May 25, 2021

Developments in IoT Security

Katerina Megas
National Institute of Standards & Technology

Robert Morgus
U.S. Cyberspace Solarium Commission

James Trilling
Federal Trade Commission

Erik Jones
Venable LLP

Privacy+ Security Forum

Developments in IoT Security

- **The Need for IoT Security**

- **Government Response**
  - NIST's Role in IoT Security
  - Solarium Commission Proposals
  - Current FTC Enforcement

- **The Road Ahead – the Administration's Executive Order & International Developments**

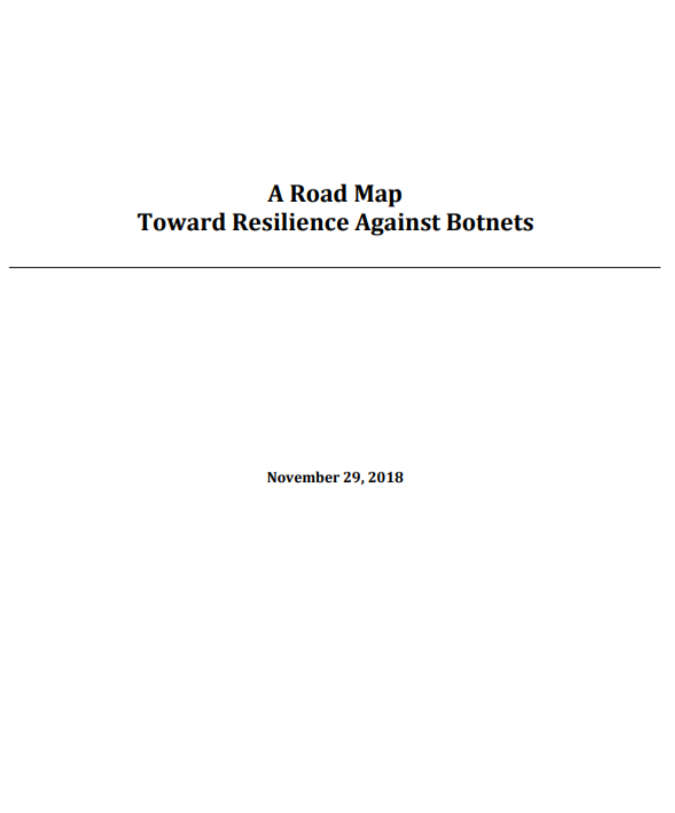
How IoT Security Became a Priority

Privacy+ Security Forum

How IoT Security Became a Priority

- ***Stunning Growth and Adoption***
  - Estimates have the global IoT market at a value of nearly $1.4 trillion by 2026. Up from approximately $761 billion in 2020.
  - In 2010, there were approximately 800 million active IoT device connections worldwide. In 2025, estimates have the number at over 30 billion.

- ***Targets for Hackers and Cybercriminals***
  - Spreading malware via IoT devices
  - Hacking cameras and other smart home devices
  - Botnets (*e.g., the Mirai Botnet)*



A Road Map
Toward Resilience Against Botnets

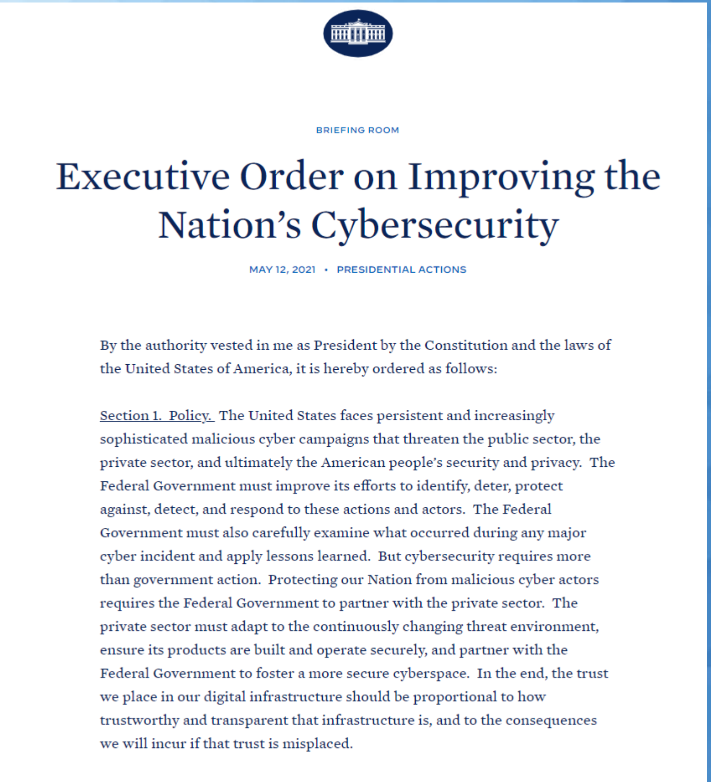
November 29, 2018

Action on IoT Security During the Trump Administration

Recent IoT Security Laws

- **2018 – *California passes first IoT security law***
  - Requires manufacturers of connected devices to equip the device with a “reasonable security” feature or features.
  - Provisions specifically tied to preprogrammed passwords and authentication during initial access
- **2019 – *Oregon passes IoT security law***
- **2020 – *President Trump Signs the Internet of Things Cybersecurity Improvement Act of 2020***
  - Requires IoT devices purchased by the government to meet minimum security requirements.
  - NIST directed to create security standards for development, patching, and identity configuration management of IoT.
  - OMB required to review agency information security policies and principles on the basis of NIST standards and guidelines.
  - Vendors will also be required to have a formal process of how vulnerabilities are reported.

