# Decorative Front Cover of the Zero Trust Architecture Solicitation Reference for Procurement of ZTA Related Goods and Services

# **Solicitation Reference for Procurement of Zero Trust Architecture (ZTA) Related Goods and Services**

**READ FIRST**

*The language in this publication is intended to be used as sample language in a federal agency's own solicitation document (e.g., Statement of Objective (SOO), Statement of Work (SOW), Request for Information (RFI), etc.) for procurement of cybersecurity goods and services. This language casts a wide net across a set of broad Zero Trust umbrella expectations to assist agencies in the implementation and maturation of the federal zero trust strategy. It also includes requirements for Cyber Supply Chain Risk Management (C-SCRM). The agency’s working solicitation document should additionally include requirements specific to the product/service being procured through the specific solicitation mechanism.*

*The language is drawn from a range of government and industry resources about Zero Trust. It also includes requirements from relevant C-SCRM practices that impact cybersecurity procurement and implementation.*

*This template provides prompts, in <red text>, for agencies to input their specific information. While it provides information on generalized cybersecurity services, agencies should also make sure their solicitation contains their agency specific requirements and adheres to any agency specific procurement guidelines.*

**(SAMPLE SOLICITATION LANGUAGE IS IN RED)**

[DISCLAIMER: The language contained herein is just a sample of what can be used. There is no requirement or expectation that agencies use the same language in the solicitation.]

# **1.0 OVERVIEW AND BACKGROUND**

[Presidential Executive Order (EO) 14028](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/) and Office of Management and Budget (OMB) Memorandum M-22-09, [Federal Zero Trust Architecture Strategy](https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf) describe federal agency directives for achieving a set of standards, based on Zero Trust, by 2024.

Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, and risk-based verification across users and associated devices. Zero Trust advocates three core principles: All entities are untrusted by default, least privilege access is enforced, and comprehensive security monitoring is implemented.

Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (for both subject and device) are discrete functions performed before establishing a session to an enterprise resource no matter its location. Zero Trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. Zero Trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

The National Institute of Standards and Technology (NIST), a federal agency within the U.S. Department of Commerce has established and published federal standards for ZTA ([NIST Special Publication (SP) 800-207](https://csrc.nist.gov/publications/detail/sp/800-207/final)).

The Cybersecurity and Infrastructure Security Agency (CISA), which leads the nation’s effort to understand, manage, and reduce cybersecurity risk, has published the [Zero Trust Maturity Model (ZTMM) Version 2.0](https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf) to assist agencies in the development of Zero Trust strategies and implementation plans.

[EO 14028](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/) also directs federal agencies to enhance the software supply chain security. Accordingly, NIST has established [SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](https://csrc.nist.gov/pubs/sp/800/161/r1/final) and [NIST Internal Report (IR) 8276, Key Practices in Cyber Supply Chain Risk Management](https://csrc.nist.gov/pubs/ir/8276/final). C-SCRM is integrated into the Enterprise-wide Risk Management process.

GSA is mandated to ensure safety in federal procurement of software by following the NIST guidelines with given notice, instruction, and incorporating contractual language into every solicitation governing acquisition of cybersecurity solutions.

Vendors and suppliers seeking to provide cybersecurity solutions software products and services under any applicable GSA contracting program are required to demonstrate their readiness to comply with the EO 14028 and related federal mandates by adhering to federal regulatory authority, policy, and the GSA established guidelines and procedures in offering cybersecurity solutions to federal agencies for purchase.

<Insert agency name> <Describe organization and outline specific departments or systems included for this solicitation.>

# **2.0 OBJECTIVES**

<Insert specific objectives the agency is seeking to accomplish through this acquisition. See below for an example.>

The primary cybersecurity objectives for this acquisition for the <agency> are to assess its current state and maturity level, identify gaps and opportunities for improvement to safeguard the security and privacy of its mission related data, and be compliant with the requirements of EO 14028.

