A CYBERSECURITY AGENDA FOR THE CONNECTED AGE

The world is more connected now than ever, with half the world's population currently online. We are connected through our smartphones and web browsers, but also through home appliances and industrial manufacturing robots. Technologies such as cloud computing services and artificial intelligence are also connecting businesses and governments, and transforming their operations.

While these online connections bring opportunity, they also create risk, including large-scale data theft, privacy violations, phishing scams, ransomware, and malicious information operations that affect millions of people in the United States and around the world each year. Cybercrime will cost up to $6 trillion by 2021 — equivalent to nearly half of today's US GDP. Beyond the financial costs, these threats erode trust in the online environment, disrupt global commerce, and cause physical damage to critical infrastructure, ultimately putting lives at risk.

To address this challenge to the connected economy, cybersecurity practices and tools must defend the integrity, privacy, and utility of the Internet ecosystem. Although businesses, private citizens, and government agencies all share responsibility for enhancing cybersecurity, the government plays a singular role. Given that effective cybersecurity requires close collaboration between the private and public sectors, **BSA | The Software Alliance** urges the US Government to expand its leadership in improving cybersecurity, both here and abroad.

More specifically, we strongly support a robust partnership of government and industry to:

- Promote **a secure software ecosystem** by creating industry benchmarks, developing tools to understand critical information, and strengthening security research and vulnerability disclosure
- **Strengthen government's approach to cybersecurity** by modernizing government IT, harmonizing federal cybersecurity regulations, and incentivizing adoption of the NIST framework

Guiding Principles for Cybersecurity Policy

Cybersecurity policies should adopt approaches that are:

- Aligned with internationally recognized standards
- Risk-based, outcome-focused, technology-neutral
- Market-driven where possible
- Flexible and adaptable to encourage innovation
- Rooted in public-private collaboration
- Oriented to protect privacy

- Pursue international consensus for cybersecurity action by **supporting international standards** development as well as adopting and streamlining international security laws
- Develop a **21st century cybersecurity workforce** by increasing access to computer science education and opening new paths to cybersecurity careers
- Advance cybersecurity by **embracing digital transformation,** leveraging the potential of emerging technologies and forging innovative partnerships to combat emerging risks

This cybersecurity agenda should be rooted in the realities of today's complex global digital economy and built upon past successes. Working together, government and industry can help the world's citizens reap the benefits of the digital economy while protecting our safety, security, and privacy.

more >>

Specifically, elements of a Cybersecurity Agenda should:

Promote a Secure Software Ecosystem

Establish an industry benchmark for software security. Support development of a set of widely recognized, industry-driven software development and management best practices to elevate cybersecurity practices.

Develop tools to communicate critical cybersecurity information to consumers and enterprise stakeholders. Establish widely used, market-driven tools for providing relevant cybersecurity information to consumers and enterprise stakeholders to inform purchasing decisions, network operation, and risk management.

Strengthen identity management. Work to expand adoption of identity management technologies across public and private sector organizations, and to increase emphasis on identity management in cybersecurity policies and frameworks.

Promote security research and vulnerability management. Strengthen investment in security research aligned to coordinated vulnerability disclosure programs, and ensure the policy environment is conducive to research that drives stronger cybersecurity.

Create a Stronger Government Approach to Cybersecurity

Modernize government IT. Invest in IT infrastructure for federal, state, and local governments with an eye toward cybersecurity, including through adoption of cloud computing, defense-in-depth, continuous monitoring, data analytics, and other innovative security technologies.

Harmonize federal cybersecurity regulations. Review regulations and standards across sectors, identify redundancies and conflicts with the NIST Framework, and promote a consistent, cross-sector approach to federal cybersecurity policies.

Improve cybersecurity in government acquisition. Incentivize cybersecurity by creating competition for cybersecurity performance in government acquisition processes.

Incentivize adoption of the NIST Framework. Develop tax, acquisition, and other incentives to encourage adoption of the NIST Framework.

Pursue International Consensus for Cybersecurity Action

Harmonize global cybersecurity laws to align security and economic growth. Support both cybersecurity and economic growth by promoting harmonization of laws and policies across countries to foster innovation, security advancements, free flows of data, and market access.

Advance international cybersecurity norms. Encourage international dialogue and drive agreements on cybersecurity practices in bilateral and multilateral frameworks.

Support international standards development and adoption. Support industry and non-governmental efforts to develop and update international standards. Encourage global adoption of international standards.

Develop a 21st Century Cybersecurity Workforce

Increase access to computer science education. Expand cybersecurity education for K–12 as well as in undergraduate computer science programs, increase scholarships, and incentivize minority students.

Promote alternative paths to cybersecurity careers. Launch careers through apprenticeship programs, community colleges, cybersecurity "boot camps," and government or military service.

Modernize training for mid-career professionals. Reform Trade Adjustment Assistance, and update other mid-career re-training programs, to provide American workers with high-demand cybersecurity and IT skills as digitalization transforms the global economy.

Improve the exchange of cybersecurity professionals between the government and private sector. Enable private sector experts to join the government for periodic or short-term assignments.

Advance Cybersecurity through Digital Transformation

Leverage emerging technologies to enhance security. Target investments and constructive policies to capitalize on the tremendous potential of artificial intelligence, quantum computing, blockchain, and other emerging technologies to enhance security.

Build on momentum of public-private collaboration to combat botnets and other automated threats. Expand public-private collaboration to confront the botnet threat.

Drive IoT cybersecurity through adoption of proven software security best practices. Integrate security-by-design principles into IoT standards and guidance, and develop frameworks for assessing risk and identifying security measures.

Help Smart Cities stay cyber resilient. Provide planning support, threat information, and incident response support to municipal planners and managers to enhance the resilience of Smart Cities against cyber threats.