RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: MBS-F01

IoT and Supply Chain Risk Management

Daniel Kroese

Associate Director, National Risk Management Center
Cybersecurity and Infrastructure Security Agency
DHS
@dgkroese

Setting the Stage

- Cybersecurity Supply Chain Risk Management (C-SCRM) has emerged as a central issue in cybersecurity and infrastructure protection issues.
- The severity of the threat landscape is real and becoming more widely understood.
- Tens of billions (and growing) connected devices globally and enhanced IoT connectivity through 5G will only increase the need for organizations to better understand their digital footprint and associated IoT risks.
- DHS – through the Cybersecurity and Infrastructure Security Agency – leads the national effort to defend our critical infrastructure against the threats of *today* while working with partners to secure against the evolving risks of *tomorrow*.
- Cybersecurity Supply Chain Risk Management, features prominently in this mission.

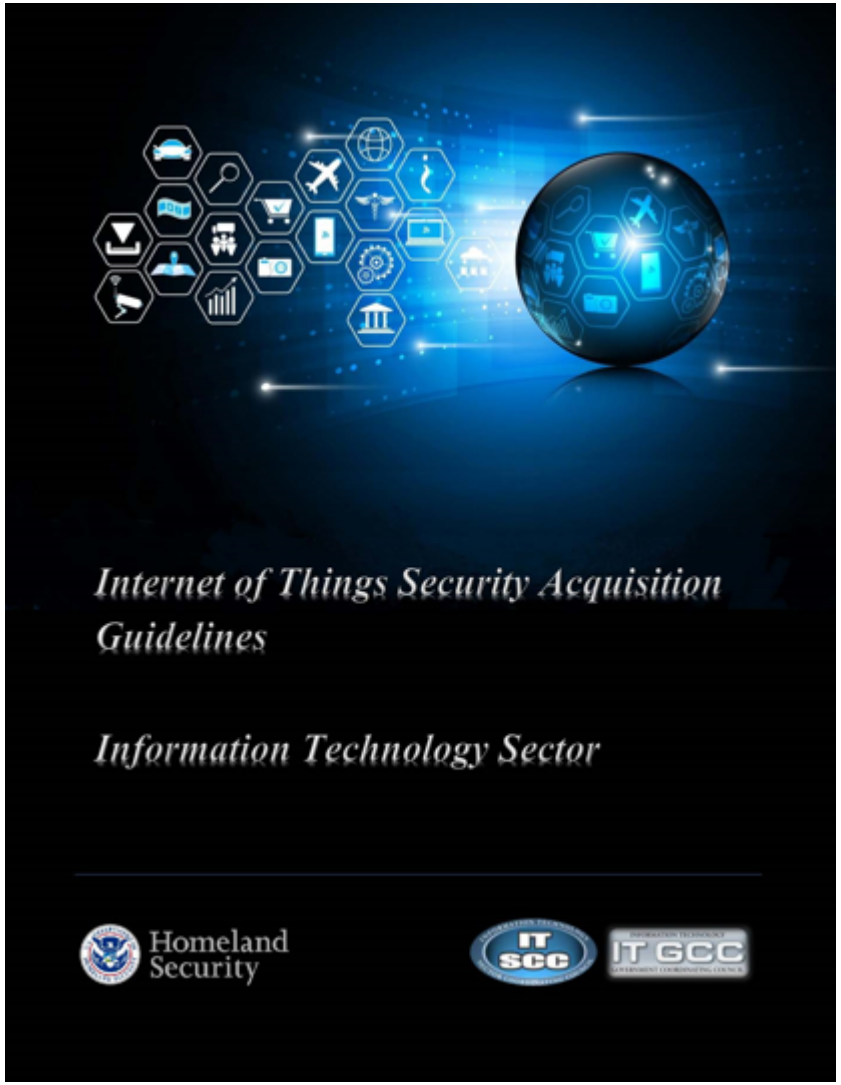
The Power of Federal Procurement

- Some market moving ability – annual government IT spend close to $100 billion per year.
- Reputational benefits for IoT manufacturers to maintain productive partnerships with the federal government.
- The power of setting a visible “North Star” can lead to voluntary change in behavior without additional acquisition requirements – e.g. Kaspersky Labs Binding Operational Directive (BOD) issued in September 2017 was followed by private sector entities not mandated by the scope of the BOD.

Recent Developments

- 2019 is shaping up to the “year of supply chain.”
- The enactment in late 2018 of the *Federal Acquisition Supply Chain Security Act* is significant.
- The ICT Supply Chain Risk Management Task Force sponsored by CISA brings together 40 of the largest players in the IT and Communications Sector and 20 supply chain leaders across the federal government.

The IoT Buyers Guide



- To be released soon
- Joint effort between DHS, IT SCC, and IT GCC
- Core audience is the acquisition team at federal agencies
- Recommended framework is non-binding and voluntary

CISA CYBER+INFRASTRUCTURE

IoT versus ICT

- For IoT, focus on the “thing”
- For example, a connected car would be considered IoT while the components that enable the connectivity are ICT.
- Many IOT and ICT risks are similar.
- However, some of the risks introduced by IoT devices, systems, and services differ from ICT - .e.g. the specific challenges associated with connecting IoT to operational and legacy systems.

IoT Examples

- HVAC
  - A modern heating and cooling system uses digital technology for both sensor and control functions; thermostats are no longer operated by coil-metal thermometers and physical switches.
- Smart TV
  - Currently, most televisions for sale contain “smart” functionality and include applications for various video content providers and often provide interactive functionality including microphones and cameras.
- Connected Car
  - Vehicles 1) interact with surrounding technology and physical environment, 2) connect with driver or passenger devices to perform functions, and 3) collect information via sensors to communicate back to a central organization (e.g. fleet management).

IoT Cybersecurity Throughout the Acquisition Lifecycle

Important IOT technology security considerations include:

- Poor design (use of plaintext and hard-coded passwords).
- Coding flaws (buffer overflows and command injection).
- Inconsistent patching of software.

The IoT Threat

- Distributed Denial of Service (DDoS)
- Data Manipulation and Privacy Leakage
- Third Party Access and Control

IOT Acquisition Lifecycle

- Assess Need
  - Purpose identification and connectivity determination
- Analyze & Select
  - Acquisition planning and requirements development
- Obtain
  - Solicitation development and contract award
- Deploy and Support
  - Contract administration and closeout

Acquisition Lifecycle – Key Threshold Issues

- Mission: For what purpose is the IoT technology being procured?
- Network/System: Is the IoT technology intended to be connected?
- Information Sharing: Is the IoT technology collecting sensor data that is sent elsewhere?
- Operating Risk: Is the IoT technology controlling physical items as part of its functionality?

IoT Technology Issues

- Type and Control of Connectivity
- Third Party Services and Data Management
- Patching
- General Vendor Cybersecurity Practices
- Security of Devices, Systems, Services, and Communications

Applying this Framework for Smarter IoT Acquisition

- The IoT Buyer's Guide provides fundamental considerations an organization should take before acquiring and deploying an IoT device, system, or service.
- Understanding IoT cybersecurity concerns across the entire acquisition lifecycle is paramount.
- The entire Acquisition Team should have access to and knowledge of risk-informed, decision-making methods when procuring, deploying, using, and sustaining IoT.