ITI Promoting Innovation Worldwide

Office of the Federal Chief Information Officer
Office of Management and Budget
Executive Office of the President
New Executive Office Building (NEOB)
725 17th St NW
Washington DC, 20006

Re: Call for public comments on the Federal Zero Trust Strategy

September 21, 2021

The Information Technology Industry Council (ITI) appreciates the opportunity to provide feedback on the recent publication of OMB's Federal Zero Trust Strategy. ITI is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

We appreciate the persistent effort from OMB and the Biden Administration to improve our nation's cybersecurity in the face of relentless threats. We commend the administration for embracing a coordinated and whole-of-government approach to cybersecurity risk management. Specifically, we would like to call out OMB's outstanding work to implement Executive Order 14028 on Improving the Nation's Cybersecurity and the decision to partner with industry on this workstream. We welcome OMB's decision to invite industry feedback on the Federal Zero Trust Strategy ("the Strategy") and are committed to serving as a helpful resource to OMB.

We agree with OMB's objective to promote the intelligent and vigorous use of modern technology and security practices, while simultaneously avoiding disruption by malicious cyber campaigns. The Strategy will provide actionable guidance to agencies as they are undergoing a major paradigm shift. Given the criticality of the subject matter, we encourage OMB to keep involving relevant stakeholders in the drafting of such guidance. We remain committed to sharing our experience and lessons learned to help streamlining the federal adoption of Zero Trust (ZT). To support agencies' migration to a Zero Trust Architecture (ZTA), we respectfully suggest the following recommendations for your consideration.

Align the targeted end-state to use cases rather than technology silos. The Strategy rightfully acknowledges that the Federal Government can no longer depend on perimeter-based defenses to protect critical systems and data. The transition to Zero Trust is an important, yet highly complex undertaking. For agencies to effectively adopt Zero Trust, it will be critical for them to understand the horizontal relationships across security segments. In its current form, the document appears to perpetuate the concept of security silos, addressing challenges in context solely to areas of functional capability (e.g., identity, data, devices). We believe that operational use cases can produce meaningful insights that bridge traditional scenarios and highlight policy, technology, and organizational gaps.

While flexibility in adoption is needed to account for agencies' unique needs, the current level of ambiguity around a silo-based approach could result in sub-optimal and divergent end-states. For example, one agency may adopt an identity-management approach to ZTA while another may assign greater importance to hardware, software, or data management. To achieve the strategy's objective of establishing a common roadmap, the administration should further refine the baseline, expand on what it wants an integrated end-state to look like, and align the target to use cases. Greater clarity around a comprehensive approach to zero trust will help agencies refine their approach across people/devices (workforce), applications/data (workload), and assets (workplace). Minimally, an emphasis on tight linkage between users and devices, and their role in approving authentication, should be defined. Further, the strategic plan should explicitly detail instructions on securing critical infrastructure and Internet of Things (IoT) devices while maintaining consistency with other security requirements developed in this space, for instance by the National Institute of Standards and Technology (NIST).

For example, a use case could focus on putting Zero Trust into action to reduce the risk of insider threat. Agencies will need to identify risks and automate responses across Identity (ID theft, privilege account misuse), Devices (compromised/stolen devices, malware, phishing), Applications and Data (data exfiltration, PII data lead). Another use case could highlight data flows across mission and/or business contexts. An agency may wish to share data externally that have been integrated from multiple sources. Such data may flow from edge collection to internal agency data centers or private clouds, and then to commercial cloud service providers (CSPs), and ultimately across CSP networks. This use case requires an effective Zero Trust strategy delineating data rights policy, network management and identity and access management. Incorporating such operational use cases will yield better outcomes and promote best practices to the maximum extent practicable. It also accelerates the adoption of emerging technology solutions and provides consistency with the approach taken in CISA's Cloud Security Technical Reference Architecture.

