2021 Committee Priorities

CompTIA Federal Cybersecurity Committee

Federal Cybersecurity funding- Federal funding for IT modernization and cybersecurity is essential both to improve productivity and to secure our nation from future devastating cyberattacks or SolarWindstype compromises. Meaningful investment in federal IT infrastructure and modern commercial capabilities across federal, state, and local governments is long overdue. The American Rescue Plan Act has provided an important down-payment towards modernizing and securing federal IT networks as the nation builds back better than before, but a sustained commitment will be required to support and secure our 21st century digital government over the long term.

Emerging Technology Security- 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. The recent and unfolding large scale supply chain hacks are strong indication that voluntary security guidance, impacting cyberspace or emerging technology, may no longer meet the nation's needs.

Cyber Framework- FISMA Reform, etc.- Any discussion of an improved cybersecurity posture for federal technology must include streamlined and improved coordination of the tools and systems used to verify the security of its contractors. To ensure innovative and cutting-edge cybersecurity solutions, better harmonization and coordination is needed between FedRAMP, the Federal Information Security Modernization Act (FISMA), the Federal IT Acquisition Reform Act (FITARA), the Department of Defense's Cybersecurity Maturity Model Certification (CMMC), regulations resulting from the Federal Acquisition Supply Chain Security Act (FASCA), and other federal cybersecurity-related rules and regulations.

Infrastructure- We must build on the down-payment for modernizing federal IT infrastructure contained in the American Rescue Plan, to include further investment in cybersecurity at the federal, state, and local levels -- and across all key infrastructure sectors including government, transportation, utilities, financial, 5G, etc. As infrastructure becomes increasingly connected and as sophisticated threats proliferate, cybersecurity software, services, and mission-critical embedded systems will be central to this effort.

Cyber Incident Reporting- Following a process of collaboration between the public and private sectors, Congress should instruct the Executive Branch to establish requirements for critical infrastructure entities to report cyber incidents to the federal government, as the federal government presently lacks a mandate to systemically collect cyber incident information reliably and at the scale necessary to inform situational awareness. The SolarWinds incident highlights how the current state of affairs, often dependent on voluntary disclosures by impacted entities, may offer inadequate protection let alone the situational awareness necessary to permit successful remediation once an incident has occurred.

Zero Trust – Zero Trust is the modern version of a 'Least Privilege" approach. The goal of Zero Trust Architecture (ZTA) is to have no implicit permissions to networks and resources so that only the explicitly allowed users, entities and devices have access and even then, only to the specific resources that they are allowed to access based upon policy. Zero Trust focuses on the security of the transactional use cases rather than just perimeter protections. This is not to say that perimeter security no longer has a role in securing networks, it just alters the paradigm to focus on the things that actually need protecting, the data. Technologies that support IdAM, NAC, SDN, and others support a robust Zero Trust approach.

DHS State and Local Cybersecurity Grant Program – Last year, the House passed H.R. 5823, The State and Local Cybersecurity Improvement Act, which establishes a $400 million grant program at DHS to address cybersecurity vulnerabilities on state and local government networks. The legislation provides long-overdue resources and support to state, local, tribal, and territorial governments across the country whose cyber defenses are outmatched by sophisticated adversaries. The legislation did not advance in the Senate. House Homeland Security Committee Chairman Thompson is expected to introduce a version of the legislation again this year.

DHS Continuous Diagnostics and Mitigation (CDM) Program –The DHS CDM Program was developed in 2012 to support government-wide and agency-specific efforts to provide risk-based, consistent, and cost-effective cybersecurity solutions to protect federal civilian networks across all organizational tiers. The DHS CDM Program provides cybersecurity tools and services to agencies so they can identify potential cybersecurity vulnerabilities, mitigate threats, or respond to potential cybersecurity attacks.