Effective Cybersecurity for the Internet of Things (IoT)

BSA Position

- IoT devices have tremendous promise to generate jobs, reduce costs, and increase efficiency and convenience for businesses and individuals.
- **To realize these benefits, we need flexible, risk-based cybersecurity policies that account for the diversity of IoT devices and facilitates collaborative, industry-led solutions.**

Issue Discussion

The decreasing cost of sensors and software combined with a nearly ubiquitous internet and cloud-powered data analytics, has allowed innovators to add "intelligence" to a wide array of devices from watches to appliances to cars. These devices collect data about their performance, usage, and power consumption among other information which can be used by the individual or business to maximize efficiency and reduce costs. For example, a "smart" thermostat can not only respond to a user's commands from a smartphone around the globe, but can "learn" an owner's behavior and automatically adjust itself saving nearly 20% on energy bills. Nearly all devices in the home, workplace, farm, or factory can benefit from being connected to the internet, with significant potential increases to productivity, efficiency, and cost-savings.

However, in order to realize these benefits, these devices must be secure from cyberattack. Improperly secured IoT devices can be hacked, reducing or inhibiting device performance or causing other significant consequences.

BSA's Position

The foundation for a successful IoT cybersecurity policy is predicated on four key principles:

1. **Recognition of the Complexity and Diversity of the Internet of Things:** Any effective IoT cybersecurity policy must account for the multi-faceted dimensions of the Internet of Things, and avoid overly simple, one-size-fits-all approaches. Such policies should acknowledge and distinguish between the broad diversity of risk, functionality, and market characteristics of IoT devices, and tailor security solutions to address the most critical risks.

2. **Multi-Stakeholder Processes Enabling Industry-Led Solutions:** Multi-stakeholder processes involving the wide range of IoT stakeholders can facilitate thoughtful and effective IoT cybersecurity policies by allowing industry to apply its expertise and global experience to drive security solutions. IoT cybersecurity will be stronger when government and industry tackle challenges as partners.

3. **Flexibility and Adaptability:** Any cybersecurity policy should be sufficiently flexible and adaptable to enable and incentivize continued innovation and customization, while also improving cybersecurity.

4. International Harmonization and Interoperability: U.S. IoT cybersecurity policies should be developed with an eye toward advancing common global approaches to shared challenges, working through international standards and multi-lateral frameworks wherever possible. Common global frameworks are critical to ensuring that IoT stakeholders can access markets fairly and equitably around the globe.

Policy Recommendations:

With solid foundational principles in place, BSA recommends that the following specific policies be included in any IoT cybersecurity plan.

1. **Develop a Risk-Based Framework for IoT Security:** Policymakers should develop a framework for categorizing IoT devices according to risk, addressing factors such as device vulnerability, cost-benefit of enhanced security, prevalence in the market, and intended use. An example is instructive; an IoT "smart plug" that provides smartphone control and energy usage information has a fundamentally different risk profile than a "smart car" operating on public streets.

2. **Promote Software Best Practices:** IoT devices' software should continue to build on established best practices from the software industry, such as secure development lifecycle, patchability, strong identity management, and coordinated disclosure of vulnerabilities.

3. **Develop Tools to Inform Consumers:** IoT device manufacturers and software developers need tools for communicating critical cybersecurity information to individuals and enterprise stakeholders, empowering them to prioritize security. The Federal Government can play a constructive role as the “convener” for multi-stakeholder processes, as it is already doing through NTIA’s IoT patchability information process.

4. **Promote Shared Responsibility:** Securing IoT devices requires an ethic of shared responsibility; no one stakeholder can secure an IoT device and no one stakeholder should be held accountable for the overall security of the device. Effective IoT policies will facilitate cross-sector collaboration between policymakers, companies and consumers to solve cybersecurity challenges together.

5. **Government's IoT Cybersecurity Role:** The Federal Government has a critical role to play in IoT device security, particularly with regard to convening and facilitating multi-stakeholder processes that can generate industry-led, collaborative solutions to IoT cybersecurity challenges. The Federal Government should also lead by example, ensuring that it is leveraging its buying power to generate competition for security, invest in innovation, and communicate its needs to the market.

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 60 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.

BSA’s members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, Datastax, DocuSign, IBM, Mastercam, Microsoft, Oracle, salesforce.com, Siemens PLM Software, Splunk, Symantec, Tekla, The MathWorks, Trend Micro, and Workday.