Expand guidance on prioritization during incremental roll out. We appreciate that OMB gives agencies sufficient time to advance on their ZTA journey. In addition to time, agencies require prioritization guidance to efficiently structure their migration to a Zero Trust Architecture. This will account for agencies' various maturity levels and the fact that ZTA migration is not a wholesale replacement of infrastructure. We encourage OMB to provide guidance on how agencies should prioritize ZTA use cases with respect to other identified priorities, such as High Value Assets (HVAs) and priority data assets identified per the Federal Data Strategy. OMB may also consider linking this guidance to known threats, existing high-risk vulnerabilities, and targeted asset classes (people, software layers, applications, devices, IoT, etc.) to have a more impactful initial response.

Moreover, we believe that administrators would benefit from an actionable roadmap of security capabilities along with guidance on how to integrate them as part of a ZTA. The *ZTA Deployment Cycle* contained in Section 7.3 of SP 800-207[1] could provide a helpful start. It identifies four ZTA implementation phases (Assessment; Risk Assessment/Policy Development; Deployment; and Operations) and maps them to the corresponding Steps in the NIST Risk Management Framework.

Involve agency leadership in ZTA migration. We endorse the Strategy's intended goal of managing agency risk holistically and involving senior leadership in the agency's ZTA migration. Zero Trust changes will impact agency processes and employee engagement at all levels. Administrators need to support the IT and Security teams by engaging in oversight committees and similar leadership fora. This will enable them to anticipate and lead the cultural changes that will occur. NIST recently released a draft ZT Starting Guide for Administrators[2] that introduces administrators to foundational ZT concepts. We encourage OMB to bolster the section on intra-agency collaboration by referring agency administrators to NIST's Starting Guide once the final version becomes available.[3] OMB should also consider providing agencies with sample governance structures that consist of agency leadership, not just IT and Security leadership. Endorsing the cultural changes at the executive level will go a long way of generating the buy-in that is needed to fully embrace ZT tenets throughout the organization.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[2] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf

[3] You can read ITI's comments on the draft here: https://iticdc.sharepoint.com/:b:/s/CyberEO/EY1VKSrBRNNGrpvkrlI2R0ABM_NEqY7ZGu2FeDhYZl4lYQ?e=WXW57H

Build out Data guidance to improve risk management. We agree with the importance of data for ZT and risk management in general. In its current form, the Data guidance focuses primarily on responsive activities such as auditing, logging, and incident response. While all these activities are important and generate valuable insights, we believe they are insufficient for comprehensive data risk management. Particularly as agencies move to share data assets as enterprise services, it is essential that they work more proactively to manage those most sensitive items. Likewise, agency CDOs and CISOs need to collaborate closely on designing internal processes with data security in mind. We encourage OMB to build out the Data section to include guidance on data classification and tagging. We believe that the detailed changes proposed in Appendix A will equip agencies with the tools they need to conduct meaningful risk assessments.

Build out Identity section to give more guidance on attributes for policy engines. OMB should clarify which attributes should be used to allow for authorization at time of access request and establish common policies for use across agencies. Agencies should consider Attribute-Based-Access-Control (ABAC) in their Zero Trust migration. To enforce the core Zero Trust principle of least privilege, agencies must regularly certify identity attributes, the associated accesses, as well as the underlying systems themselves. This will reduce the overall attack surface by ensuring that end users have only enough privileges to do their job, and no more. Simultaneously, it enables increased visibility across the attack surface. This should be a minimum requirement. While authorization is not explicitly part of Zero Trust principles, it is important to consider the role of identity management in provisioning access to data and workloads within an application and should be explicitly defined in the strategic plan.

Expand on the authentication guidance in the Identity section to include risk-based, dynamic access controls. The memorandum is quite robust in its guidance on using phishing-resistant multi-factor authentication (MFA) and enterprise SSO to be implemented at the application layer. However, it does not address the capability of using the full scope of contextual data for access control decisions that is inherent in dynamic, risk-based access control mechanisms. Risk-based authentication, such as WebAuthN, can verify the context of an individual during a user access attempt and can 'step up' authentication to include additional assurances when users attempt to access sensitive data, or data categorized at a higher level of risk. As a security best practice, all data pertaining to user identities, cookies, and other derived credentials should be protected using end-to-end encryption.

