Business Software Alliance

2025 Cyber Legislative Agenda

Congress' Path to a Stronger, Secure, Resilient, and Prosperous Nation

2025 presents a pivotal opportunity for Congress to strengthen cybersecurity, ensure efficient operation of government agencies, and improve the American economy. The following recommendations are designed to enhance cybersecurity, improve the effectiveness and efficiency of the US Government, set the Nation on a path for sustained growth, and better serve the American people. These actions will help Congress change the status quo, drive economic growth, and ensure American leadership.

1 Require Harmonization

BSA urges Congress to pass legislation that requires agencies to harmonize their cyber requirements, including those pertaining to (1) cyber incident reporting, (2) cloud security, (3) cyber supply chain risk management, and (4) software security. Agencies should map existing and new requirements to internationally recognized standards or National Institute of Standards and Technology (NIST) standards or guidelines. Harmonizing cyber requirements would help government agencies to collaborate, for example detecting and responding to threats and vulnerabilities; reduce barriers to the introduction of better, innovative security solutions; and ease the strain on a cyber workforce whose responsibilities are already over capacity. In some cases, Congress should consider using the Congressional Review Act when agencies issue cyber regulations that are not harmonized.

2 Modernize Government IT

BSA urges Congress to actively help bring the Federal Government's IT into the 21st century, which means investing in new, secure IT and updating how agencies purchase IT. Business-to-business technology has driven the private sector's advance, and Congress has an essential role to help drive agency adoption of modern and industry-proven systems through efficient procurement rules. Both legislation and oversight should, among other things, ensure agencies look to commercial product software for solutions, streamline certifications like FedRAMP and invest in new IT solutions to serve the American people.

3 Advance AI for Cybersecurity

BSA urges Congress to pass legislation that explicitly exempts artificial intelligence (AI) used for cybersecurity purposes from other laws and policies that otherwise limit or control the use of AI to ensure laws do not unintentionally hamper cyber defenders working to protect Americans and their economy. To keep pace with malicious actors, and even shift the balance in favor of defensive cybersecurity activities, cyber defenders need to be able to use AI for activities including developing more secure code, detecting and responding to threats, protecting against malware, patching and managing vulnerabilities, improving identity management, analyzing user behavior, generating threat intelligence, and easing the cyber workforce gap.

4 Build a Cyber Workforce for the Present and Future

BSA urges Congress to help prepare Americans to quickly fill open cybersecurity jobs. Today, there are approximately 500,000 open cyber jobs in the US; for the sake of security they must be filled. Congress should direct CISA to use the NIST Workforce Framework for Cybersecurity to identify the work role categories, work roles, and competency areas of greatest need to government agencies and US businesses and then drive the demand for cyber training and education from workers, including entry-level workers and career changers, as well as those not pursuing four-year degrees through incentives (e.g., scholarships and tuition reimbursement) and the supply of training and education by leveraging America's two-year colleges.