AMPERE

IOT CYBERSECURITY IMPROVEMENT ACT OF 2020

7th annual Control Systems Cyber Security USA Conference

CyberSenate – March 31, 2021

INTRODUCTION

- Former utility staff (telecommunications, water & electric)
- First NERC CIP auditor in the US
- Drafter of NERC CIP standards and formal interpretations
- NERC CIP Supply Chain Working Group contributor
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Director and President Emeritus
- Centro de Ciberseguridad Industrial (CCI) US Coordinator
- Ampere Industrial Security
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- Advisor to multiple industrial security product vendors
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP

WHAT IS IOT (IIOT)?

- Legal definitions for IT, OT, IOT and IIOT are challenging
- *"…have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices…"*
- *"…the extension of internet connectivity into physical devices and everyday objects."*
- Other people's computers in your home or business
- Has widespread inertia and install base already
- Installations will significantly expand with 5G, satellite internet and even more inexpensive sensors
- Tracking to exceed 21.5 billion devices by 2025, possibly up to 75B
- Very long list of attacks (DDOS), botnets, data exfiltration, etc.

[PARTIAL] SCOPE OF THE PROBLEM

- Lower cost per device; higher volume deployment
- Lower computing power; can't handle a lot of the IT security stuff
- Hyperembeddedness
- Always-on network connectivity, often directly to Internet
- Ease of use prioritized, not security
- APIs and interaction with everything
- The companion "app" could be even worse
- Rushed to market, security de-prioritized if even considered
- Disruptive space with rapid shifts and entire tech platforms left behind
- Disposability paradox for consumer vs. industrial
- Responsible for almost a third of all mobile and Wi-Fi network infections
- Generally considered an example of bad security practice

OVERALL LEGAL LANDSCAPE

- Three different IOT legal regimes in the US
  - State level: targets manufacturers, defined broadly, likely up to AG
  - FTC: focus on consumer-level goods
  - Federal: targets IOT devices through government purchasing process
- Manufacturers should consider programmatic approach to security with demonstrable secure development (pre-sale) and maintenance (post-sale)
- Organizations/Agencies should have a security program that governs the integration and use of these devices
- Common threads:
  - Identity management
  - Patching
  - Configuration management
- Demonstrable (documented) controls are best defense for everyone

CALIFORNIA PRECEDENT

- Regulated companies that manufacture connected devices sold in the state
- A “connected device” is any device that connects to the internet, directly or indirectly
- Connected devices must have “reasonable” security features:
  - Appropriate to the nature and function of the device
  - Appropriate to the information the device may collect
  - Designed to protect both the device and its information from unauthorized access
- Pretty much left up to the AG to decide what is reasonable
- Oregon soon followed, as did Europe, Singapore, Australia…

IOT CYBERSECURITY IMPROVEMENT ACT OF 2020

- Enacted December 4, 2020
- *"…to establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes."*
- *"minimum information security requirements for managing cybersecurity risks associated with such devices."*

- Affects the purchase and use of IoT devices by federal government agencies
- Requires the NIST and the OMB to take specified steps to increase cybersecurity in respect of such IoT devices

IOTCIA2020 REQUIREMENTS

- NIST must “develop and publish standards and guidelines for the federal government on the appropriate use and management by agencies of IoT devices owned or controlled by an agency and connected to information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices.”

- The act also requires the OMB to review agency information security policies and principles on the basis of the NIST standards and guidelines, and issue such policies and principles as necessary to ensure the agencies’ policies and principles are consistent with the NIST standards and guidelines.

IOTCIA2020 REQUIREMENTS

- Require NIST to publish standards and guidelines on the use and management of IoT devices by the federal government, including minimum information security requirements for managing cybersecurity risks associated with IoT devices
- Direct OMB to review federal government information security policies and make any necessary changes to ensure they are consistent with NIST's recommendations
- Require NIST and OMB to update IoT security standards, guidelines and policies at least every five years
- Prohibit the procurement or use by federal agencies of IoT devices that do not comply with these security requirements, subject to a waiver process for devices necessary for national security, needed for research or that are secured using alternative and effective methods

IOTCIA2020 REQUIREMENTS

- Require NIST to publish guidelines for reporting security vulnerabilities relating to federal agency information systems, including IoT devices
- Direct OMB to develop and implement policies that are necessary to address security vulnerabilities relating to federal agency information systems, including IoT devices, consistent with NIST's published guidelines
- Require contractors providing IoT devices to the U.S. government to adopt coordinated vulnerability disclosure policies, so that if a vulnerability is uncovered, that information is disseminated
- Updates to the Federal Acquisition Regulation for consistency with the NIST standards and guidelines

IOTCIA2020 REQUIREMENTS

- New standards and guidelines to be consistent with NIST's current guidance regarding:
  - Vulnerability identification and management
  - Secure development
  - Identity management
  - Patch management
  - Configuration management