An important part of Identity in a Zero Trust context is to bring the verification and authorization of the user identity as close to the requested access transaction as possible. This can help enforce the ZT tenet of least privilege. The authorization can be dynamically escalated to include additional authentication factors commensurate to the risk assessment results. For example, if the user is requesting access from an unrecognized IP, at a time or geolocation that is untypical for that user, or within the context of any known set of typical user behavior, authentication should be stepped up to require additional verification in real time. Phishing-resistant MFA is important and dynamic, risk-based authentication should be used as a complement to MFA for the highest sensitivity of access, such as for privileged users accessing critical agency assets.

Encourage agencies to consolidate and secure identity systems. OMB appropriately advocates for agencies to formalize their participation in the Continuous Diagnostics and Mitigation (CDM) program. This will help to improve agencies' situational awareness as well as their inventorying of devices and assets that connect to their network. We encourage OMB to further build out the Identity guidance to drive the consolidation of agency identity systems. Moreover, we encourage OMB to reiterate the importance of applying zero trust principles to systems that manage user identities and privileges. For example, OMB could promote the CDM Master User Record as a central agency repository of all agency user identities. The CDM Master User Record equips agencies with the centralized identity management data and tools that they need to begin to consolidate identity systems and implement the protections required by this memorandum.

Expand guidance on the EDR information-sharing that agencies will need to participate in with CISA. The memorandum appropriately mandates that agencies must provide CISA with ongoing access to the agency's endpoint detection and response (EDR) data. Yet, the Devices guidance falls short of defining the parameters for this information sharing. For example, the memorandum does not mandate a timeline (from the date of memorandum) that agencies will be required to start sharing this EDR data with CISA. Neither does it explicitly indicate that CISA will define the terms of the information-sharing mechanism. To ensure a comprehensive view of all assets and the vulnerabilities that exist on those assets, agencies should deploy a vulnerability management platform for continuous assessment and auditing of assets and connected devices. Finally, the guidance should encourage agencies to quickly move beyond current endpoint detection technologies and into next generation solutions that provide extended integration of more actionable data across networks. With such guidance readily available, agencies will not have to arbitrarily devise their own parameters for information-sharing, such as what EDR data they will share or how frequently. Many agencies may categorize their EDR data as sensitive and may object to a mandate that is loosely stated without indication that proper elaboration will be forthcoming from CISA.

Expand guidance on hybrid and BYOD work environments. The future of work will rely heavily on remote and hybrid work environments – a change that the US government is already undergoing. Agencies have recognized this and adopted policies that provide the required structure and tools for these work environments. Yet, the strategy in its current form remains silent on how to build a ZTA in work environments with hybrid or bring-your-own-device (BYOD) policies.

Constraints on agency budgets may limit additional deployment of technology for home use, which, absent strictures to the contrary, will naturally lead them to rely on employees accessing agency resources from personally owned devices—e.g., phones, tablets, and computers. Any agency's Zero Trust Architecture needs to take this reality into consideration, to ensure robust on-device security. Commercial best-in-class products offer a broad range of technical solutions that the implementing agency may wish to consider. Samples include confidential computing, network micro-segmentation/isolation, enhanced edge computing, software-defined WAN to eliminate the burdensome network performance and weak cybersecurity of back-hauling data over the traditional VPN to cloud-hosted agency applications, on-device hardware-enhancing security/threat detection, security update manageability, virtual desktop infrastructure (VDI), and sandboxing solutions for business and private data. The employee needs to understand that these solutions will require specific configurations. If BYOD is used, employees may be required to consent to giving up some of the control over their personal device in exchange for working from a personal device.

