PSC PROFESSIONAL SERVICES COUNCIL

U.S. Office of Management and Budget
725 17th Street, NW
Washington, DC 20503
https://zerotrust.cyber.gov/

September 22, 2021

RE: Comments on "Moving the U.S. Government Towards Zero Trust Cybersecurity Principles"

On behalf of the Professional Services Council (PSC)[1], I am pleased to submit comments in response to the Office of Management and Budget's (OMB's) September 8 notice related to a draft strategy document titled *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles.* The draft document provides strategic guidance for U.S. Government (USG) departments and agencies containing baseline expectations for their migrations to a zero trust architecture and in support of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, signed by President Biden on May 12, 2021.

As the leading trade association of companies providing information technology (IT) and professional services for the federal government, PSC often emphasizes the importance of cybersecurity guidance that is both improved and standardized across government networks. Government-wide use of a zero trust architecture, as outlined in the aforementioned EO, partially addresses both of these elements.

Thus, PSC supports the application of the expertise of the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency in cybersecurity and IT infrastructure protection for this requirement, as well as for the overall shift to a zero trust architecture that considers agencies' individual needs while promulgating a system of standardized cybersecurity requirements. Further, PSC appreciates the opportunity to comment on key documents, like the statement of zero trust cybersecurity principles, and highlights the need for additional information in several areas within this effort. These areas include:

1) **Burdening Existing Applications (Software);**
2) **Identity Management / Segmentation of Networks;**
3) **Funding;**
4) **Device Management;**
5) **Potential Updates to the Federal Information Security Modernization Act; and**
6) **Harmonization of Federal Cybersecurity Approaches.**

[1] PSC is the voice of the government technology and professional services industry, representing the full range and diversity of the government services sector. As a trusted industry leader on legislative and regulatory issues related to government acquisition, business and technology, PSC helps build consensus between government and industry. Our 400 member companies represent small, medium, and large businesses that provide federal agencies with services of all kinds, including information technology, engineering, logistics, facilities management, operations and maintenance, consulting, international development, scientific, social, environmental services, and more. Together, the trade association's members employ hundreds of thousands of Americans in all 50 states.

Observations/Recommendations and Discussion

Area 1) Burdening Existing Applications (Software).

Observation/Recommendation: U.S. Government (USG) departments and agencies, and the government contractor companies implementing zero trust in partnership with the USG, will need specific, standardized guidance for networked applications whose owners may, or may not, allow interference of applications connected within networks.

Discussion: A core challenge with a zero trust architecture and existing applications is implementing custom interferences. Application owners typically build-in custom interferences (e.g., patches, content). However, requiring a zero trust architecture without guidance on such interferences may leave existing applications, especially those that are older or less modularly designed, less functional without inputs from the application owner. Neither EO 14028 nor the *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles* strategy document provide specific guidance to departments, agencies, and contractor companies to ensure systems using common applications allow interference connected within networks or have replacement systems available / in budget.

Further, application owners inside and outside of the USG will need guidance on how to provide for custom interferences while maintaining automation in an existing application. Without guidance on funding for application redesigns, contractor or USG application owners themselves may not have the funds or incentives to modify custom interference for existing applications operating in the USG.

Area 2) Identity Management / Segmentation of Networks.

Observation/Recommendation: Specific guidance where automated machine-machine verification can be implemented, and where personnel would be required to intervene in chains, is essential to maintaining productivity and continuity with USG and industry networks.

Discussion: Operating within a zero trust network will require connected systems across the government to establish segmentation between or among bureaus, agencies, and departments which, absent guidance for automated authentication, could reduce productivity and efforts toward cloud-based computing and edge-processing. Moving to a zero trust architecture without specific guidance on human versus automated authentication in systems and applications adds an extra level of uncertainty to existing integrated systems.

OMB or CISA guidance on automated multi-factor authentication without human intervention would minimize related uncertainty and potential loss of productivity.

Area 3) Funding.

Observation/Recommendation: Specifically, guidance on long-term funding will help ensure the migrations can occur seamlessly (i.e., without undesirable disruptions in operations and services) in accordance with the fiscal year 2024 (FY2024) goal.

Discussion: Although the strategy document recommends "seek[ing] funding from alternative sources" or "re-prioritiz[ing] funding," those sources will be unable to account for complete system overhauls and potential redesigning of extensively integrated applications. Without specific funding guidance, agencies and departments may find themselves cutting costs across the board, potentially impacting productivity. Specific funding for zero trust capabilities would help ensure that this initiative meets the FY2024 goal.

