ITI Promoting Innovation Worldwide

Eric Goldstein
Executive Assistant Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380

October 1, 2021

Dear Mr. Goldstein,

The Information Technology Industry Council (ITI) appreciates the opportunity to provide feedback on the recent publication of three strategic and technical guidance documents focusing on zero trust. 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 the Biden Administration to improve our nation's cybersecurity in the face of relentless threats. We agree with the overall objectives of Executive Order 14028 and commend the administration for embracing a coordinated and whole-of-government approach to cybersecurity risk management. The requirements pursuant to Section 3 will advance a common security baseline across the federal government by linking the modernization of government IT to cybersecurity, specifically zero trust. We appreciate the recent publication of three important strategic and technical guidance documents, namely OMB's Federal Zero Trust Strategy, CISA's Zero Trust Maturity Model (ZTMM), and CISA's Cloud Security Technical Reference Architecture (Cloud Security TRA). We welcome the inclusion of stakeholder feedback in the drafting process and respectfully offer the comments below for your consideration.

Observations on interplay of the three documents

We appreciate that CISA and OMB decided to publish the three documents concurrently. This accurately reflects the interlinkages and interdependencies between these three documents. It is critical that CISA and OMB maintain their close collaboration. All changes to any of these documents should be discussed in the interagency and appropriately reflected in the remaining documents. As CISA and OMB revise the initial drafts, we would like to offer the following recommendations to further align and strengthen the three documents.

Align the targeted end-state to use cases rather than technology silos. In a dynamic threat environment, 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 their current form, the Federal Strategy and the ZTMM appear 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 like those included in the Cloud Security TRA, 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 establish a coherent roadmap, we encourage CISA to work with OMB to define a mutual baseline, expand on what an integrated end-state should look like, and align the target to use cases. Minimally, the final guidance should emphasize the tight linkage between users and devices, and their role in approving authentication. Further, the end state should extend beyond a static/binary one-time technology implementation and promote an ongoing process of using risk-based policies to apply security controls to assets and resources that are dynamic, resilient, continuously monitored and updated. The final guidance should also 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, capturing north/south and east/west network flows while providing distributed security services (firewall and intrusion detection/prevention) to optimize data flows. 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 throughout all three documents will yield better outcomes and promote best practices to the maximum extent practicable. It also accelerates the adoption of emerging technology solutions.

Include guidance on migration to hybrid cloud environments. Agencies will not migrate all systems to the cloud immediately. Agencies will likely operate hybrid models with on-prem, private cloud, and commercial cloud systems for an extended period of time, perhaps even indefinitely. None of the three documents currently addresses this reality. This lack of guidance does not align well with agencies' fiscal realities, their need to prioritize resources, their risk posture of systems, or the potential cost of upgrading legacy systems. The Cloud Security TRA, in particular, would be strengthened by considerations of this possibility, for example in the contexts of consolidating and managing user identities across hybrid systems and providing the same security policies while workloads move back and forth from on-prem to cloud resources.

Build out Data pillar 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 CISA and OMB to build out the Data pillar to include guidance about data classification and tagging to equip agencies with the tools they need to conduct meaningful risk assessments. We further encourage highlighting the pros and cons of different approaches to data security. For example, data-at-rest encryption provides a secure container but does not mitigate accidents or exfiltration for espionage because the content is no longer encrypted when it is removed from the container. In contrast, Data Rights Management (DRM) persistently protects content independent of storage and transport and enforces authentication, authorization, and auditing of that content, inside and outside of organizations.

Expand guidance on hybrid and BYOD work environments. The future of work will rely heavily on remote and hybrid work environments, a change the US government is already undergoing. Agencies have recognized this and adopted policies that provide the required structure and tools for these work environments. In their current form, none of the three documents discuss how to build a ZTA in work environments with hybrid or bring-your-own-device (BYOD) policies. 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 and Secure Access Service Edge (SASE) technology 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), which allows for quarantine of workloads when security anomalies occur, 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. CISA and OMB should clarify BYOD policies in federal agencies and how to ensure ZTA is incorporated.

Retain expanded encryption requirement. We endorse the 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 undermines encryption, including measures to provide law enforcement with access to encrypted data. OMB can address this vulnerability by requiring end-to-end encryption. Concurrently, we support the notion that metadata collection and anomaly analysis can be a primary means of protection and threat detection.

