Cybersecurity & Information Systems Information Analysis Center

CSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

Open Standards That Support Zero Trust Implementation

Report Number:

CSIAC-BCO-2025-692

July 2025

CSIAC is a U.S. Department of Defense Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017

-1505
Office: 443-360-4600

REPORT PREPARED BY:
Olutoye Sekiteri
Office: CSIAC

Information contained in this report does not constitute endorsement by the U.S. Department of Defense of any nonfederal entity or technology sponsored by a nonfederal entity.

CSIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. CSIAC is operated by the SURVICE Engineering Company.

Distribution Statement A. Approved for public release: distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering, and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
11-07-2024	Technical Research Report	

4. TITLE AND SUBTITLE

Open Standards That Support Zero Trust Implementation

5a. CONTRACT NUMBER
FA8075-21-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Olutoye Sekiteri

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Cybersecurity & Information Systems Information Analysis Center (CSIAC)
SURVICE Engineering Company
4695 Millennium Drive
Belcamp, MD 21017-1505

8. PERFORMING ORGANIZATION REPORT NUMBER

CSIAC-BCO-2025

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center (DTIC)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Statement A. Approved for public release: distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Cybersecurity and Information Systems Information Analysis Center (CSIAC) was tasked with researching and providing information on open standards applicable to zero trust implementation. CSIAC identified various open standards being used today that support and uphold the implementation of the zero trust architecture within the U.S. Department of Defense.

15. SUBJECT TERMS

zero trust, open standards, cybersecurity, network infrastructure

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Ted Welsh, CSIAC Director
U	U	U	UU	20	**19b. TELEPHONE NUMBER** *(include area code)* 443-360-4600

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Distribution Statement A. Approved for public release: distribution is unlimited.

About

DTIC and CSIAC

The Defense Technical Information Center (DTIC) preserves, curates, and shares knowledge from the U.S. Department of Defense's (DoD's) annual multibillion-dollar investment in science and technology, multiplying the value and accelerating capability to the Warfighter. DTIC amplifies this investment by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision-makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Centers (DoDIAC), which provide critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a DoDIAC sponsored by DTIC to provide expertise in four technical focus areas: cybersecurity, knowledge management & information sharing, modeling & simulation, and software data & analysis. CSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

TI Research

A chief service of the DoDIAC is free technical inquiry (TI) research limited to four research hours per inquiry. This TI response report summarizes the research findings of one such inquiry. Given the limited duration of the research effort, this report is not intended to be a deep, comprehensive analysis but rather a curated compilation of relevant information to give the reader/inquirer a "head start" or direction for continued research.

Abstract

The Cybersecurity and Information Systems Information Analysis Center (CSIAC) was tasked with researching and providing information on open standards applicable to zero trust implementation. CSIAC identified various open standards being used today that support and uphold the implementation of the zero trust architecture within the U.S. Department of Defense.

Contents

List of Figures

1.0 TI Request

1.1 Inquiry

What open standards apply to zero trust implementation?

1.2 Description

The Cybersecurity and Information Systems Information Analysis Center (CSIAC) was asked to identify open standards that are directly applicable to the implementation of zero trust within the U.S. federal government's information networks. The inquirer also wanted to know of the existence, applicability, and status of relevant open standards.

2.0 TI Response

2.1 What Is Zero Trust?

The zero trust architecture (ZTA) and philosophy are based on a strict security strategy that focuses on the belief that trust in an entity is a vulnerability [1]. ZTA operates under the premise that every internal or external user and device attempting to access resources on a network are suspicious [2]. It is not a service or project but a security approach for designing, constructing, and implementing an organization's computer and information systems. It shifts the focus of security from being location-based to being data-based. ZTA requires continuous authentication, authorization, and validation of security configurations before access is granted to applications and data [3]. This security framework focuses on the following core security principles [4]:

- Always Verify: Always authenticate and authorize users and devices based on all available data points, prior to granting access.
- Use Least Privileged Access: Limit user access with just-in-time and just-enough access. Use risk-based adaptive policies and viable data protections.
- Assume a Breach: Minimize the damage or "blast radius" during an incident and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.
- Continuous Monitoring: Require constant monitoring and validation from an entity's point-of-entry throughout the duration of the entity's session on the network.