OMB should also encourage agencies to assess the full range of options from a cost and risk management standpoint. For example, the initial budgetary outlays will need to be considered as part of the hybrid/BYOD working model. Tradeoffs will occur, such as procuring new devices rather than allowing BYOD, or investing in suitable technical countermeasures to secure personal devices in a BYOD environment.

Retain expanded encryption requirement. We endorse OMB's decision to expand support for encryption on government networks. Industry recognizes the importance of encryption, specifically end-to-end encryption, as a general security best practice. If present, advanced persistent threats will eventually exploit any tool that provides law enforcement with access to encrypted data. OMB can remove this vulnerability from its systems by requiring end-to-end encryption and can help with the adoption of end-to-end encryption by clarifying guidance on the use of different architectures, including hardware solutions when appropriate. Concurrently, we support the notion that metadata collection and anomaly analysis can be a primary means of protection and threat detection.

Reflect mandates in agency budgets. We support the administration's coordinated and whole-of-government approach to cybersecurity risk management and appreciate the complexity of the undertaking. Because of its complexity, we suspect that the ZTA adoption mandate will present budgetary challenges for many federal agencies. While the memorandum calls on agencies to submit budget estimates for FY23-24, agencies may struggle to absorb the costs for FY22 through rebalancing alone. The outlays for FY22 will likely be disproportionally higher as agencies lay the foundation for security improvements.

For example, OMB Memorandum M-21-31[4] directs agencies to achieve EL1 by the end of FY22. Building this foundational capability will possibly be as resource intensive as the subsequent scale up. Agencies will have to make these investments now, through internal re-prioritization of skilled personnel, to produce the desired outcomes by FY23-24. We suggest that OMB consider tagging agency investments within a Technology Business Management breakout category and include that requirement in their Capital Planning and Investment Control (CPIC) guidance to Agencies.

Admittedly, the Federal Strategy does mention alternative resources like the Technology Modernization Fund (TMF). However, the TMF proposal deadline for FY22 has already passed and there is a significant project backlog that may prevent agencies from accessing these funds. Further, even with budget estimates for FY23-24, there is no guarantee that these budgets will be authorized and appropriated. Because we agree with the objectives of EO 14028 and the Federal ZT Strategy, we urge OMB to provide sufficient funding for the cybersecurity requirements contained therein.

Thank you for your consideration of our comments. ITI looks forward to serving as a resource representing the technology industry perspective to OMB as it continues the important work of improving the nation's cybersecurity posture. If you have any questions or would like to discuss our comments in greater depth, please contact Leopold Wildenauer (lwildenauer@itic.org).

Respectfully submitted,

Gordon Bitko

Gordon Bitko
Senior Vice President of Policy, Public Sector
Information Technology Industry Council (ITI)

[4] https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

Appendix A - Comments and Recommendations

Section E. Data, page 19 of Federal Zero Trust Strategy Draft dated September 7, 2021

#	Strategy Section	Strategy Text	Comment / Recommendation
1	Data / Vision (paragraph 1)	Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies take advantage of cloud security services and tools to discover, classify, and protect their sensitive data, and have implemented enterprise-wide logging and information sharing.	Recommend expanding the sentence to include "protect their sensitive content and data" as industry delineates the difference between data and content. Content (i.e, PDF, MS Word, Excel, PowerPoint, etc.) is contextualized data. Context situates data within a system of values, concepts, and utterances. Content has also been defined as a High Value Assets (HVA).
2	Data / Actions #3	Agencies must audit access to any data encrypted at rest in commercial cloud infrastructure.	Some security compliance frameworks state that data encryption should happen at rest and in motion. Yet all encryption methods aren't equal. Technology decision-makers must evaluate each approach against the threat models for the environments they manage. For instance, whole-disk encryption defends against physical theft of the drive. Moving up the stack to network protection measures like Secure Sockets Layer (SSL), Transport Layer Security (TLS), or virtual private networking (VPN) also can pose potential issues. Data is encrypted at one end, only to be decrypted at the other end and could be exposed to unauthorized activities. Application security measures like transparent encryption in the database are potentially prone to Structured Query Language (SQL) injection attacks and application exploits to access information.
3	Data / 1. Federal Data Security Strategy (para 2)	Agencies must not only develop protections for the packaged datasets they store in databases or publish online, but must also grapple with more loosely structured and dispersed data systems (such as email and document collaboration) and intermediate datasets which exist principally to support the	Recommend expanding the sentence to include "dispersed data systems across cloud and on-premise environments."

