CompTIA

Public Sector Cybersecurity Committee

2022 PRIORITIES

The Public Sector Cybersecurity Committee connects leading cybersecurity and information technology companies with key cybersecurity decision makers and stakeholders across the federal government. It works closely with federal departments and agencies, the White House, and Congress, to advocate for sustained federal investment in cybersecurity and modern commercial capabilities across government and privately-owned critical infrastructure. The Committee also promotes the adoption of cybersecurity best practices and the prioritization of cybersecurity in the deployment and integration of emerging technologies.

CompTIA Public Sector Cybersecurity Committee 2022 Policy Priorities

- Ensure robust cybersecurity funding
- Enact meaningful cyber incident reporting legislation
- Build on opportunities provided by the 2021 Infrastructure Investment and Jobs Act
    - Securing our infrastructure
    - Implementation of state and local cybersecurity grant program
- Provide a balanced approach to the implementation of emerging technologies
- Provide a modernized federal cybersecurity framework through governance reform and cloud security programs
- Ensure that federal Zero Trust is implemented in a comprehensive, transparent and timely fashion

1 Robust federal cybersecurity funding is needed to secure the infrastructure that will underpin our digital future

Background:

Federal funding for IT modernization, including cybersecurity, is essential both to improve productivity and to secure our nation from future devastating cyberattacks. Meaningful investment in federal IT infrastructure and modern commercial capabilities across federal, state, and local governments is long overdue. In 2021, Congress made an important down-payment via the 2021 American Rescue Plan Act towards modernizing and securing federal IT networks, but a sustained federal commitment will be required to secure our 21st century digital ecosystem over the long term.

Recommendation:

Ensure sustained federal funding to address IT modernization, including cybersecurity, particularly as new federally-supported infrastructure projects are rolled out and EO 14028 and its follow-on activities are implemented.

2 Enactment of a meaningful cyber incident reporting law is needed to address an increasingly volatile threat landscape

Background:

Congress should build on its notable efforts in 2021 with the Administration, and in close consultation with industry, to pass meaningful cyber incident reporting legislation in 2022. Major cyber threats and vulnerabilities exposed over the past year have highlighted the need for the systemic and reliable collection of cyber incident information from critical infrastructure entities at the scale necessary to improve our nation's cyber situational awareness.

Recommendation:

Pass cyber incident reporting legislation to improve our nation's cyber situational awareness of current and future threats.

3 Build on the opportunities provided by the 2021 Infrastructure Investment and Jobs Act

Secure Infrastructure

Background:

The Infrastructure Investment and Jobs Act (P.L. 117-58) recognizes that protecting modern infrastructure from cybersecurity threats is a national security issue. In 2022, there is a crucial opportunity for the public sector and the private cybersecurity industry to partner and ensure cybersecurity is incorporated into the rollout of this once-in-a-generation investment in our nation's digital infrastructure.

Recommendation:

The strategic implementation of federal funding can help to increase efficiencies, effectiveness and security within existing infrastructure and set the foundation for future innovation and advancement. Federal funding must be expedited to federal, state, and local projects and must incorporate cybersecurity measures to address the persistent threat to our nation's critical infrastructure.

State and Local Cybersecurity Grant Program

Background:

The Infrastructure Investment and Jobs Act created a new $1 billion (over 4 years) cybersecurity grant program to help state, local, tribal and territorial (SLTT) agencies improve their cyber posture and address cybersecurity threats and risks to their information systems. The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency are in the process of developing the guidance to create and administer this grant program.

Recommendation:

Partner with CompTIA Public Technology Institute to serve as a resource to CISA and FEMA as they develop grant guidance. Provide support and technical assistance to SLTT agencies as they develop cyber plans and determine their cybersecurity priorities.

4 Provide a balanced approach to the implementation of emerging technologies

Background:

The federal government should leverage innovative technologies and invest in its cybersecurity capabilities and workforce to help prevent, respond to, and recover from cyberattacks. For example, agencies may prioritize cybersecurity tools applying artificial intelligence (AI) and machine learning (ML) to improve cyber threat prevention, protection, and remediation

Recommendation:

Ensure that there is clear guidance (from both a technical and implementation perspective) and consistent funding to integrate emerging technologies that support the federal government's cybersecurity mission.

5 Provide a modernized federal Cybersecurity Framework through governance reform

Background:

We support improved coordination and streamlining across cybersecurity governance regimes used to verify the cybersecurity of federal systems and federal contractors

Recommendation:

As federal cybersecurity requirements develop and evolve, private sector innovation advances, and oversight policies are updated and modernized, ensure that there is transparency for industry into the process. Ensure that the metrics aligned with the various policies match the evolving digital landscape. Add additional cybersecurity components to the FITARA scorecard.

6 Ensure that the federal transition to Zero Trust is implemented in a transparent and timely fashion that stresses consistent funding, requirements, and proper governance

Background:

The Administration's federal Zero Trust policy directs federal agencies to quickly integrate zero trust requirements into their planning and budgets, and implement stronger enterprise identity and access controls, including more widespread use of multi-factor authentication. Agencies will also need to complete an inventory of every device authorized and operated for official business, to be monitored according to specifications set by CISA.

Recommendation:

As Zero Trust is implemented within federal agencies, make sure they take a comprehensive approach to Zero Trust and that the process is transparent to industry and incorporates industry expertise and perspective obtained through public-private partnerships.