The important aspects of ZTA can also be visualized with the depiction of the pillars of zero trust, which include identity, devices, network, applications and workloads, and data (Figure 1).

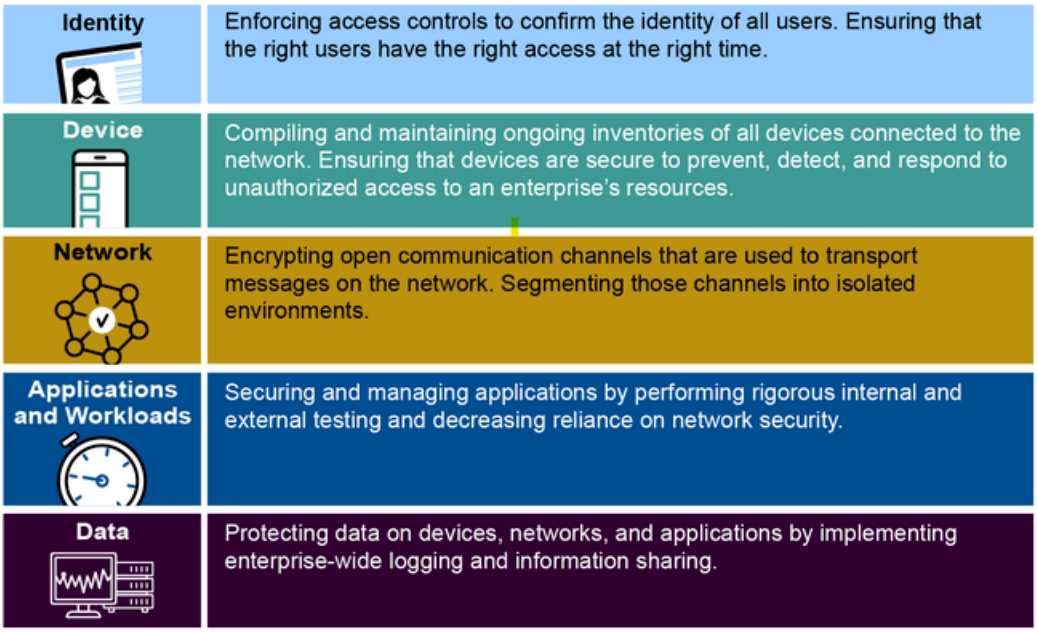

Figure 1. U.S. Government Accountability Office Analysis of the Cybersecurity and Infrastructure Security's Zero Trust Maturity Model [5].

2.1.1 Zero Trust Network Infrastructure Components

Network infrastructures are subject to different organizational requirements, limitations, and existing technological implementations, all of which affect how ZTA is planned and executed. According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, there are several logical tools, components, and data sources used to facilitate ZTA and its core principles [6]:

- Policy Engine (PE): This component is responsible for the ultimate decision to grant access to a resource for a given subject. The PE uses enterprise policy as well as input from external sources (e.g., [continuous diagnostics and mitigation systems] CDM, threat intelligence services) as input to a trust algorithm to grant, deny, or revoke access to the resource. The PE is paired with the policy administrator (PA) component. The PE makes and logs the decision (as approved or denied), and the PA executes the decision.
- PA: This component is responsible for establishing and/or shutting down the communication path between a subject and a resource (via

commands to relevant policy enforcement points (PEPs)). It would generate any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. It is closely tied to the PE and relies on its decision to ultimately allow or deny a session. If the session is authorized and the request authenticated, the PA configures the PEP to allow the session to start. If the session is denied (or a previous approval is countermanded), the PA signals to the PEP to shut down the connection. Some implementations may treat the PE and PA as a single service; here, it is divided into its two logical components. The PA communicates with the PEP when creating the communication path. This communication is done via the control plane.

