CompTIA

CompTIA Federal Procurement Council

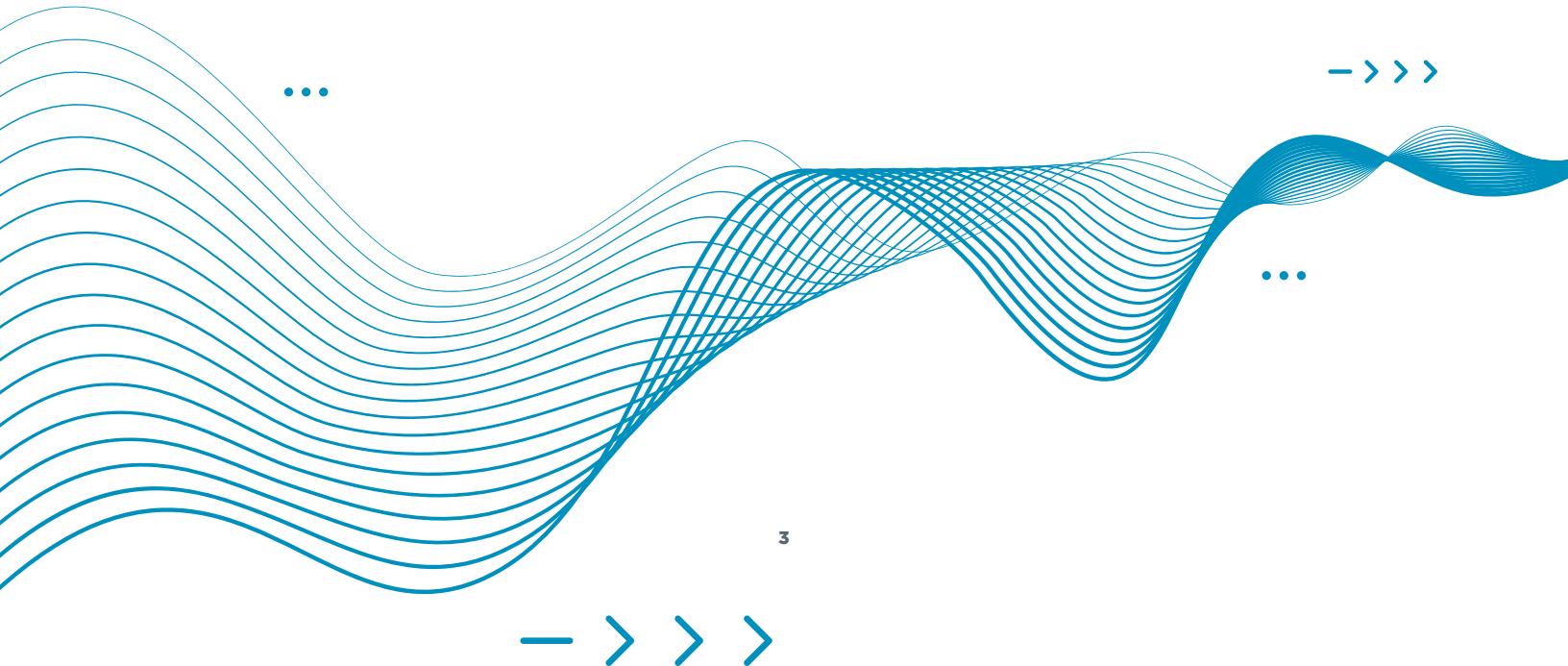
2021 PRIORITIES

The Federal Procurement Council connects leading technology companies with policy and decision makers in the Federal government. The council works closely with Federal agencies, Congress, and the White House to help define, outline, and implement a forward-leaning, IT-focused modernized acquisition framework that promotes improved emerging technology adoption.

Through advocacy and education efforts, articulate the critical importance of modernizing our federal IT infrastructure.

Outdated government IT systems and processes hinder many federal and state agencies' ability to deliver services. This fact has been well known and disturbingly unresolved, even before the COVID-19 pandemic hit. The rapid transition to remote telework during the pandemic also created new challenges for government agencies, including increased cybersecurity threats.