# **3.0 REFERENCES**

The offeror shall be familiar with Federal policies, program standards, and guidelines to include, but not limited to, those listed below or later versions as applicable:

| **REFERENCE** | **DESCRIPTION / TITLE** |
| --- | --- |
| **CISA** | *Zero Trust Maturity Model Version 2.0* |
| **EO 14028, May 12, 2021** | *Improving the Nation’s Cybersecurity* |
| **FISMA** | *Federal Information System Modernization Act (2014)* |
| **FIPS 199** | *Federal Information Processing Standards Publication (FIPS) 199 - Standards for Security Categorization of Federal Information and Information Systems* |
| **FIPS 200** | *Minimum Security Requirements for Federal Information and Information Systems* |
| **NIST SP 800-30 Rev 1** | *National Institute of Standards and Technology (NIST) Guide for Conducting Risk Assessments* |
| **NIST SP 800-35** | *Guide to Information Technology Security Services* |
| **NIST SP 800-37 Rev 2** | *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* |
| **NIST SP 800-39** | *Managing Information Security Risk: Organization, Mission, and Information System View* |
| **NIST SP 800-44 Version 2** | *Guidelines on Securing Public Web Servers* |
| **NIST SP 800-53 Rev 4** | *Security and Privacy Controls for Federal Information Systems and Organizations* |
| **NIST SP 800-53A Rev 4** | *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* |
| **NIST SP 800-61 Rev 2** | *Computer Security Incident Handling Guide* |
| **NIST SP 800-86** | *Guide to Integrating Forensic Techniques into Incident Response* |
| **NIST SP 800-115** | *Technical Guide to Information Security Testing and Assessment* |
| **NIST SP 800-128** | *Guide for Security-Focused Configuration Management of Information Systems* |
| **NIST SP 800-137** | *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* |
| **NIST SP 800-153** | *Guidelines for Securing Wireless Local Area Networks (WLANs)* |
| **NIST SP-800-160 Vol 1** | *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* |
| **NIST SP 800-161r1** | *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* |
| **NIST SP 800-171** **Rev 1** | *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* |
| **NIST SP 800-171A** | *Assessing Security Requirements for Controlled Unclassified Information* |
| **NIST SP 800-207** | *Zero Trust Architecture* |
| **P.L. 93-579** | *Public Law 93-579 Privacy Act, December 1974 (Privacy Act)* |
| **40 U.S.C. 11331** | *Responsibilities for Federal Information Systems Standards* |
| **OMB M-19-03** | *Office of Management and Budget (OMB) Memorandum 19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program* |
| **OMB M-22-09** | *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* |
| **OMB A-130** | *OMB Circular A-130, Managing Information as a Strategic Resource, July 2016* |
| **BOD 18-02** | *Department of Homeland Security’s Binding Operational Directive 18-02, Securing High Value Assets* |
| **NISTIR 8276** | *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* |
| **NISTIR 7622** | *Provides a wide array of practices that, when implemented, will help mitigate supply chain risk to federal information systems.* |
| **<Add as needed>** |  |

For any terms not explicitly defined, refer to the NIST Computer Security Resource Center (CSRC) Glossary (<https://csrc.nist.gov/glossary>).

# **4.0 REQUIREMENTS**

<Include product-specific requirements. Additionally, this section will include the sample language described in the following paragraph and the rest of this document.>

*General requirements:* All work associated with U.S. Federal Government information, systems, and information security must be compliant with the Federal Information Security Modernization Act (FISMA) of 2014 as implemented by Federal Information Processing Standards Publication 200 (FIPS 200), Minimum Security Requirements for Federal Information and Information Systems. This standard specifies minimum security requirements federal agencies must meet. The appropriate security controls and assurance requirements to be selected are described in the NIST SP 800-53 Rev 5, Security and Privacy Controls for Federal Information Systems and Organizations and associated documents. Specific impact levels required (per FIPS 200) for government information and information systems may vary and will be specified as requirements are identified.

If applicable, the work must also be compliant with the C-SCRM security controls as defined in the NIST SP 800-161r1 (APPENDIX A).

# **4.1 ADHERENCE TO THE FEDERAL ZERO TRUST TENETS:**

As stated in [NIST SP 800-207](https://doi.org/10.6028/NIST.SP.800-207), the offeror must demonstrate how the offering (including, but not limited to, the product or service as delivered plus all processes and infrastructure used to develop and support the offering) adheres to the following Federal Zero Trust tenets:

1. **All data sources and computing services are considered resources.** A network may be composed of multiple classes of devices. A network may also have small footprint devices that send data to aggregators/storage, software as a service (SaaS), systems sending instructions to actuators, and other functions. Also, an enterprise may decide to classify personally owned devices as resources if they can access enterprise-owned resources.

