Considerations for Managing IoT Cybersecurity and Privacy Risks

Wednesday, July 11, 2018 | National Institute of Standards and Technology (NIST)
Administration Building 101, 100 Bureau Drive, Gaithersburg, MD

Time	Topic
7:30 AM	**Registrant Check-In** | NIST cafeteria is available to attendees
8:30 AM	**Opening Remarks** | *Green Auditorium* Kevin Stine | *Chief, Applied Cybersecurity Division, NIST*
8:40 AM	**Fireside Chat |** *Green Auditorium* Katerina Megas | *Program Lead, NIST Cybersecurity for IoT Program* Naomi Lefkovitz | *Senior Privacy Policy Advisor, NIST Privacy Engineering Program*
9:15 AM	**A Proposed IoT Model** | *Green Auditorium* Eric Simmon | *Senior Scientist, Cyber Infrastructure Group, NIST*
10:00 AM	**Breakout Session #1** **Risk Considerations for IoT** | *Portrait Room* This breakout will discuss the cybersecurity risk considerations from IoT device capabilities and the challenges in addressing these risk considerations. **Applying IT Cybersecurity Controls to IoT** | *Green Auditorium* There are numerous concerns about relying on existing IT cybersecurity controls for IoT, from the lack of controls built into many IoT devices to the negative impact some controls may cause to the physical world. This breakout session will highlight these concerns and explore how compensating controls can be leveraged to mitigate risk. **IoT Baselines and Overlays** |*West Square* Stakeholders have expressed a strong interest in cybersecurity and privacy baselines and overlays for IoT, such as minimum sets of SP 800-53 controls to be used for all IoT devices. This discussion will focus on opportunities to create IoT baselines and overlays, including the Cybersecurity Framework and SP 800-53 overlays, and examine possible candidates for inclusion. **Identifying and Managing Privacy Risks for IoT** | *Lecture Room F (Downstairs)* Privacy and cybersecurity overlap in terms of securing PII, but privacy risks extend beyond security – and can occur even when the processing of PII is authorized. This breakout will focus on these extended privacy risk considerations for IoT capabilities, as well as how to apply IT privacy controls to managing these risks.
11:30 AM	**Lunch** | NIST cafeteria is available to attendees
12:30 PM	**Breakout Session #2** | *See above for descriptions* **Risk Considerations for IoT** | *Portrait Room* **Applying IT Cybersecurity Controls to IoT** | *Green Auditorium* **IoT Baselines and Overlays** | *West Square* **Identifying and Managing Privacy Risk for IoT** | *Lecture Room C*
2:00 PM	**Break** | NIST cafeteria is available to attendees
2:15 PM	**Botnet Report Roadmap and Next Steps** | *Green Auditorium* Tim Polk |*Computer Scientist, NIST* Evelyn Remaley | *Deputy Associate Administrator, Office of Policy Analysis and Development, National Telecommunications & Information Administration*
3:15 PM	**Recap and Next Steps** | *Green Auditorium*
3:45 PM	**Adjourn** | *Green Auditorium*

Considerations for Managing IoT Cybersecurity and Privacy Risks

Wednesday, July 11, 2018 | National Institute of Standards and Technology (NIST) Administration Building 101, 100 Bureau Drive, Gaithersburg, MD

The National Institute of Standards and Technology (NIST) Cybersecurity for the Internet of Things (IoT) Program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

There has been broad support for NIST to provide guidance for federal agencies on how to secure their IoT within our Federal Information Security Modernization Act (FISMA) responsibilities. While agencies are aware that IoT affects cybersecurity and privacy risks, there remain questions about how to manage these risks.

NIST's Cybersecurity for IoT Program is drafting guidance for federal agencies on common high-level cybersecurity and privacy risks for IoT. NIST is interested in hearing practitioners' insights on managing cybersecurity and privacy risks for their IoT devices, using tools like the Cybersecurity Framework and NIST Special Publication (SP) 800-53 to help manage that risk, and specific feedback on what the use of these tools would look like.

Considerations for Managing IoT Cybersecurity and Privacy Risks

Wednesday, July 11, 2018 | National Institute of Standards and Technology (NIST)
Administration Building 101, 100 Bureau Drive, Gaithersburg, MD

Below are IoT-specific questions to think about in advance of the breakout sessions:

Risk Considerations for IoT

- *Do the risk considerations listed in the discussion draft sufficiently cover the most important risks an organization should be aware of?*
- *How is your organization addressing IoT-specific cybersecurity risks in terms of each risk consideration?*
    - *Consideration 1: Heterogeneous Capabilities*
    - *Consideration 2: Lack of Device Access, Management, and Monitoring Features*
    - *Consideration 3: Control Availability, Efficiency, and Effectiveness*

Applying IT Cybersecurity Controls to IoT

- *Which cybersecurity controls are most challenging to implement for your IoT devices?*
- *Do the five focus areas for cybersecurity risk mitigation—asset management, vulnerability management, access management, data protection, and incident detection and handling—correspond to the areas of greatest concern for your organization? If not, which areas are missing? Which are most important? Which are least important?*
- *What post-market controls would be most valuable for securing your IoT devices?*
    - *What post-market controls are your organization currently using or planning to use?*

IoT Baselines and Overlays

- *What terms are your organization using to discuss baselines and overlays?*
- *Is a universal minimum set of controls for managing IoT cybersecurity and privacy risk feasible?*
    - *Is there interest in a minimum set of controls or a tool to identify the appropriate controls for both:*
        1. *Pre-market considerations (e.g., to help with procurement decisions)*
        2. *Post-market considerations (e.g., to facilitate implementation of procured devices)*
- *How could a minimum set of controls be created and applied?*
- *Is your organization currently using or planning to use minimum sets of controls for managing these risks? To use a tool to identify the appropriate controls?*
- *Which controls are most important to include in a minimum set?*

Identifying and Managing Privacy Risks for IoT

- *Do the risk considerations listed in the discussion draft sufficiently cover the most important risks an organization should be aware of?*
- *How is your organization addressing IoT-specific privacy risks in terms of each risk consideration?*
    - *Consideration 1: Heterogeneous Capabilities*
    - *Consideration 2: Lack of Device Access, Management, and Monitoring Features*
    - *Consideration 3: Control Availability, Efficiency, and Effectiveness*
- *Have you heard any concerns from individuals you interact with about the connectedness of certain devices?*
- *Which privacy controls are most challenging to implement for your IoT devices?*
- *What post-market controls would be most valuable for protecting individuals' privacy on devices?*
    - *What post-market controls are your organization currently using or planning to use?*