CompTIA

September 24, 2021

Office of Management and Budget

725 17th Street NW

Washington, DC 20503

RE: Ensuring Adequate COVID Safety Protocols for Federal Contractors Executive Order, Section 5 Applicability Definitions

On behalf of the Computing Technology Industry Association "CompTIA", the largest US technology trade association with over 2,200 members, we respectfully submit the following inquiry on the Ensuring Adequate COVID Safety Protocols for Federal Contractors Executive Order, Section 5 Applicability definitions.

The common roadmap for ZTA transition

CompTIA agrees with the OMB's strategy to put all Federal agencies on a common roadmap by laying out the initial steps agencies must take to enable their journey toward a highly mature zero trust architecture. We would like to see OMB's further leadership in support of government-wide coordination to ensure the greatest consistency across agencies' implementation plans to reduce cost and increase efficiency. We believe this greatly increases the chances of a successful outcome. We would also like to suggest that OMB consider an open, ongoing dialogue with industry as the roadmap matures.

Continuous authentication

CompTIA agrees with the vision and actions laid out in Section A. A single sign-on service, phishing-resistant multi-factor authentication (MFA) and secure password policy form a great starting point. At the same time, identity can still be compromised by a sophisticated adversary penetrating the protections. For that reason, we would recommend extending capabilities to provide continuous authentication in which the identity risk score is continuously evaluated by user and entity behavior analytics (UEBA).

We understand that there currently exists a government wide effort to incorporate emerging technologies to help widen the secure environment. Advanced Artificial Intelligence (AI)/Machine Learning (ML) can predict whether the individual using the device is really the person who he or she claims to be. If the risk score deteriorates beneath a certain threshold, identity validation or MFA can be triggered and isolate the user.

Cloud based software defined network

CompTIA agrees that agencies should maximize internal use of recent versions of standard encryption protocols, such as TLS 1.3, that are designed to resist bulk decryption for protection against threats including MitM attacks. As explained in the strategy document, traffic monitoring and analysis should be performed utilizing visible metadata and ML techniques except in cases where deep traffic inspection is necessary. Inspection via TLS handshakes should trigger the use of AI/ML techniques to detect anomalies in areas of phishing, malware, beaconing and command and control techniques.

We propose a cloud-based software defined network with an advanced AI network risk engine. Running on a scalable cloud platform, the engine would continuously analyze a number of factors when determining trust and access levels of remote users. When a user's trust score changes, the cloud AI can be configured to take various actions. For positive changes in trust, a user may be rewarded with continued or upgraded access. Negative trust changes may result in diminished access, a request to re-authenticate, or trigger security alerts and remediation procedures including isolation of the user.

Emerging technologies such as artificial intelligence and quantum information science pose both opportunities and risks that we can only truly exploit and prepare for, much less commercialize or deploy, with the sustained support of the federal government for research and development. As cyberspace security and emerging technology are closely associated, any effort to increase security for one must not neglect the other.

Thank you for your consideration of our consensus industry comments. We stand ready to work closely with OMB as strategy development moves forward.

Very Respectfully,

David Logsdon

Staff Director

CompTIA Federal Cybersecurity Committee