

Further guidance

NSA is assisting DoD customers that are piloting ZT capabilities, coordinating ZT activities with NIST, CISA, NSS, and DoD, and developing additional ZT guidance to support system developers through the challenges of integrating ZT within NSS, DoD, and Defense Industrial Base (DIB) environments. Upcoming additional guidance will help organize, guide, and simplify incorporating Zero Trust principles and designs into enterprise networks.

Supplementary NSA guidance on implementing a Zero Trust architecture and ensuring a secure and defensible network environment are available at https://www.nsa.gov/cybersecurity-guidance:

- NSA CSI Embracing a Zero Trust Security Model
- NSA's Top Ten Cybersecurity Mitigation Strategies
- Defend Privileges and Accounts
- Continuously Hunt for Network Intrusions
- Segment Networks and Deploy Application-aware Defenses
- Transition to Multi-factor Authentication
- Actively Manage Systems and Configurations
- Performing Out-of-Band Network Management
- Hardening SIEM Solutions
- Mitigating Cloud Vulnerabilities
- Selecting Secure Multi-Factor Authentication Solutions

Partners at NIST, CISA, DoD, and others have produced guidance that relates to ZT architecture and capabilities, including:

- NIST SP 800-53 rev 5: Assessing Security and Privacy Controls in Information Systems and Organizations
- NIST SP 800-63-3: Digital Identity Guidelines (overview and parts a, b, c)
- NISTIR 8149: Developing Trust Frameworks to Support Identity Federations
- Federal ICAM Architecture
- NIST SP 800-207: Zero Trust Architecture
- CISA Zero Trust Maturity Model
- DoD Zero Trust Reference Architecture

Works cited

[1] Verizon (2021), 2020 Verizon Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf

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

[3] NIST (2020), NIST Special Publication 800-207: Zero Trust Architecture. https://csrc.nist.gov/publications/detail/sp/800-207/final

[4] CISA (2021), CISA Zero Trust Maturity Model. https://cisa.gov/zero-trust-maturity-model

[5] DoD (2021), DoD Zero Trust Reference Architecture. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[6] GSA (2021), Federal Identity, Credential, and Access Management (FICAM) Architecture. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf

[7] The White House (2021), Executive Order 14028: Improving the Nation's Cybersecurity. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[8] The White House (2022), National Security Memorandum 8: Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

[9] NIST (2022), NIST Federal Information Processing Standards (FIPS) 201-3. https://csrc.nist.gov/publications/detail/fips/201/3/final

[10] NIST (2017), Special Publication 800-63: Digital Identity Guidelines. https://pages.nist.gov/800-63-3/

[11] NSA (2019), Transition to Multifactor Authentication. https://media.defense.gov/2019/Sep/09/2002180346/-1/-1/0/Transition%20to%20Multi-factor%20Authentication%20-%20Copy.pdf

[12] CISA (2022), Implementing Phishing-Resistant MFA. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[13] NSA (2020), Selecting Secure Multi-factor Authentication Solutions. https://media.defense.gov/2020/Sep/22/2002502665/-1/-1/0/Multifactor_Authentication_Solutions_UOO17091520_V1.1%20-%20Copy.PDF

[14] NIST (2014), NIST Special Publication 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf

[15] The White House (2022), National Security Memorandum 10: Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[16] CNSS (2016), Committee on National Security Systems (CNSS) Policy 15: Use of Public Standards for Secure Information Sharing. https://www.cnss.gov/CNSS/issuances/Policies.cfm

[17] NIST (2019), NIST Special Publication 800-162: Guide to Attribute Based Access Control (ABAC) Definitions and Considerations. https://csrc.nist.gov/publications/detail/sp/800-162/final

[18] NIST (2021), NISTIR 8336 (Draft): Background on Identity Federation Technologies for the Public Safety Community. https://csrc.nist.gov/publications/detail/nistir/8336/draft

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov