The Software Alliance

BSA

Priorities in Cybersecurity

The incoming Administration must take robust action to confront cybersecurity threats to US networks and systems and to elevate US global cybersecurity leadership. BSA's cybersecurity agenda outlines a fulsome agenda for securing our digital future. Immediate priorities for action in the incoming Administration include:

1. Securing the Software Ecosystem
2. Recalibrating Supply Chain Policies
3. Securing the Internet of Things
4. Advancing Cybersecurity Through Digital Transformation
5. Organizing the Government to Combat Cyber Threats

1 Securing the Software Ecosystem

Government policies have focused on defending networks, but security for the software products and services on those networks has too often been neglected. The BSA Framework for Secure Software is a first-of-its-kind tool enabling stakeholders, including those in the government, to communicate and evaluate secure outcomes associated with software products and services. Tools like the BSA Framework should be leveraged to incentivize smart software purchasing decisions. In addition, the incoming Administration should:

- ☑ Support widespread adoption of cloud technologies by advancing standards-based cloud security policies that enable innovative, adaptable security solutions.
- ☑ Support development of internationally recognized software security standards and ensure software security policies are based on those standards.
- ☑ Strengthen investment in security research aligned to coordinated vulnerability disclosure programs and drive widespread adoption of coordinated vulnerability disclosure.

2 Recalibrating Supply Chain Policies

Supply chain risk management policies are most effective when they respond to clearly identified risk and establish fair, transparent, and collaborative processes to mitigate risk. Some recent policy measures have fallen short of these goals, targeting overbroad categories of products or failing to communicate information about risk and process to the public. The incoming Administration should:

- ☑ Lead multilateral coalitions to advance shared, standards-based supply chain risk management policies consistent with international obligations.
- ☑ Amend Executive Order 13873 to narrow government intervention in private-sector supply chains, focusing on mitigating specific and demonstrable risk in a transparent manner.
- ☑ Work with Congress to build consistent, transparent approaches to supply chain risk management that establish common methods across government agencies, prioritize risk, provide clear guidance on compliance, and offer affected vendors mechanisms to remediate supply chain concerns.

For more on supply chain issues, please see BSA's Principles for Supply Chain Risk Management.

3 Securing the Internet of Things

Inadequately secured IoT devices and services can serve as entry points for cyberattacks, compromising sensitive data and threatening the safety of individual users. Attacks on infrastructure and other users, fueled by networks of poorly secured IoT devices, can affect the delivery of essential services, put the security and privacy of others at risk, and threaten the resilience of the internet globally. Governments have taken various approaches to confront these threats, but US leadership has lagged. The incoming Administration should:

- ☑ Establish a common approach to IoT security that provides clear, flexible, outcome-focused security guidance and avoids state-level policy fragmentation.
- ☑ Lead international efforts to establish widely recognized IoT standards based on industry best practices and harmonize policy approaches.
- ☑ Create policies that help consumers gain access to security information about IoT devices, enabling smart purchasing decisions.

For more on IoT security, please see BSA's Policy Principles for Building a Secure and Trustworthy Internet of Things.

4 Advancing Cybersecurity Through Digital Transformation

Strong cybersecurity depends on strong information technology infrastructure. By embracing digital transformation, the incoming Administration can build a solid foundation for cybersecurity efforts across the board. Specifically, the incoming Administration should:

- ☑ Invest in advancing IT modernization in federal government agencies, and supporting IT modernization at state and local governments.
- ☑ Accelerate adoption of cloud services, and drive innovation in cloud security policies and practices.
- ☑ Expand open data policies, including international agreements, to accelerate development to AI-driven security tools.
- ☑ Strengthen R&D efforts for securing quantum computing environments.
- ☑ Integrate security best practices for 5G, IoT, and other areas into smart city security requirements.

5 Organizing the Government to Combat Cyber Threats

Global cybersecurity benefits from strong US government leadership, and such leadership demands an agile, coherent organizational structure to unite the interagency toward common objectives. The incoming Administration should:

- ☑ Continue to empower, with both new resources and improved authorities, the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security as the focal point of domestic cybersecurity leadership.
- ☑ Establish a National Cybersecurity Coordinator to lead interagency cybersecurity initiatives.
- ☑ Appoint an ambassador-level official to lead a dedicated cybersecurity bureau at the Department of State.

ABOUT BSA

BSA | The Software Alliance is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life.

With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.