Address workforce concerns. None of the three documents address the issue of a significant shortage of a highly skilled workforce that is needed to implement the guidance and mandates pursuant to EO 14028 and related documents. This gap is not unique to government agencies as cloud security skills are in-demand globally. However, it is felt most acutely in the government as security clearances and IT certifications work against the long-term retention of qualified cloud security personnel within a given agency. Good guidance is a necessary first step, but most of the work rests with the implementation. Agencies do not have enough qualified people to effectively implement most of the guidance from the documents. We encourage agencies to consider the "total cost of ownership" as they build out their cloud security architecture. Some solutions may be easy to adopt within one account or a specific region but may not scale well to multiple accounts or regions. This has exacerbated the fragmentation of solutions across various federal agencies. Section 5 of the Technical Reference Architecture mentions this fragmentation challenge in passing but should be augmented to include a discussion of workforce issues. That language should also be aligned with the guidance provided in the Federal ZT strategy.

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 Federal ZT Strategy calls on agencies to submit budget estimates for FY23-24, agencies may struggle to absorb the costs for FY22 through internal re-prioritization

alone. The outlays for FY22 will likely be disproportionally higher as agencies lay the foundation for security improvements.

As agencies migrate to cloud-based environments and improve their ZTMM results, they will have to make investments now to produce the desired outcomes by FY23-24. Admittedly, the Federal Strategy does mention alternative resources like the Technology Modernization Fund (TMF) and the latest round of project funding did support zero trust projects at GSA, OPM, and the Department of Education. However, while the TMF can provide much needed funds to these selected projects, this option is no longer available for FY22. Consequently, agencies that are just getting started on their ZTA journey must look for alternative sources of funding. 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, we urge OMB to consult with CISA to estimate costs accurately and to provide sufficient funding for the cybersecurity requirements contained in EO 14028.

Comments on Cloud Security Technical Reference Architecture

We appreciate CISA's leadership in developing the Cloud Security Technical Reference Architecture (TRA). Particularly, we would like to commend CISA for including relevant stakeholders from industry, FedRAMP and USDS in the drafting process. The document is thorough in the breadth of subject matter that it covers. We encourage CISA to deepen the technical guidance where appropriate to empower agencies to convert concept into practical application. Additionally, the reader would benefit from understanding how this document relates to, complements, and/or enhances other cloud security guidelines, standards, and/or frameworks.

Expand operational FedRAMP guidance in Section 3. We agree with CISA's decision to spotlight GSA's Federal Risk and Authorization Management Program (FedRAMP) as a central piece of a secure federal cloud migration strategy. Dynamic cloud-based environments offer a strong baseline for agencies to build a ZTA and to develop more secure applications. Typically, agencies can expedite an ATO and ease the migration process when they identify the appropriate FedRAMP approval level for services in the cloud. Further, FedRAMP allows agencies to adopt a risk-based, rather than a 'check the box' compliance approach. In recognition of FedRAMP's importance, we encourage CISA to expand Section 3 of the TRA to provide additional guidance at the operational level on how applicable provisions of FedRAMP can support federal agencies in implementing ZTA.

Add data privacy as a challenge in Section 4.2.1. As data are moved within the scope of migration, an organization will necessarily need to comply with the privacy laws that govern where the data are sourced from, where the data are processed, and where the data are accessed, which could all be different in the case of cloud-based services. There

may also be local specific regulations that an organization may need to comply with regarding what constitutes data producers, processors, and consumers. As such, the TRA should acknowledge this as an additional challenge.

Discuss and rank additional cloud migration scenarios. The cloud migration scenarios in Section 4.3 provide insightful use cases that agencies may encounter. As agencies embark on their migration journey, they first must focus on getting the basics right before they move to more mature cyber practices. Commensurate with the agency's level of cyber maturity, the nature of the use case will change. For further improvement, we recommend starting out with simple use cases that lay the ZT groundwork and subsequently progressing into more complex/advanced concepts like application security, DevSecOps, and CI/CD use cases. CISA may also consider framing and ranking the scenarios in the context of the ZTMM.