2. **All communication is secured regardless of network location.** Network location alone does not imply trust. Access requests from assets located on enterprise-owned network infrastructure (e.g., inside a legacy network perimeter) must meet the same security requirements as access requests and communication from any other non-enterprise-owned network.

3. **Access to individual enterprise resources is granted on a per-session basis.** Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task. This could mean only “sometime recently” for this particular transaction and may not occur directly before initiating a session or performing a transaction with a resource. However, authentication and authorization to one resource will not automatically grant access to a different resource.

4. **Access to resources is determined by dynamic policy**. An organization protects resources by defining what resources it has, who its members are (or ability to authenticate users from a federated community), and what access to resources those members need. For Zero Trust, client identity can include the user account (or service identity) and any associated attributes assigned by the enterprise to that account or artifacts to authenticate automated tasks.

5. **The enterprise monitors and measures the integrity and security posture of all owned and associated assets.** No asset is inherently trusted. The enterprise evaluates the security posture of the asset when evaluating a resource request. An enterprise implementing a ZTA should establish a Continuous Diagnostics and Mitigation (CDM) or similar system to monitor the state of devices and applications and should apply patches/fixes as needed.

6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.** This is a constant cycle of obtaining access, scanning, and assessing threats, adapting, and continually reevaluating trust in ongoing communication. An enterprise implementing a ZTA would be expected to have Identity, Credential, and Access Management (ICAM) and asset management systems in place.

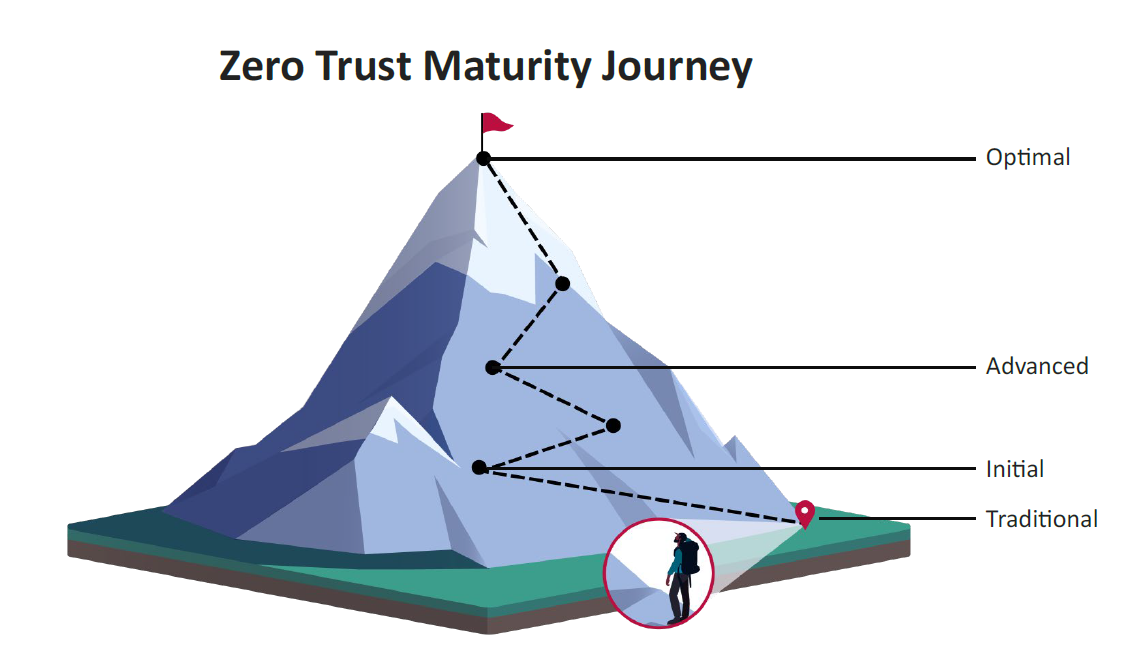
7. **The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.** An enterprise should collect data about asset security posture, network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects.

