The Software Alliance

BSA

Priorities in 5G

The United States should seize the opportunity to shape the future of global 5G networks based on software solutions. As BSA's 5G Security Agenda emphasizes, governments must act now to achieve effective, sustainable security. The incoming Administration should:

1. Harness Software Innovation
2. Recalibrate Supply Chain Policies
3. Secure Software and the Cloud
4. Build Smart, Effective Governance

1 Harness Software Innovation

Unlike previous generations, 5G is a shift to an IT-based system that replaces purpose-build hardware with software running in hyperscale clouds. As such, software solutions can be leveraged to mitigate high-priority risks. Software solutions can create greater flexibility, agility, and supplier diversity; driving innovation and competition in addition to security. The incoming Administration should harness software innovation by:

- ☑ Investing in the development and deployment of Radio Access Network (RAN) technologies that are both software-based (virtualized RAN) and built on open standards and interfaces (open RAN).
- ☑ Enhance research and development (R&D) investments in critical 5G security technologies, including secure network slicing, automated vulnerability screening, AI applications, supply chain management tools, secure open source architectures, and more.
- ☑ Support the deployment and continued development of strong encryption modules, avoiding government access mandates and other policies that could undermine a key technology for securing 5G.
- ☑ Expand efforts—building on work at the National Institute for Standards and Technology (NIST) and elsewhere—to develop zero-trust architectural approaches to securing 5G networks.

2 Recalibrate Supply Chain Policies

Threats to hardware and software supply chains have emerged as a priority for securing 5G networks. Supply chain risk management policies are most effective when they respond to clearly identified risks and establish fair, transparent, and collaborative processes to mitigate that risk. Unfortunately, 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 needs to recalibrate the US approach to supply chain risk management. Specifically, it 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 approaches across government agencies, prioritize regulation based on 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 Secure Software and the Cloud

Cloud services will play a central role in the 5G network architecture from core operating services to edge computing environments. Cloud infrastructure will drive many of the security benefits of 5G, including enabling rapid deployment of mitigations, dynamic assignment of compute resources to meet security and resource demands, and greater overall network resilience. Fully capitalizing on these benefits will require secure and trustworthy cloud environments. Likewise, because 5G and cloud services are largely software-based, 5G networks will not be secure without greater software assurance. The incoming Administration should:

- ☑ Reinvigorate US leadership to advance development of internationally recognized standards for cloud security, and promote standards-based, harmonized policy approaches globally.
- ☑ Modernize FedRAMP and other US government cloud policies to more deeply integrate agile, risk-based approaches to cloud security that leverage continuous monitoring and automation to improve both efficiency and security outcomes.
- ☑ Leverage tools like the BSA Framework for Secure Software and the recently-published NIST Secure Software Development Framework to incentivize smart software purchasing decisions in the government and beyond.

4 Build Smart, Effective Governance

Strong security controls and technical measures rely upon effective 5G governance, particularly regarding the technical standards that underpin 5G development around the world. To realize the potential of 5G's built-in security advantages, and to ensure the US government is well-prepared to guide and respond to evolving 5G security priorities, the incoming Administration should:

- ☑ Substantially increase US government participation in international standards development, prioritizing development of open standards and interfaces for 5G.
- ☑ Strengthen the US *National Strategy to Secure 5G* by identifying resources for key priorities and embracing software innovation as a core element of 5G security.
- ☑ Conduct a government-wide review of 5G governance, agency roles and responsibilities, and coordination mechanisms to ensure consistency and coherence across the US government.
- ☑ Ensure that government mechanisms for stakeholder engagement include stakeholders that reflect 5G's evolution to a largely software- and cloud-based architecture.

The Software Alliance
BSA

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.