Add a section on policy as code. Over the past year, cloud service providers (CSPs) have moved toward a rapid adoption of Policy as Code (PaC) to apply Cloud Security Posture Management at the earliest stage possible. CSPs offer many native features already and are working on deploying additional PaC features. All configuration settings relating to policy conformance should be automatable through code. As such, we encourage CISA to include a Section 4.X to define and distinguish PaC from infrastructure as code (IaC). IaC defines what will be deployed through automation and is typically written from the developer perspective. PaC, on the other hand, defines what can be deployed through automation and is typically written from the security perspective. Practitioners have learned the hard way that IaC can create more problems than it solves without some additional layer of PaC validation for IaC changes. The trend towards formalizing PaC for IaC aligns with the principle of least-privilege/zero trust as PaC allows for security personnel to push CSPM policies to prevent misconfigurations (pre-deployment), rather than applying CSPM remediations in response to misconfigurations.

Refine the CSPM Section. The section on Cloud Security Posture Management (CSPM) introduces CSPM as well as related security capabilities and outcomes. The model appears to combine various controls (risk, IAM, infrastructure, etc.) under the moniker of CSPM. While the relationship of these controls to posture management is understood, agencies are likely to encounter CSPM tools and services that focus more on automating configuration management and detection of misconfigurations. Because the model groups together various capabilities under CSPM, it implies that this domain will address a broader scope of requirements than in reality.

We believe that the section will be strengthened by calling out additional capabilities, namely cloud inventory management of resources and entitlements. In addition, we also recommend leveraging data discovery and classification, as well as threat hunting, in conjunction with CSPM.

First, we believe cloud inventory management of cloud resources and entitlements should be called out as a CSPM capability because it is easy to overlook yet directly supports several other CSPM capabilities and outcomes. Automated discovery and monitoring of cloud resources, along with entitlements across resources, is fundamental to maintaining the integrity and security posture for all cloud deployments, which is a fundamental ZTA tenet. Automated and centralized management of cloud assets and their entitlements will only rise in importance as agencies move towards adopting multi-cloud solutions.

Second, we also recommend adding "data discovery and classification" as an essential capability alongside CSPM. This capability supports identity and access management (IAM) decisions but does not necessarily sit underneath IAM. We see the purpose of this data discovery and classification capability as twofold: (1) it supplements IAM by ensuring that authorized users are accessing the appropriate data or, in other words, it supports data centric IAM decisions; and (2) it allows the detection of collections or pools of sensitive government data which could indicate anything from accidental mishandling to malicious aggregation of stolen information prior to exfiltration.

Third, we support the inclusion of CSPM as part of an agency's threat hunting program. Threat hunting is a proactive activity whereby potential risks are identified before being exploited and remediated. This requires search and hunt tools, which should be deployed as a part of the cloud environment. Doing so would drive multiple desired outcomes and is consistent with CISA's new threat hunting authorities.

Comments on Zero Trust Maturity Model

The Zero Trust Maturity Model (ZTMM) provides agencies with a helpful tool to support their transition to zero trust. The ZTMM offers a clear way for agencies to understand where they currently are, and what constitutes more advanced levels of zero trust maturity. It enables agencies to conduct a qualitative assessment of their current maturity level and to understand what actions need to be taken to reach the next destination on their zero trust journey. We believe CISA could strengthen the maturity model by including quantitative metrics for measuring zero trust maturity. Agencies could use a quantitative assessment that is aligned to the use case scenario approach recommended above to accurately gauge and baseline its current maturity. Such an assessment could also detail the specific areas that agencies need to improve to reach their targeted level of maturity.

The way that CISA has broken down the five pillars (identity; device; network/environment; application workload; and data) makes good sense to us, and we further believe that the cross-cutting capabilities are constituted appropriately. The emphasis on leveraging automation and machine-learning tools at the "Advanced" level is particularly welcome, as such tools can allow for improvements across all pillars. Simultaneously, we encourage CISA to update the scope of the maturity model to align with the level of detail that is included in the final guidance

documents. For example, CISA should update the ZTMM to include the previously mentioned entitlements management within IAM.

Further, we caution CISA that the advanced criteria for the accessibility function of the application pillar should not be dependent on physical location. Instead, decisions should be made based on the mission considerations, data classification, risk assessment, system value, proximity of supporting capabilities, and other similar dimensions. This change allows for the underlying intent (i.e. progress towards ubiquity) without arbitrarily constraining the prioritization criteria for agencies or unintentionally interlocking the large scale transformations of cloud adoption and Zero Trust.

Another area that may be helpful for CISA to address more specifically is around cross-pillar coordination. Indeed, the Zero Trust Maturity Model states that "each pillar can progress at its own pace…until cross-pillar coordination is required." We recognize that coordination across pillars is necessary and believe it would be prudent for CISA to provide more specific guidance around such coordination. Again, we caution CISA against perpetuating the concept of security silos and encourage the inclusion of use-case scenarios that span these traditional silos. For agencies adopting Zero Trust, it will be critical to understand the horizontal relationships across the various functional capabilities, particularly as they look to mature their overall cybersecurity posture.