RELEVANT NIST DOCUMENTS

IOT CIA Law

NIST SP 800-213

NIST IR 8259	NIST IR 8259A	NIST IR 8259B	NIST IR 8259C	NIST IR 8259D

RELEVANT NIST DOCUMENTS

- **SP 800-213:** IoT Device Cybersecurity Guidance for the Federal Government - Establishing IoT Device Cybersecurity Requirements
- **IR 8259:** Foundational Cybersecurity Activities for IoT Device Manufacturers
- **IR 8259A:** IoT Device Cybersecurity Capability Core Baseline
- **IR 8259B:** IoT Non-Technical Supporting Capability Core Baseline
- **IR 8259C:** Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline
- **IR 8259D:** Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

NIST SP 800-213

- Links and alignment with CSF, RMF, 800-53 and FISMA
- 10 questions…
  - What is the benefit of the IoT device and how will it be utilized?
  - What data is collected?
    - Personal, confidential/federal, environmental
  - In what technologies will the data be stored?
  - In what geographic areas will the data be shared and/or stored?
  - With what other third parties will data from, or about, the IoT devices be shared and/or stored?
  - Might the device interfere with other aspects of operations or system functionality?
  - Would the IoT device introduce unacceptable risks to the agency or result in noncompliance with cybersecurity requirements?
  - Is the IoT device known to have had published security and/or privacy 524 vulnerabilities?
  - Does the IoT device lack key device cybersecurity requirements?
  - Will the implementation or maturity of device cybersecurity capabilities and/or non-technical supporting capabilities fail to satisfy the agency's key device cybersecurity requirements?

NIST IR 8259

- Core Cybersecurity Feature Baseline for Securable IoT Devices
- Describes recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to [federal] customers:
  - Encryption at rest and in transit
  - Security by design
  - Software and firmware updates
  - Security incident logs
  - Restricted access to local and network interfaces
  - Identification and authentication protocols

NIST IR 8259A

- IoT Device Cybersecurity Capability Core Baseline
  - Provide organizations a starting point to use in identifying the core device cybersecurity capabilities for new IoT devices they will manufacture, integrate, or acquire.
  - Device cybersecurity capabilities:
    - Device Identification
    - Device Configuration
    - Data Protection
    - Logical Access to Interfaces
    - Software Update
    - Cybersecurity State Awareness

NIST IR 8259B

- IoT Non-Technical Supporting Capability Core Baseline
- Complements the NIST IR 8259A by detailing additional, non-technical supporting activities typically needed from manufacturers and/or associated third parties
  - Documentation
  - Information and Query Reception
  - Information Dissemination
  - Education and Awareness

NIST IR 8259C

- Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline
- Complements the NIST IR 8259A and 8259B by guiding organizations needing to define more detailed capabilities
- Expands upon A&B based on more specific contextual information
- Method used to create the profile meeting the requirements of the federal information system low baseline found in NIST IR 8259D

NIST IR 8259D

- Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

- Example result of applying the NIST IR 8259C process against the requirements of the FISMA process and SP 800-53

BENEFITS

- Federal law on IOT sets minimum bar for all agencies
- Should adapt with technology
- Potentially useful reports based on actuarial data
- Advances vulnerability reporting and disclosure discussion
- Trickle-down effect through the supply chain
- Sets a precedent for the private sector as well
- Signals increasing future enforcement and regulation of IOT
- Likely to influence state law and private sector practices
- Many IOT devices sold to the federal government that meet the NIST bar will also be sold to the private sector
- NIST standards have a broader impact on security practices across the IoT industry

CHALLENGES

- Does not set any minimum threshold for standards
- What about legacy?
  - “All government agencies can no longer renew procurement contracts with companies where their IoT devices will not comply with NIST standards and guidelines as of 12/5/2020”
- “…secured using alternative and effective methods
  - Implies an ecosystem perspective and allows some flexibility
- May have some interesting overlaps or conflicts with existing regulations like NERC CIP
- Cost will likely increase for “NIST compliant” devices
- Vulnerability reporting and disclosure is hotly debated
- EULA restrictions are not addressed (bug bounties?)
- Serial not included in examples of network interfaces in IR 8259

IOTCIA2020 SUMMARY

- NIST will create standards and guidelines
- OMB will assess and “enforce” within govt agencies
- Applies to purchase and use of IOT
- Will likely trickle down to private space
- Standardizes vulnerability reporting and disclosure
- Updates to standards and guidelines within 5 years
- Regular reports
- Coverage areas include
  - Vulnerability identification and management
  - Secure development
  - Identity management
  - Patch management
  - Configuration management

CONTACT ME


@PATRICKCMILLER


LINKEDIN.COM/IN/MILLERPATRICKC


PMILLER@AMPERESEC.COM


WWW.AMPERESEC.COM


+15032721414