- PEP: This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and/or receive policy updates from the PA. This is a single logical component in ZTA but may be broken into two different components: the client (e.g., agent on a laptop) and resource side (e.g., gateway component in front of a resource that controls access) or a single portal component that acts as a gatekeeper for communication paths. Beyond the PEP is the trust zone hosting the enterprise resource.
- Enterprise Public-Key Infrastructure (PKI): This system is responsible for generating and logging certificates issued by the enterprise to resources, subjects, services, and applications. This also includes the global certificate authority ecosystem and the federal PKI, which may or may not be integrated with the enterprise PKI.
- Identity (ID) Management System: This is responsible for creating, storing, and managing enterprise user accounts and identity records (e.g., lightweight directory access protocol [LDAP] server). This system contains the necessary subject information (e.g., name, email address, certificates) and other enterprise characteristics such as role, access attributes, and assigned assets. This system often utilizes other systems (such as a PKI) for artifacts associated with user accounts.

- Security Information and Event Management (SIEM) System: This collects security-centric information for later analysis. These data are then used to refine policies and warn of possible attacks against enterprise assets.
- Threat Intelligence Platforms: This provides information from internal or external sources that help the PE make access decisions. These could be multiple services that take data from internal and/or multiple external sources and provide information about newly discovered attacks or vulnerabilities.

Two more components/tools mentioned in NIST SP 800-207 are [6]:

- Risk-Based Multifactor Authentication: Verifies the identities of users and systems based on their risk profile at any given moment.
- Cloud Workloads: Maintain security across cloud environments, including virtual machines, containers, and hybrid deployments, ensuring that workloads are protected from breaches.

2.1.2 Different Approaches to Zero Trust

NIST SP 800-207 also describes different approaches to implementing ZTA [6]:

- Enhanced Identity Governance: This approach to ZTA focuses on user and device identity as the main factors for access control. Organizational policies are driven by identity, device status, location, time, and other attributes such as role and group membership. This approach requires explicit verification of any access request from all related entities, which goes beyond traditional perimeter-based security. The system continuously monitors access and makes changes to policies as needed. This works well for network environments with cloud-based services, guest access, or bring-your-own-device policies. It demands robust identity and access management (IAM) and proactive threat monitoring capabilities.
- Micro-Segmentation: This approach separates the network into smaller, isolated segments. This segmentation limits the potential impact a breach may have on the network environment. Each network segment is protected by PEPs that act as the gateway that enforces strict access control policies; this reduces the chance of unauthorized lateral movement. The identity governance aspect of ZTA helps define access privileges, but the implementation relies heavily on network controls. Taking this

approach requires the management of the numerous segments and all the associated policies for improved security, which can be complex and result in increased administrative overhead.

- Software-Defined Perimeters (SDP) and Network Infrastructure: This leverages network infrastructure and software-defined principles to create a dynamic, policy-driven security perimeter. Resources are effectively "hidden" until a user or device is authenticated and authorized. The SDP dynamically creates secure one-to-one connections using overlay networks and software-designed networks to enforce access policies. The PA controls the network, reconfiguring it based on policy decisions. This approach offers specialized control and resource camouflaging but requires deep expertise in networking and security technologies.

2.2 What Are Open Standards?

The International Organization for Standardization (ISO) is an independent, nongovernmental international organization that develops international standards. It defines a standard as a [7]:

> …document, established by consensus and approved by a recognized body, that provides—for common and repeated use—rules, guidelines, or characteristics for activities or for their results, aimed at the achievement of the optimum degree of order in a given context.

For a standard to be considered an "open" standard, the specification and rights to implement it must be publicly available to any person or organization without signing a nondisclosure agreement or paying a fee. Open standards also must be approved and maintained for the public by a governing body of qualified contributors using a consensus-driven process.

