The Software Alliance

BSA

Priorities in Cybersecurity

The incoming Administration must take robust action to confront cybersecurity threats to US citizens, companies, and communities and to elevate US global cybersecurity leadership. The Administration's National Cyber Strategy should recognize the important role that strong businesses play in our national and economic security, develop its strategy in collaboration with private sector partners, and recommit to using risk-based approaches to regulation.

BSA's 2025 Global Cyber Agenda outlines recommendations to elevate, improve, and integrate better cybersecurity throughout the nation. Immediate priorities for action in the incoming Administration include:

1. Enhancing Software Security
2. Elevating and Improving Cybersecurity Risk Management
3. Collaborating Across Borders
4. Investing in Long-Term Digital Resilience

1 Enhancing Software Security

Government policies should create a sustainable marketplace in which responsible companies are rewarded for using secure software development best practices. The incoming Administration should:

- **Drive Demand for Software, Including AI Software, Developed Using Secure Software Development Best Practices.**
- **Assure Safe Harbor From Liability for Software Producers That Use Best Practices for Secure Software Development.**
- **Rationalize Recent Software Security Requirements, Voluntary Pledges, Guidance, and Other Activities to Create a Consistent, Coordinated, Whole-of-Government Approach to Cybersecurity.**

2 Elevate and Improve Cybersecurity Risk Management

Government policies should harness the power of risk-based approaches that empower organizational leaders to deliver concrete cybersecurity improvements. The incoming Administration should:

- **Embrace AI to Bolster Cybersecurity.** The Administration can embrace AI by only supporting laws and policies that address high-risk uses of AI which do not unintentionally impede the use of AI to improve cybersecurity.
- **Work With Industry to Develop or Identify Metrics.** The Administration should use these metrics to help organizations understand threats and risks and deploy resources effectively and efficiently.

- **Harmonize US Government Laws and Policies.** The Administration should tailor cyber incident reporting regulations under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) to obtain information on only the most impactful cyber incidents, and aligning all other cyber incident reporting regulations to those promulgated under CIRCIA, as well as aligning requirements of CMMC, FedRAMP, and other cybersecurity procurement requirements across the US Government.

3 Collaborate Across Borders

Government policies should leverage relationships with like-minded allies to amplify the effectiveness of their cybersecurity laws and policies and ensure businesses compete, not on which has the larger team of compliance attorneys, but which can better deliver functional and secure solutions. The incoming Administration should:

- **Harmonize Cybersecurity Laws and Policies Internationally.** The Administration should prioritize working with like-minded governments to align cyber incident reporting requirements and to develop a process to provide mutual recognition of like-minded government's cloud security certifications.
- **Support Domestic Harmonization.** Require alignment between CMMC, FedRAMP, government-wide efforts led by CISA, like the Secure Software Attestation Form, and the cybersecurity requirements of each agency.
- **Ensure Data Flows Across Borders to Improve Secure Services and Put Actionable Information in Cyber Defenders' Hands.**

4 Invest in Long-Term Digital Resilience

Government policies should have a long-term vision, making investments today that will ensure future generations can continue contribute to and reap the benefits of digital transformation. The incoming Administration should:

- **Leap Forward From Legacy to Modern IT.** The Administration can support this progress by increasing the focus on moving legacy systems to modern technology by taking the steps outlined in BSA's Procurement Agenda: Better Purchasing for US Government IT Transformation.
- **Transition to Post-Quantum Cryptographic Algorithms.** The Administration can support this transition by taking the steps outlined in Quantum Computing and Encryption: Six Actions Governments Should Take to Secure Information.
- **Build a Cybersecurity Workforce for the Present and Future.**