		maintenance of other primary datasets.	
4	Data / 2. Automating Security Responses (para 6)	For example, an agency which uses a standard template for procurement-sensitive documents could attempt to detect when this template is in use. An agency could monitor for potentially excessive sharing of this document when shared via collaboration tools or sent through email. Depending on the characteristics of a document and the features in an agency's collaboration suite, an agency could potentially automate the restriction of permissions around viewing this document.	The government may want to consider simplifying this example by using the term "file" instead of template. To ensure consistency between this strategy and the Cloud Security Technical Reference Architecture the government may want to pick an example using digital rights management or another technology. For example, technology such as digital rights management provides server-side policy control that allows tracking and access changes to distributed content and documents. Using a policy to protect a file would give an organization's ongoing control over that file, even after the file is distributed, which is a critical piece to Zero Trust Architectures. Organizations can audit events to track who, when, where and how recipients are using your file. Organizations can prevent users from continuing to access the file and change the policy that is attached to the file.
5	Data / 3. Auditing access to the sensitive data in the cloud (para 1)	EO 14028 calls for agencies to use encryption to protect data at rest. Encryption at rest can protect data that is copied while at rest, but does not protect against access by compromised system components that are authorized to decrypt data. However, cloud-based infrastructure providers now offer a wide variety of services that support cloud-managed encryption and decryption operations, with their own associated logs.	In order for a system to enforce Zero Trust principles down to the content/data level, the following are mandatory: • **Persistent protection:** This can be thought of as firewalls for your data, content, & documents. Since documents are widely distributed, this needs to be provided by encryption at the file format level. This means that the file stays more secure, regardless of whether it's at rest or in transport in cloud or on-premise environments. • **Integration with the Control Plane for dynamic authorization decisions:** The system must be able to enforce the Control Plane's dynamic authorizations to content, data, documents, like an PDF, or Microsoft Word, Excel, and PowerPoint, already distributed, regardless of their location. For example, documents moved to a USB drive must still enforce dynamic authorizations. Note: these decisions are based on the attributes made available to the Control Plane (ABAC: Attribute-Based Access Control) via the

			viewing client and other contributing systems. • **Real-time streaming of content and document interactions to the Control Plane:** Streaming data document interactions back to the Control Plane in real time provides much-needed intelligence for risk/trust decisions. For instance, what time and from where did an employee print that document? Did they read the last page? Or copy content from the document? With these requirements met, Zero Trust is available at the data level. This provides powerful new mitigations against potential attacks. For example, giving access to a document by a user from their normal location during typical working hours would be granted, but access from a new location at different working hours might initiate an out-of-band authentication (phone call, mobile phone push request, etc.) before granting access.
6	Data / 3. Auditing access to the sensitive data in the cloud (para 3)	When agencies encrypt data at rest in the cloud, agencies must use independently operated key management tools to create a trustworthy audit log of access to that data. This can be achieved by using key management tools operated by the cloud provider, or by key management tools that are on-premise or otherwise external to the agency-controlled cloud environment. In either case, access to key management tools and their audit logs must be isolated from the applications whose activity is being logged. This requirement does not apply to data encrypted in on-premise environments because they do not consistently have third-party components available whose trustworthiness could be relied upon in the event of a total agency compromise.	Based on experience and industry best practices, industry would also recommend implementing a separation of duties to mitigate any chokepoints of one person having access to encrypted content, keys, policies, and monitoring.