Other notable standardization organizations (along with their more well-known acronyms) include [8]:

- Internet Engineering Task Force (IETF)
- International Electrotechnical Commission (IEC)
- International Telecommunication Union (ITU)
- World Wide Web Consortium (W3C)
- European Committee for Standardization (CEN)
- European Telecommunications Standards Institute (ETSI)
- Institute of Electrical and Electronics Engineers Standardization Association (IEEE SA)
- National Institute of Standards and Technology (NIST)

This collaboration of multiple knowledgeable entities promotes vendor neutrality and prevents vendor lock-in. This means that no single company controls the standard, which encourages competition and gives users more choices in selecting hardware and software. This open approach fosters interoperability and agnostic usage, enabling diverse systems from different vendors to seamlessly communicate and share data, which is essential for data exchange and software integration and for avoiding data silos. Furthermore, a governing body of qualified contributors maintains and approves these standards through a public, consensus-driven process, ensuring transparency and broad community involvement. The collaborative environment created with the development of open standards fosters innovation by providing a common platform for developers, which leads to faster development and more robust solutions. In contrast to proprietary standards, which can limit choices and create compatibility issues, open standards encourage a more interconnected and collaborative digital ecosystem. This open development process, unlike the closed nature of proprietary technologies, allows for greater community input, leading to higher-quality standards and minimizing the risks associated with vendor lock-in. Some common examples of open standards seen and used widely across different technologies and manufacturers regularly include Wi-Fi, Hypertext Markup Language, Structured Query Language, and Extensible Markup Language (better known as HTML, SQL, and XML, respectively).

2.3 Open Standards That Support Zero Trust Implementation

This section provides a list of open standards used today within the general information technology space that supports the principles of ZTA. Open standards are categorized based on what pillar of zero trust they align with the most.

2.3.1 IAM

A description and current status for IAM open standards OAuth 2.0, OpenID Connect (OIDC), Security Assertion Markup Language (SAML), Fast Identity Online (FIDO), System for Cross-Domain Identity Management (SCIM), and the Secure Production Identity Framework for Everyone (SPIFFE) are detailed as follows:

- OAuth 2.0
  - Description: An authorization framework that allows a resource owner to grant a third party limited access to their hypertext transfer protocol (HTTP) services without sharing credentials [9].

  - Status: Widely used and included in just about every U.S. Department of Defense (DoD) Chief Information Officer-approved identity, credential, and access management solution with any fidelity.

- OIDC
  - Description: An authentication protocol based on the OAuth 2.0 framework that enables secure user authentication. "It simplifies the way to verify the identity of users based on the authentication performed by an authorization server and to obtain user profile information in an interoperable and representational state transfer (REST)-like manner" [10].
  - Status: Widely used in information technology solutions such as Microsoft Azure Active Directory, Okta, and Ping Identity.
- SAML
  - Description: An XML-based framework for exchanging authentication and authorization data between parties. "SAML makes single sign-on (SSO) technology possible by providing a way to authenticate a user once and then communicate that authentication to multiple applications" [11].
  - Status: Widely used in information technology solutions such as Microsoft Azure Active Directory, Office 365, Okta, and ServiceNow. SAML tokens are also used in various enterprises and cloud architectures.
- FIDO
  - Description: A set of standard authentication protocols for strong authentication using public-key cryptography that is meant to replace passwords with secure cryptographic keys stored on user devices. FIDO uses "passkeys" such as fingerprints, facial recognition, speaking to a microphone (voice recognition), entering a personal identification number (better known as PIN), or inputting a pattern instead of password [12].
  - Status: Commercially available but has not seen use within the DoD.
- SCIM
  - Description: A protocol that standardizes how identity information is exchanged between one entity and another. SCIM automates the flow of information between an identity provider or IAM system and cloud-based applications [13].

- Status: Widely used commercially. Used in the DoD for identity federation, for some cases.