Moreover, we would like to underscore the importance of aligning the ZTMM to other federal guidance. The ZTMM correctly points out that "this maturity model is only one of many paths to support the transition to zero trust." We appreciate that CISA aligned the model's pillars with those contained in OMB's Federal ZT Strategy. This is an important step towards a coherent strategy throughout the federal government. We strongly encourage CISA to continue this close collaboration with OMB and other federal agencies to prevent the divergence of the aforementioned paths to support the transition to zero trust.

Comments on Federal Zero Trust Strategy

We recognize that the Zero Trust Strategy falls outside of CISA's scope. However, given the document's close relationship with the ZTMM, we would like to highlight a few considerations from our comments to OMB[1] and their potential impact on the ZTMM. CISA should collaborate closely with OMB to ensure all updates to either document are appropriately reflected in the other. These collaborative updates are key to ensure consistency across the various federal ZT documents. A coherent approach directly supports the administration's objective of managing federal cyber risk holistically. To that end, CISA and OMB should also collaborate with other federal agencies, including NIST, on developing ZT guidance.

[1] You can read ITI's comments to OMB here: https://iticdc.sharepoint.com/:b:/s/CyberEO/EQWyqPqcaDRMiC2AtluXJS8Brjx9Z4PIfBowzL1aVVO3xQ?e=2MmKJ6

Align the maturity model to use cases rather than silos. What makes Zero Trust so challenging is the confluence of implementing the right deny-by-default policies and integration across multiple domains. Applying a Zero Trust approach to use case scenarios helps make Zero Trust achievable and can help improve maturity across multiple security domains in a targeted way. Example use case scenarios that cut across security domains may include, but are not limited to, collaboration across agency boundaries, BYOD, remote employee or contractor access, and migrating to the cloud. A use case scenario approach is not simply solving a single maturity gap in one security domain but rather potentially solving a group of maturity gaps and aligning directly to an agency's business and IT objectives and priorities. Following this method, agencies will be able to address challenges that span data, users, workloads, networking, security orchestration, automation, and response. CISA should discourage agencies from trying to do everything at once. Describing use cases can support an incremental roll out while maintaining measurability of progress toward maturity.

Expand guidance on prioritization during incremental roll out. We appreciate that OMB gives agencies sufficient time to advance 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. If OMB updates the ZT Strategy to include prioritization guidance, CISA should also update the ZTMM with the same prioritization guidance to maintain consistency across ZT documents.

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[2] 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. CISA should consider whether it can incorporate such a roadmap as a part of its ZTMM.

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

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

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[3] that introduces administrators to foundational ZT concepts. We encourage CISA to reference NIST's Starting Guide in the ZTMM once the final version becomes available.[4] The OMB Strategy 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. To the extent that CISA can reflect this in its ZTMM, we encourage it to do so.

Encourage agencies to consolidate and secure identity systems. In the ZT Strategy, 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. In our comments, 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. Again, we encourage CISA to also consider how it might adopt or otherwise include such guidance as a part of the ZTMM.

Expand guidance on the EDR information-sharing that agencies will need to participate in with CISA. The Strategy 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 Federal Strategy does not mandate a timeline 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 an independent, third-party vulnerability management platform for continuous assessment and auditing of assets and connected devices.

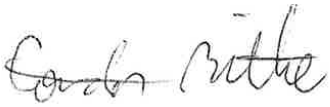
[3] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf
[4] You can read ITI's comments on the draft here: https://iticdc.sharepoint.com/:b:/s/CyberEO/EY1VKSrBRNNGrpvkrlI2R0ABM_NEqY7ZGu2FeDhYZl4lYQ?e=WXW57H

Relying on EDR alone will be insufficient to gain the necessary visibility into all exposures supporting all assets required for the ZTMM.

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. Should the guidance be expanded in the Strategy, we encourage CISA to consider how to fold such attributes into the ZTMM in the Device pillar.

Thank you for your consideration of our comments. ITI looks forward to serving as a resource representing the technology industry perspective to CISA as it continues the important work of improving the nation's cybersecurity. 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
Senior Vice President of Policy, Public Sector
Information Technology Industry Council (ITI)