See [NIST SP 800-207](https://doi.org/10.6028/NIST.SP.800-207) for more details about these tenets.

# **4.2 ADVANCING THE AGENCY IN THE ZERO TRUST MATURITY MODEL**

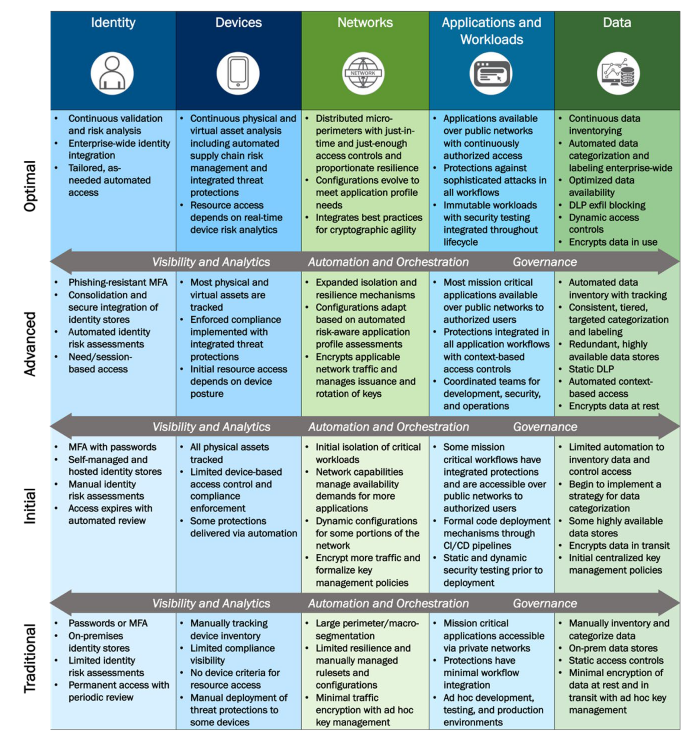
CISA’s ZTMM1 provides an approach to achieve continued modernization efforts related to zero trust within a rapidly evolving environment and technology landscape. This ZTMM is one of many paths an organization can take in designing and implementing their transition plan to a ZTA in accordance withEO 14028.

The offeror must demonstrate how the offering will assist the agency in the journey to the next maturity level (see Figure 1).



*Figure 1 Zero Trust Maturity Model (ZTMM)*

The offeror may use the following table (see Figure 2) as a guide to more fully demonstrate how the offering assists the agency to transition to the next maturity level.

[[](https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf#page=10)](https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf#page=10)*Figure 2 High-Level Zero Trust Maturity Model Overview*

Specifically, the offeror must demonstrate, as applicable, how the offering:

1. strengthens the agency’s posture in the identity pillar of the ZTMM and assists in the transition from the current maturity level to the next.
2. strengthens the agency’s posture in the device pillar of the ZTMM and assists in the transition from the current maturity level to the next.
3. strengthens the agency’s posture in the network pillar of the ZTMM and assists in the transition from the current maturity level to the next.
4. strengthens the agency’s posture in the applications and workload pillar of the ZTMM and assists in the transition from the current maturity level to the next.
5. strengthens the agency’s posture in the data pillar of the ZTMM and assists in the transition from the current maturity level to the next.
6. strengthens the agency’s posture in the cross-cutting capability of visibility and analytics.
7. strengthens the agency’s posture in the cross-cutting capability of automation and orchestration.
8. strengthens the agency’s posture in the cross-cutting capability of governance.
9. supports and enhances the cross-pillar coordination and maturity.

# **4.3 IMPLEMENTATION OF THE ZERO TRUST ARCHITECTURE (ZTA):**

The offeror must demonstrate how the offering will assist the agency in the implementation roadmap of ZTA ([NIST SP 800-207](https://doi.org/10.6028/NIST.SP.800-207)).