- SPIFFE
  - Description: "A set of open-source standards for securely identifying software systems in dynamic and heterogeneous environments." SPIFFE provides "specifications for a framework capable of bootstrapping and issuing identity to services across heterogeneous environments and organizational boundaries" [14].
  - Status: Supports workload identity federation with Kubernetes and use of X.509, mutual transport layer security (TLS), and JavaScript Object Notation (JSON) web token (known as JWT) secure and verifiable ID authentication [14].

2.3.2 Device Security

A description and current status for device security open standards Trusted Platform Module (TPM) and endpoint detection and response (EDR) are detailed as follows:

- TPM
  - Description: A hardware-based security feature for secure cryptographic operations that can securely store artifacts used to authenticate the platform (a personal computer or laptop). These artifacts can potentially be passwords, encryption keys, or certificates. A TPM can also be used to save platform measurements that help ensure that the platform remains trustworthy [15].
  - Status: Widely used and required to run Windows 11.
- EDR Standards
  - Description: Standards for detecting and responding to threats on endpoints, often guided by frameworks like MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).
  - Status: Commercially available and included in standards/guidelines such as the MITRE ATT&CK framework [16], NIST SP 800-137 ("Information Security Continuous Monitoring [ISCM] for Federal Information Systems and Organizations") [17], NIST SP 800-83 ("Guide to Malware Incident Prevention and Handling for Desktops and Laptops") [18], and Center for Internet Security Controls [19].

2.3.3 Network Security

A description and current status for network security open standards TLS, internet protocol security (IPsec), and zero trust network access (ZTNA) are detailed as follows:

- TLS
  - Description: A protocol for providing "a secure channel between two communicating peers" over a computer network. The only requirement from the underlying transport is a reliable, in-order data stream [20].
  - Status: Widely used across DoD networks and is currently at Version 1.3. This is included in many Defense Information Systems Agency security technical implementation guides [20].
- IPsec
  - Description: A suite of protocols for securing internet protocol communications. Commonly used to provide virtual private networks (VPNs) [21].
  - Status: Widely used across DoD networks for many site-to-site and remote-access VPN connections.
- ZTNA Standards
  - Description: Guidelines and protocols for implementing zero trust principles in network access [6].
  - Status: Nascent/conceptual.

2.3.4 Application Security

A description and current status for application security open standards Open Web Application Security Project (OWASP), software composition analysis (SCA), and OpenAPI specification are detailed as follows:

- OWASP
  - Description: Community-driven project focused on improving the security of software [22].
  - Status: Widely used and assists developers with understanding application security, especially surrounding web applications.
- SCA Standards
  - Description: Standards for analyzing and managing open-source components in software. This includes OWASP software component verification standard for its

dependency check tool [23], NIST SP 800-161 (“Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations”) [24], and ISO/IEC 5230:2020 (“Information Technology—OpenChain Specification”) [25].

- Status: Commercially available.

- OpenAPI Specification
  - Description: A standard for defining RESTful application programming interfaces (APIs), allowing both humans and computers to discover and understand the capabilities of a service without access to source code [26].
  - Status: This open standard and Swagger are on Version 3.1.0 and are used in DoD’s HTTP APIs. DoD officials are looking to enforce this across the DoD. CSIAC also advocated for this standard’s use within its own programs of record.

2.3.5 Data Security

A description and current status for data security open standards advanced encryption standard (AES) data loss prevention (DLP), and Secure/Multipurpose Internet Mail Extension (S/MIME) are detailed as follows:

- AES
  - Description: A symmetric encryption standard that is used worldwide [27].
  - Status: Widely used and even acceptable by the National Security Agency for the Commercial Solutions for Classified Program to transport classified information.
- DLP Standards
  - Description: Standards and guidelines for preventing unauthorized data exfiltration.
  - Status: Commercially available and seen extensively within standards/frameworks such as ISO/IEC 27001:2022 (“Information Security, Cybersecurity, and Privacy Protection—Information Security Management Systems—Requirement”) [28], NIST SP 800-53 (“Security and Privacy Controls for Information Systems and Organizations”) [29], General Data Protection Regulation [30], Payment Card Industry Data Security Standard [31], and Health Insurance Portability and Accountability Act (better known as HIPAA) [32].
- S/MIME

- Description: An email encryption and signing industry standard widely used by corporations to enhance email security. S/MIME is compatible with most enterprise email clients [33].
- Status: Widely used. Functionality is built into Microsoft Outlook and 365.

