Carnegie Mellon University
Software Engineering Institute

# SEI Zero Trust Industry Day

## Request for Information (RFI)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

The purpose of this RFI is to gather proposals for providing guidance to U.S. federal agencies that must transition to a zero trust (ZT) cybersecurity strategy to address the Office of Management and Budget Memorandum (OMB) OMB M-22-09 (Moving the US Government Toward Zero Trust Cybersecurity Principles), which calls out OMB M-21-31 (Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents) based on this scenario:

> *A large U.S. federal agency provides services used by global users. The agency currently is operating a hybrid, multi-cloud enterprise that supports about 45,000 federal employees and 15,000 contractors. The enterprise's networks break down into Information Technology (IT) (75%), Operational Technology (OT) (15%), and Supervisory Control and Data Acquisition (SCADA) (10%). The OT and SCADA networks support the agency's smart buildings' controls/operations and distribution centers.*
>
> *Currently, the agency has identified three high-value assets (HVAs): two legacy systems and one database containing Protected Personal Information (PPI). The agency is currently using four different identity and access management systems (Okta Identity Cloud, Cirrus Identity, Azure AD, and Google Cloud Identity) and lacks a centralized security operations center (SOC).*
>
> *The agency is currently unable to integrate logging information due to the continued use of legacy systems: an organizational structure where SOC operations are broken across different teams and a hybrid, multi-cloud implementation where services provide different formats for the information. The agency must implement two-factor authentication but also must provide multi-factor authentication (MFA) for some parts of the enterprise.*
>
> *The agency has a budget of $3 million and a one-year timeline during which it must start to address M-22-09. Given this last constraint, each proposal should address its compatibility with the agency's existing hardware and software infrastructure.*

You must address the following specific OMB M-22-09 requirements in your proposal:

1. Identity
   a. Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.
   b. Agencies must use strong MFA throughout the enterprise.

c. Agencies must enforce MFA at the network and application layers.

2. Devices
   a. Agencies must create reliable asset inventories through participation in the Cybersecurity and Infrastructure Security Agency's (CISA's) Continuous Diagnostics and Mitigation (CDM) program.
   b. Agencies must ensure their endpoint detection and response (EDR) tools meet CISA technical requirements and are widely deployed.

3. Networks
   a. Agencies must develop a zero-trust architecture (ZTA) plan that describes the agency's approach to environmental isolation (in consultation with CISA) and submit it to OMB as part of its ZT implementation plan.

4. Data
   a. Agencies must implement initial automation of data categorization and security response, focusing on tagging and managing access to sensitive documents.
   b. Agencies must work with CISA to implement comprehensive logging and information-sharing capabilities, as described in OMB M-21-31 where the advanced level would be needed to support ZTA tenets.

We recommend that you produce and discuss the following artifacts and information in your presentation:

1. Cybersecurity architecture strategy to implement ZT
   a. How ZT tenets are prioritized based on requirements and impact to agency
   b. Considerations
      i. Support for a mixed environment or not for hardware (i.e., multiple vendor products)
      ii. Software interoperability
      iii. Impact on data management

2. Two ZT roadmaps: one near-term (0-2 years) and one long term (3-5 years)
   a. Addresses OMB M-22-09 and M-21-31, the CISA Maturity Model, CISA Trusted Internet Connection (TIC) 3.0 guidance, and the CISA Cloud Security Technical Reference Architecture

3. ZT implementation plan
   a. Identifies the assumptions and constraints the agency faces
   b. Identifies how the ZT roadmap would be implemented
   c. Addresses and prioritizes the risks the agency faces to implement its strategy and roadmap
   d. Discusses the impact to the agency's organizational and financial planning
   e. Includes how application programming interfaces (APIs), agents, and cloud services will be used

4. Impact on the organization's training needs
    a. What training is needed to implement the proposal by addressing both the technical staff and the users?
    b. Specific technical staff question: After receiving the required training, how long will it take a trained novice/apprentice network technician to become proficient in the effective installation, configuration, and operation of this proposed solution?
    c. Specific user question: How much training will a user need to be able to support the anticipated changes (virtual private network [VPN], bring your own device [BYOD], installation of agents, etc.)?

5. Total cost of operation
    a. Procurement and implementation costs
    b. Ongoing support and maintenance costs
    c. Proposed staffing plan that identifies the number and required expertise level for the operators of the proposed solution
    d. Potential for cost savings

6. User interface/user experience
    a. How will users be impacted by your proposal?

7. Transferability to other agencies
    a. How might your proposal change if it were applied to a small or medium-sized agency?

During the ZT Industry Day, each organization will provide a presentation that addresses the scenario and share the information it has developed from the recommended artifacts.

After the ZT Industry Day, the SEI will develop white papers that will cover the following:

1. documentation of the event

2. highlights of best practices for organizations to consider when transitioning to a ZT cybersecurity strategy

3. ZT cybersecurity areas of research

Please sign and return the *Authorization to Use Materials and Contributions* form.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.



DM22-0650