The offeror must demonstrate, as applicable:

1. how the offering supports the core logical components of a ZTA, namely the Policy Decision Point (PDP) and Policy Enforcement Points (PEPs).
2. how the offering supports implementing ZTA using the enhanced identity governance, specifically identifying the logical ZTA components.
3. how the offering supports implementing ZTA using micro-segmentation, specifically identifying the logical ZTA components.
4. how the offering supports implementing ZTA using network infrastructure and software-defined perimeter, specifically identifying the logical ZTA components.

Additionally, the offeror must demonstrate, as applicable, how the offering integrates with the following external systems, also known as Policy Information Points (PIPs):

1. CDM system
2. external threat intelligence feed(s)
3. external network and system activity logs
4. external data access Policy Engine (PE)
5. external ID management systems (e.g., LDAP server)
6. a Security Information and Event Management (SIEM) system
7. Federal Public-key Infrastructure (PKI) system and a global certificate authority system based on the X.509 standard

The offeror must demonstrate, as applicable:

1. that the offering embodies Zero Trust core principles and functionalities necessary to address multiple use cases and aid in the cultural and process changes Zero Trust adoption requires. The offering, if applicable, must integrate with third-party solutions — those the <agency> currently have in place — and vendors’ own standalone solutions through a unified approach. The offering should allow the agency to complete its Zero Trust implementation without the need for rip-and-replace of current investments.
2. its ability to reduce complexity of deployments and configuration management while enhancing user experience for auditing and reporting with customizable dashboards that consolidate events and logs.
3. how it supports the new norm of hybrid everything (workforce, workloads, and workplaces), enabled by continued cloud services adoption, expansion of BYO policies, deperimeterization of information systems, and the work-from-anywhere model.
4. the degree of the zero trust functionalities across multiple zero trust pillars, such as firewalls (networks), multi-factor authentication (people), and endpoint detection and response (devices) with centralized management and reporting, that are implemented natively and through partnership arrangement with other providers.
5. how the offering supports multiple Zero Trust domains in hybrid environments that span cloud and on-premises environments.
6. how it enables and supports the agency in managing complex technology environments with limited skills and budgets.
7. how it enables the support for complex environments consisting of a mix of legacy, on-premises technologies, cloud infrastructure, and SaaS.
8. how the offering has incorporated Artificial Intelligence (AI)/Machine Learning (ML) functionalities to automate network and security controls and reduce the complexity and necessary steps for managing and maintaining security controls in a dynamic organization.

This section may be amended from time to time with the current policy information points.

# **4.4 SUPPORTING CYBER SUPPLY CHAIN RISK MANAGEMENT:**

The NIST C-SCRM program has published guidelines and practices for federal agencies to manage the increasing risk of supply chain compromise related to cybersecurity. These include key practices for the agencies such as:

1. Know and manage critical suppliers
2. Closely collaborate with key suppliers
3. Include key suppliers in resilience and improvement activities

NIST has also published recommendations related to the key practices for agencies to establish and maintain a C-SCRM program. Several of these recommendations specify a role for suppliers as provided below:

1. Establish visibility into the suppliers’ production processes (e.g., capture defect rates, causes of failure, and testing)
2. Know if the data and infrastructure are accessible to suppliers’ sub-suppliers
3. Include key suppliers in incident response, business continuity, and disaster recovery plans and tests
4. Establish protocols for vulnerability disclosure and incident notification
5. Establish remediation acceptance criteria for the identified risks
6. Establish protocols for communications with external stakeholders during incidents
7. Collaborate on lessons learned, and update joint plans based on lessons learned
8. Use third-party assessments, site visits, and formal certification to assess critical suppliers

The offeror must demonstrate how it will support and fulfill its role vis-à-vis above key practices to strengthen the agency’s cybersecurity and Zero Trust journeys.

These requirements may be subsumed and superseded by the specific requirements imposed by the agency’s robust C-SCRM program.

ZTA drastically altered federal agencies' approach to implementing security controls and assessing their effectiveness. From the C-SCRM viewpoint, the suppliers play a crucial role in protecting mission-critical data and information systems throughout the enterprise. NIST SP 800-207 conveys the need for government agencies to have visibility into supplier security controls and risks that may impact the organizations through acquisitions. Thus, the suppliers should share their Cybersecurity Supply Chain Risk Information (C-SCRI) with the buying agencies so they can satisfactorily assess the risks (NIST SP 800-207).