3.0 Conclusions

Designing a network infrastructure and environment with zero trust in mind can significantly enhance an organization's cybersecurity posture. ZTA bolsters cyberdefenses by removing implicit trust, enforcing least-privilege access, and continuously verifying and validating each access request for resources. These security principles improve network visibility, monitoring capabilities, incident response, and support for cloud services while still granting an organization flexibility to scale its network to meet its demands. The open standards like OAuth 2.0, SAML, SCIM, OpenAPI, IPSec, TPM, and TLS can further strengthen an organization's cybersecurity posture by ensuring secure authentication, efficient identity management, encrypted communications, and hardware-compatible security. Due to the agnostic and interoperable nature of open standards, secure protocols and best practices can be implemented across a diverse set of information technology environments using ZTA. By combining and implementing these technologies, organizations can create a more future-proof and robust security framework that reduces insider and advanced persistent threats and addresses necessary compliance requirements.

References

[1] Cunningham, C. "A Look Back at Zero Trust: Never Trust, Always Verify." Forrester, https://www.forrester.com/blogs/a-look-back-at-zero-trust-never-trust-always-verify/, 20 August 2020.

[2] Cybersecurity & Infrastructure Security Agency. "No Trust? No Problem: Maturing Towards Zero Trust Architectures." https://www.cisa.gov/news-events/news/no-trust-no-problem-maturing-towards-zero-trust-architectures, 7 September 2021.

[3] Terry, R. "Zero Trust Security Explained: Principles of the Zero Trust Model." CrowdStrike, https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/, 13 March 2025.

[4] Microsoft. "What Is Zero Trust." Microsoft Security, https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview, 27 February 2025.

[5] U.S. Government Accountability Office. "Cybersecurity: Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains." GAO, https://www.gao.gov/products/gao-23-105466#:~:text=Secret%20Service%20had%20additional%20efforts,all%20of%20OMB's%20required%20actions, 15 November 2022.

[6] National Institute of Standards and Technology. "Zero Trust Architecture." NIST SP 800-207, https://csrc.nist.gov/pubs/sp/800/207/final, 11 August 2020.

[7] American Society for Quality. "ISO Standards." ASQ, https://asq.org/quality-resources/standards-101?srsltid=AfmBOorh1UOJcf57_o4HORNfhpQxCdbnPyWWI2MrYDleW4NXqwzTxBko#standards, accessed on 10 May 2025.

[8] Next Generation IoT Initiative. "Standardization Bodies." Next Generation IoT, https://ngiot.eu/standardization-bodies/, accessed on 10 May 2025.

[9] OAuth 2.0. "OAuth 2.0." https://oauth.net/2/, accessed on 10 May 2025.

[10] OpenID Foundation. "How OpenID Connect Works." OpenID, https://openid.net/developers/how-connect-works/, accessed on 10 May 2025.

[11] CloudFlare, Inc. "What Is SAML | How SAML Authentication Works." CloudFlare, https://www.cloudflare.com/learning/access-management/what-is-saml/, accessed on 10 May 2025.

[12] FIDO Alliance. "Passkeys." https://fidoalliance.org/passkeys/, accessed on 10 May 2025.

[13] SCIM. "SCIM: System for Cross-Domain Identity Management." https://scim.cloud/, accessed on 10 May 2025.