Congress can still make a transformative investment in IT modernization – and must do so now, before we fall even further behind. This opportunity coincides with a shift to cloud computing, which allows agencies at all levels of government to leverage private sector investment in IT infrastructure to improve cybersecurity and adaptability. Modern digital architectures also allow government organizations to scale more quickly to meet spikes in demand for services. New commercial capabilities enable public sector organizations to leverage data as a strategic asset to meet their mission more effectively and efficiently. Importantly, the gains from investing in technology now will continue to accrue far after the current emergency ends.



Encourage and support a balanced approach to the "Made in America" Executive Order that emphasizes American competitiveness and a healthy defense industrial base.

The new "Made in America" Executive Order (EO) will make broad changes in how the Buy American Act and trade agreements are applied. Although the details will be in forthcoming regulations, the EO establishes a new term ("Made in America Laws"), creates a new position for monitoring this issue inside the Office of Management and Budget (OMB), and sets up new standards for what will constitute a domestic end item. Working closely with the various technology industry stakeholders (Administration, federal agencies, and Congress), the Council will strive to ensure that the implementation of the EO emphasizes American competitiveness while safeguarding a healthy defense industrial base.

Create a permanent Section 3610 authority.

Over the past year, the CompTIA Federal Procurement Council has consistently supported the extension of Section 3610. Section 3610 has proven to be an important means of providing necessary relief during the pandemic to critical intelligence community industry partners —and particularly to small businesses that provide highly specialized capabilities —to retain key national security capabilities. With telework being an integral component of the national security workforce for the foreseeable future and COVID still upon us, CompTIA supports a permanent Section 3610 authority.

Support cloud computing procurement policy.

FedRAMP

While well-intended and partially successful, FedRAMP's design is no longer optimized for modern security solutions. It is unsuited to the growth of emerging technologies like the Internet of Things (IoT) and artificial intelligence/machine learning (AI/ML) and is not dynamic enough to incorporate new innovative products. These deficiencies are a result of FedRAMP's limited resourcing and ability to keep pace with agency and cloud service provider (CSP) demand for review and authorization, agencies' limited reuse of authorizations to operate (ATOs), and the compliance-focused, manually driven certification and maintenance process that underpins the interaction between agencies and CSPs. This is further complicated by the implementation of multiple new competing cybersecurity regulations.

Given this growing complexity, rather than codifying FedRAMP, we ask for a comprehensive GAO report on the laws and regulations impacting the U.S. government cybersecurity framework. The report shall describe how these laws and regulations differ among agencies, how agencies are managing risk within their networks, and agency acceptance of FedRAMP JAB certifications, as well as the application of agency Authorities to Operate (ATOs) across government and by other agencies, how the accreditation program at the Defense Information Systems Agency (DISA) corresponds to FedRAMP and other cybersecurity requirements, and proposals for centralizing the U.S. government cybersecurity posture to better coordinate agency systems and processes.

DISA

The Department of Defense has stipulated that cloud and cognitive computing will significantly alter warfighting and defense business operations. Recognizing this, the Department established the Joint Artificial Intelligence Center (JAIC) to accelerate delivery of AI-enabled capabilities and is partnering with industry to securely deliver commercial cloud capabilities in alignment with mission requirements. To enable this transition, the Department has tasked the Defense Information Systems Agency (DISA) with the migration of DoD applications and services out of DoD-owned and -operated data centers to commercial cloud services while maintaining the security of, and the control over, all DoD data in accordance with DoD policies.

DISA must also establish a basis on which DoD can assess the security posture of DoD and non-DoD CSP's cloud service offerings (CSOs) and grant a DoD Provisional Authorization (PA) to host DoD information and systems. Industry is concerned about delays in issuing PAs and ATOs to CSPs, especially those who have achieved FedRAMP certification. In addition, a multi-CSP environment enables greater competition and cost savings. We would ask the committee to instruct DISA to issue a report every six months to the Armed Services committees, starting 30 days after the enactment of this legislation, detailing the process for accrediting CSPs, the number of CSPs that have applied for accreditation, and where the CSPs are in the PA and ATO process, as well as other pertinent information.