IT Sector IoT Security Working Group

Briefing for Software and Supply Chain Assurance Forum

August 29, 2017

Overview

- Working group consists of personnel from IT Sector Coordinating Council and DHS Office of Cybersecurity and Communications.

- Focus is IoT implementations most prevalent in the Federal environment and to identify baseline security considerations applicable to acquisitions of those IoT systems and devices.

- Primary audience is the Federal Acquisition Team, including but not limited to the government’s Program Office, IT Security, Legal, and Contracting Office personnel.

Guidance Outline

- Overview of IoT Cybersecurity Considerations
  - ➢ *Identification of IoT Solution Characteristics:* characteristics of IoT that should be identified in the early stages of the acquisition and procurement lifecycles.
  - ➢ *Definition of Base Requirements*: how basic cybersecurity requirements can be grouped by IoT characteristic or function (tasks to be performed, performance required, essential physical characteristics, etc.).
  - ➢ *Security Implementation Guidance:* introduce the Cybersecurity Framework and provide an overview of cybersecurity activities related to deploying IoT and their relationship to the CSF Functions and Categories.

Guidance Outline (cont’d)

- Procurement Lifecycle Mapping:
    - *Requirements Development*: best practices for identifying and documenting IoT characteristics during the requirements definition process, including:
        - Mission Needs; and
        - Operational Requirements.
    - *Acquisition Planning:* best practices for addressing IoT security during the acquisition planning process, including:
        - Industry/Vendor Engagement;
        - Contract type;
        - Independent cost estimates;
        - Market Research; and
        - Price-performance tradeoff considerations.

Guidance Outline (cont’d)

- Procurement Lifecycle Mapping (cont’d):
  - ➢*Solicitation Development and Contract Award:* best practices for addressing IoT risks during the solicitation development and contract award processes, including:
    - ❑Source Selection and Evaluation Criteria;
    - ❑Price/Cost and Technical Evaluations;
    - ❑Deliverables;
    - ❑Developing meaningful Key Performance Indicators (KPIs) for IoT;
    - ❑Risk Assessment of IoT deliverables, contractors and subcontractors.
  - ➢*Contract Administration and Closeout:* best practices for addressing IoT risks during the contract administration and closeout processes, including:
    - ❑Tracking vendor performance against KPIs; and
    - ❑Ensuring proper disposal of IoT device.

Guidance Outline (cont’d)

- Additional Considerations for Implementation
  - ➢additional cybersecurity considerations not specified in the previous sections.
- Integrating New and Legacy Capabilities
  - ➢cybersecurity considerations specific to connecting new IoT systems and devices to legacy systems.
- References and Additional Resources
  - ➢references and links to additional standards and resources to the topics above.

Timeline

- Sep 6th – WG approval of outline
- Q1FY2018 – first draft guidance document
- Q2-Q3FY2018 – final guidance document

- Comments? Edits? Suggestions? Want to participate in WG?
    - ➢Send to: emile.Monette@hq.dhs.gov