ASPEN CYBERSECURITY GROUP

THE ASPEN INSTITUTE

Aspen Cybersecurity Group
Internet of Things (IoT) Security First Principles

The Aspen Cybersecurity Group is a cross-sector public-private forum comprised of former government officials, Capitol Hill leaders, industry executives, and respected voices from academia, journalism, and civil society that have come together to translate pressing cybersecurity conversations into action. At its inaugural meeting in January 2018, the group decided to focus its efforts in three key areas of need: (1) improving operational collaboration between the public and private sector; (2) developing the skills and education necessary for a workforce that will increasingly confront cybersecurity challenges; and (3) securing and ensuring confidence in emerging technologies, including the Internet of Things (IoT).

The proliferation of connected devices has created great benefits for individual consumers, businesses, and communities. Through the convenience of a handheld device, consumers can quickly arrange for transportation to their next destination, monitor their physical activity and nutritional intake, and ensure their child is sleeping safely and comfortably at home. Similarly, businesses leverage IoT to better anticipate the needs of their customers, save consumers time and money, and to automate industrial processes.

When left unsecured, however, these devices also carry increased risks to public health and safety, business operations, and individual privacy. As the attack surface continues to expand, there is an acute need to ensure the benefits of IoT—and technological innovation more broadly—are nurtured while simultaneously mitigating against the associated risks.

Changing the dynamic requires an environment that incentivizes products be secure-by-design and increases transparency to give consumers an opportunity to consider the security and privacy impacts of a product in their purchasing decisions. Towards that end, the Aspen Cybersecurity Group has articulated an overarching set of principles intended to establish common expectations for IoT product consumers and developers/manufacturers alike, both domestic and international. These principles are informed by a months-long comprehensive review of existing efforts, are geared towards consumers and product developers/manufacturers, and are put forth with a clear-eyed understanding that further work is necessary to find effective ways to encourage the adoptions of these – or similar – principles.

IoT[1] Security First Principles

1. **IoT devices should have appropriate security "Baked-In":** while difficult to achieve, the burden on consumers and those in the supply chain should be reduced by incorporating security at the design phase;

2. **There should be transparency on product security:** the security attributes of products and services should be identified and explained to promote awareness;

3. **There should be transparency on product privacy:** consumers have a right to know what their device is doing, including what data is going into the device, what data is stored on the device, and what data is going out of the device; privacy protections should be clarified and consumers should have choice and consent on how their data is used;

4. **Manufacturers/developers should be held accountable for the security of their devices:** the responsibilities of all parties should be articulated and there should be an enforcement and redress mechanism; devices should "timeout" if updates are unavailable and the device can no longer meet a minimum standard;

5. **IoT devices should have updateable security:** products and devices must be updateable and the ecosystem must be capable of addressing evolving security concerns;

6. **Security should be in multiple layers:** security controls should be equivalent across interfaces and countermeasures must perform at volume without degrading in the absence of connectivity; this includes device, router, and network;

7. **Device features should be limited by necessity:** IoT components should be stripped down to the minimum viable feature set and devices should connect carefully and deliberately.

---

[1] A common, universally applied definition or general description of IoT does not currently exist. For the purposes of the IoT Security First Principles, two definitions were relied upon by the Aspen Cyber Group. First, the IEEE's low complexity systems definition: *IoT is a network that connects uniquely identifiable "Things" to the Internet. The "Things" have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the "Thing" can be collected and the state of the "Thing" can be changed from anywhere, anytime, by anything.* A NIST draft report from February 2018 also described IoT as consisting of two foundational concepts. When combined, those concepts can form the basis of a NIST-derived definition: *Components (some of which may have sensors and actuators that allow them to interact with the physical world) that are connected by a network providing the potential for a many-to-many relationship between components.*