[14] The SPIFFE Authors. "SPIFFE Overview." SPIFFE, https://spiffe.io/docs/latest/spiffe-about/overview/, accessed on 25 June 2025.

[15] Trusted Computing Group. "Trusted Platform Module (TPM) Summary." https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/, accessed on 10 May 2025.

[16] The MITRE Corporation. "ATT&CK." MITRE | ATT&CK, https://attack.mitre.org/, accessed on 10 May 2025.

[17] National Institute of Standards and Technology. "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations." NIST, NIST SP 800-137, https://csrc.nist.gov/pubs/sp/800/137/final, 1 September 2011.

[18] National Institute of Standards and Technology. "Guide to Malware Incident Prevention and Handling for Desktops and Laptops." NIST, NIST SP 800-83, Revision 1, https://csrc.nist.gov/pubs/sp/800/83/r1/final, 23 July 2013.

[19] Center for internet Security. "Creating Confidence in the Connected World." CIS, https://www.cisecurity.org/, accessed on 10 May 2025.

[20] Internet Engineering Task Force. "The Transport Layer Security (TLS) Protocol Version 1.3." IETF, https://datatracker.ietf.org/doc/html/rfc8446, 1 August 2018.

[21] Internet Engineering Task Force. "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap." IETF, https://datatracker.ietf.org/doc/html/rfc6071, 1 February 2011.

[22] OWASP Foundation, Inc. "OWASP: Explore the World of Cyber Security." OWASP, https://owasp.org/, accessed on 10 May 2025.

[23] OWASP Foundation, Inc. "OWASP Dependency-Check." OWASP, https://owasp.org/www-project-dependency-check/, accessed on 10 May 2025.

[24] National Institute of Standards and Technology. "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." NIST SP 800-161, Revision 1, https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final, 1 November 2024.

[25] International Organization for Standardization. "Information Technology—OpenChain Specification." ISO, ISO/IEC 5230:2020, https://www.iso.org/standard/81039.html, 1 December 2020.

[26] The Linux Foundation. "What Is OpenAPI?" OpenAPI Initiative, https://www.openapis.org/what-is-openapi, accessed on 10 May 2025.

[27] National Institute of Standards and Technology. "Advanced Encryption Standard (AES)." NIST, https://www.nist.gov/publications/advanced-encryption-standard-aes, 26 November 2001.

[28] International Organization for Standardization. "Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements." ISO, ISO/IEC 27001:2022, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en, 2022.

[29] National Institute of Standards and Technology. "Security and Privacy Controls for Information Systems and Organizations." NIST SP 800-53, Revision 5, https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final, 10 December 2020.

[30] European Parliament and the Council of the European Union. "General Data Protection Regulation (GDPR)." *Official Journal of the European Union,* vol. 59, pp. L119/1–L119/88, Regulation EU 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng, 27 April 2016.

[31] PCI Security Standards Council, LLC. "PCI DSS: v4.0.1." https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf, June 2024.

[32] 104th U.S. Congress. "Health Insurance Portability and Accountability Act of 1996." P.L. 104-191, U.S. Government Publishing Office, Washington, DC, https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996, 20 August 1996.

[33] Microsoft. "S/MIME for Message Signing and Encryption in Exchange Online." Microsoft Ignite, https://learn.microsoft.com/en-us/exchange/security-and-compliance/smime-exo/smime-exo, 2 February 2024.

Biography

Olutoye Sekiteri works with the Cybersecurity & Information Systems Information Analysis Center (CSIAC) as a research analyst. He provides research efforts related to CSIAC's four technical focus areas, conducts data analysis to support U.S. Department of Defense science and technology communities, and connects government clients with subject matter experts to aid in answering technical inquiries. He holds a B.S. in information systems from the University of Maryland, Baltimore County (UMBC), where he is also currently pursuing a master's degree in Cybersecurity. At UMBC, Mr. Sekiteri worked as a research assistant for its Department of Information Systems, supporting a research project recording emergency medical technician stress levels during interactive simulations.