A government-wide migration to a zero trust architecture will be costly both in dollars and time. Transitioning agency applications to a zero trust environment instead of leveraging role-based access controls will require a level of funding, contracting, work, and time that USG must account for over a sustained, long-term effort with appropriate funding.

Area 4) Device Management.

Observation/Recommendation: Implementing a zero trust model that applies to shared and / or personal devices will require OMB guidance. Currently, without such guidance, devices may be able to comply with zero trust principles.

Discussion: In light of communications protocols, requirements, and properties of personal and "take home" devices, implementation of any zero trust strategy should address those challenges associated with inventory management. Increases in tele- and remote-work have underscored the need for USG departments and agencies to adapt support for a greater variety of device types and properties. These devices may also have their own technical challenges in complying with zero trust-related principles and policies—e.g., remote access through the cloud or an external partner / provider.

OMB should consider ways in which to address these differences early within the zero trust strategy. More specifically, clear OMB guidance on ownership of inventoried devices—and agency and user responsibilities—is needed. Devices will need further authorizations and protocols with shared inventories to function properly within a zero trust architecture.

Area 5) Potential Updates to Federal Information Security Modernization Act of 2002.

Observation/Recommendation: Numerous cybersecurity events since 2014 provide a reasonable rationale for updates to the *Federal Information Security Modernization Act of 2002* (FISMA; Public Law 107-347), as well as potential updates to other technology-related legislation, in an effort to bring structures, roles, and requirements in line with a strategy to implement a zero trust architecture.

Discussion: In addition to FISMA, the U.S. Congress passed in 2018 the *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act* (SECURE Technology Act; Public Law 115-390). One of the most important elements of this 2018 law is Title II, the Federal Acquisition Supply Chain Security Act of 2018, which amended Title 41 of the U.S. Code and created the Federal Acquisition Security Council (FASC).

One might reasonably wonder whether recent cybersecurity events argue for improvements or amendments to FISMA, the SECURE Technology Act, or both. Questions for OMB's consideration include the role of Chief Technology Officers (CTOs) in efforts to implement a zero trust architecture and whether CTOs' roles should be standardized across government. (Note: PSC explored these questions in 2016, recommending that the U.S. CTO be located within OMB alongside the U.S. Chief Information Officer and U.S. Chief Information Security Officer.) Questions also include the role of the FASC going forward.

Area 6) Harmonization of Federal Cybersecurity Approaches.

Observation/Recommendation: Recognizing national security and programmatic implications of recent cybersecurity events, the Federal Acquisition Regulations (FAR) include provisions on controlled unclassified information (CUI), assessment score management in the Supplier Performance Risk System (SPRS), and other key areas of importance to contractor companies that support federal agencies. Harmonizing, and streamlining where appropriate, of these regulations is key to reducing conflicts and confusion among the many agency approaches to cybersecurity.

Discussion: Not surprisingly, federal contractors are making their own budgetary, strategic planning, and resource allocation decisions—but they are currently doing so with no firm knowledge of the status of cybersecurity policy implementation at large departments (e.g., Department of Defense) or any plans to allow reciprocity of these policies across agencies. Further, individual agencies continue to develop and promulgate cybersecurity requirements, compounding this uncertainty. It remains unclear how government-wide requirements will align with those already required by agencies.

By requesting comments on a draft strategy document, the USG has indicated a desire to pursue zero trust architecture with some urgency. Toward that end, harmonization of applicable regulations to the maximum extent practicable within the relevant FAR and DFARS is ke, to adopting an outcomes-focused approach to information risk management, as are framework reciprocity and standardized performance metrics. Accord across agencies and at program levels will strengthen our nation's defenses and avoid divergence of national security, critical infrastructure, and civilian security. Ultimately, the harmonization of existing and future directives will move the USG closer toward coherent information and cybersecurity risk management.

Conclusion

We at PSC commend OMB for developing and publishing a draft strategy document such as *Moving the U.S. Government Towards a Zero Trust Cybersecurity Principles* and for requesting public comments. We support the intent to move toward a more holistic, government-wide

approach to federal cybersecurity policies, standards, and requirements and a continued commitment to development of a coherent strategy. We emphasize the need for guidance and planning early in this process, especially as these elements pertain to key points mentioned above. Without clear expectations and funding, departments, agencies, and contractors who support the federal government will struggle to meet zero trust requirements while maintaining current or targeted levels of services and cybersecurity.

PSC looks forward to working with the Department in its approach to EO 14028 implementation and appreciates the opportunity to submit comments. If you have any questions, please contact me at (703) 875-8059 or kostro@pscouncil.org.

Sincerely,

Stephanie Sanok Kostro

Stephanie Sanok Kostro
Executive Vice President for Policy