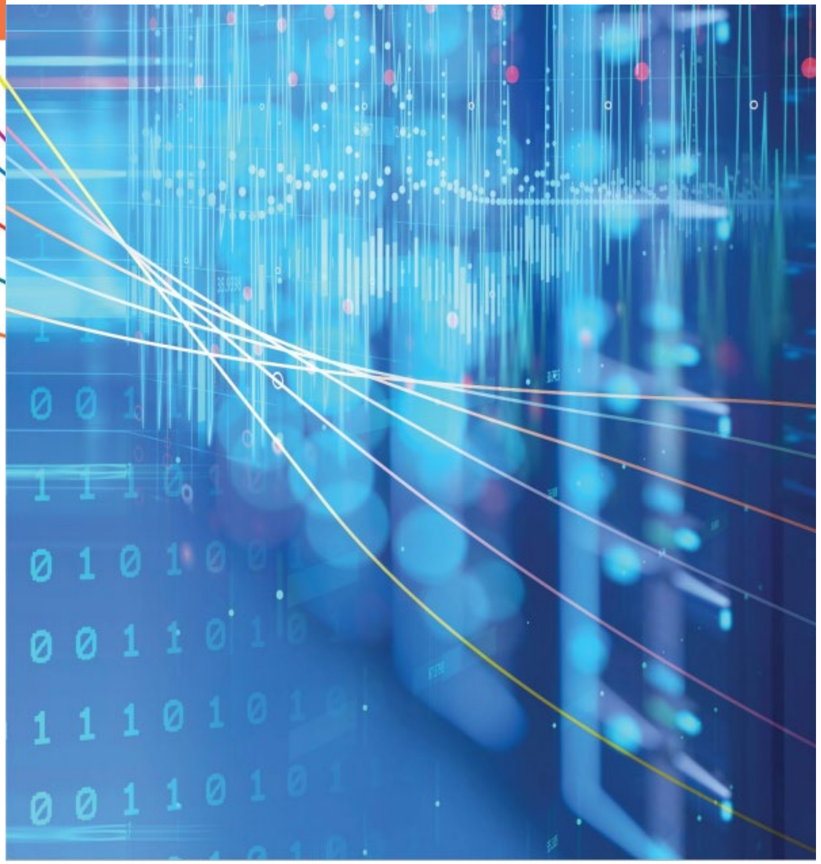
Report to NIST IoT Advisory Board



July 18, 2023

Presenter: Paul Eisler, USTelecom Vice President
Cybersecurity

USTELECOM
THE BROADBAND ASSOCIATION

Core IoT Security Policy Principles

These principles are derived from the Council to Secure the Digital Economy (CSDE) IoT Security Policy Principles, endorsed by 27 leading technology and security organizations.

CSDE was co-founded by USTelecom and the Consumer Technology Association (CTA) and currently includes 15 global ICT companies.

Learn more at **CSDE.org**

1. IoT Can Rely on Existing Security Policy Principles

- **Harmonization**
- **Interoperable Approach**
- **Design Neutrality**
- **Flexible Adoption of Consensus-based Standards**

💡 These principles will ensure policy and regulatory frameworks can comport with evolving technical landscapes in a **flexible manner**, while **promoting innovation** and certainty for businesses developing IoT products.

2. Leverage Existing Consensus-Based Standards and Best Practices on IoT Security

- Consider frameworks that create proper incentives (legal, such as liability protections and safe harbors) to foster the adoption of such standards by industry, and **avoid divergence** from these key practices.

- Make consistent use of clear definitions based on such consensus efforts to **avoid fragmentation**.

💡 Standards-driven approaches facilitate interoperability across IoT ecosystems, foster innovation and technology development, improve international collaboration, serve as the basis for market-tested attestation and certification frameworks, and enable cost-effective security solutions.

3. The Risk Analysis Approach

- Applicability of IoT security capabilities depends on:
  - Device complexity
  - Deployment environment
  - Risk management profile
  - Use case
  - Context

Policies that allow for the flexible adoption of standards based on the risk management profile of particular industry verticals and enterprises will enable manufacturers to better identify and remedy security threats that arise.

4. Leverage Public-Private Partnerships and Multi-Stakeholder Efforts

- Private-public partnerships are an important mechanism to incentivize the adoption and deployment of secure IoT devices.

- Further consider supporting multi-stakeholder efforts as well as studying and addressing potential barriers to international standards development in these domains.

💡 Successful public-private sector collaboration should provide ample time for consultation and seek to avoid duplicative or counterproductive and conflicting regulatory approaches.

5. A Thoughtful and Holistic Approach to Device Security

- The IoT landscape is diverse and complex. Regulatory policies should therefore comport with policy and security principles underpinning domains that closely interact with this ecosystem (e.g., cloud security, consumer products, 5G, and telecom security).

- Consider security practices that may extend beyond the observable device characteristics, such as risk assessment and secure development.

6. Consider Existing Self Attestation and Conformity Assessments

- Contrary to the argument for mandatory certification or labeling, security is enhanced by policies that preserve flexibility and allow for alternative approaches to demonstrating compliance.

- The ability to leverage multiple alternatives is instrumental since many valid approaches are used by vendors globally to address security risks.

💡 Utilizing industry’s experience in varied approaches increases the security delivered to the marketplace as a whole, and promotes interoperability, scalability, and innovation.

International Standards & Competition

The following recommendations were endorsed by six leading trade associations representing the Communications and IT sectors to ensure that U.S. technology firms continue to be able to compete on a global scale.

Full report available at USTelecom.org (click here)

International Standards Policy Recommendations

- Facilitating the hosting of global standards and specification-setting bodies meetings in the U.S. would facilitate greater industry and U.S. government participation in standards and specification development organizations.
    - Global bodies typically avoid holding their meetings in the U.S. because visa processes or overt visa restrictions often make it very difficult for foreign participants to attend in a timely manner.

- In international bodies that are member state or government-driven, such as ITU-T, the U.S. should seek like-minded government partners to reform such body's governance and working methods, and to focus on the appropriate technology within the scope of that organization.

- Provide targeted financial incentives to support participation in industry-driven global standards and specification development bodies.

Questions/Discussion