Continued Action on IoT Security During the Biden Administration



BRIEFING ROOM

Executive Order on Improving the Nation’s Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Overview of NIST’s Efforts

Kat Megas

Privacy+ Security Forum

NIST and work that advances cybersecurity of the Internet of Things

- Non-Regulatory agency and technical arm of the U.S. Department of Commerce
- NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
- In accordance with the Federal Information Security Modernization Act (FISMA), NIST develops information security standards and guidelines for federal information systems.

IoT cybersecurity related initiatives

Research/Reports

- Mitigating IoT-Based DDoS/Botnet Report
- Cybersecurity for Cyber Physical Systems
- Cybersecurity Framework
- Cybersecurity Framework Manufacturing Profile
- Cybersecurity for Smart Grid Systems
- Cyber Threat Information Sharing
- Lightweight Encryption
- Low Power Wide Area IoT
- Network of Things
- Report on State of International Cybersecurity Standards for IoT
- Security and privacy concerns of intelligent virtual assistances
- Security of Interactive and Automated Access Management Using Secure Shell (SSH)
- Considerations for Managing IoT Cybersecurity and Privacy Risks
- Core Cybersecurity Feature Baseline for Securable IoT Devices
- Trustworthy Network of Things

Special Publications

- BLE Bluetooth
- Cloud security
- Digital Identity Guidelines
- Guide to Industrial Control Systems (ICS) Security
- RFID Security Guidelines
- Software Assessment Management Standards and Guidelines
- Supply Chain Risk Management
- Security Content Automation Protocol (SCAP) Standards and Guidelines
- Security Systems Engineering
- ABCs of Conformity Assessment
- Conformity Assessment Considerations for Federal Agencies

Applied

- Galois IoT Authentication & PDS Pilot
- GSMA Trusted Identities Pilot
- National Vulnerability Database
- Securing the Industrial IoT (IIoT)
- IIoT-Based Automated Distributed Threats
- Capabilities Assessment for Securing Manufacturing Industrial Control Systems
- Security Review of Consumer Home IoT Products
- Security for IoT Sensor Networks
- Healthcare Sector Projects
  - Wireless Infusion Pumps
  - Securing Telehealth Remote Patient Monitoring Ecosystem
- Privacy Engineering Program
- Zero Trust Architecture Project
- IoT Device Network-Layer Onboarding Taxonomy

The IoT Cybersecurity Program charter established end of 2016 with three overarching program goals

Standards
Guidelines
Tools
Stakeholder
Engagement
Trust
Innovation

Support 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.

Collaborate with stakeholders across government, industry, international bodies, and academia

Cultivate trust and foster an environment that enables innovation on a global scale

The NIST Information Technology Lab's purpose is to cultivate trust in IT and metrology.

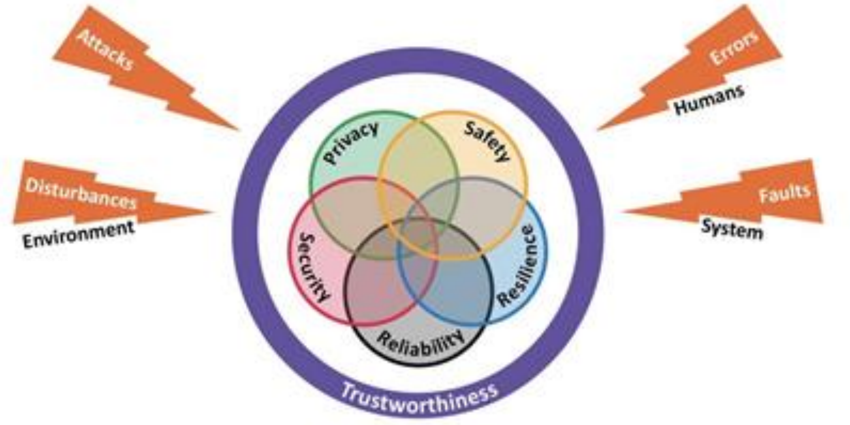
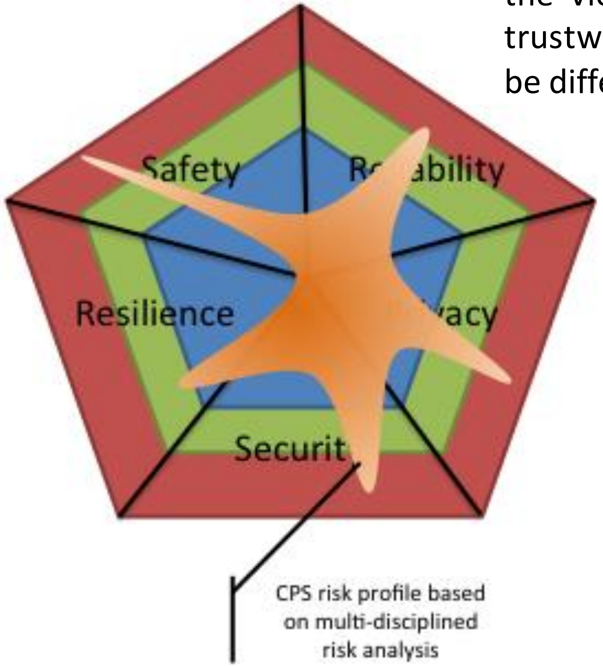


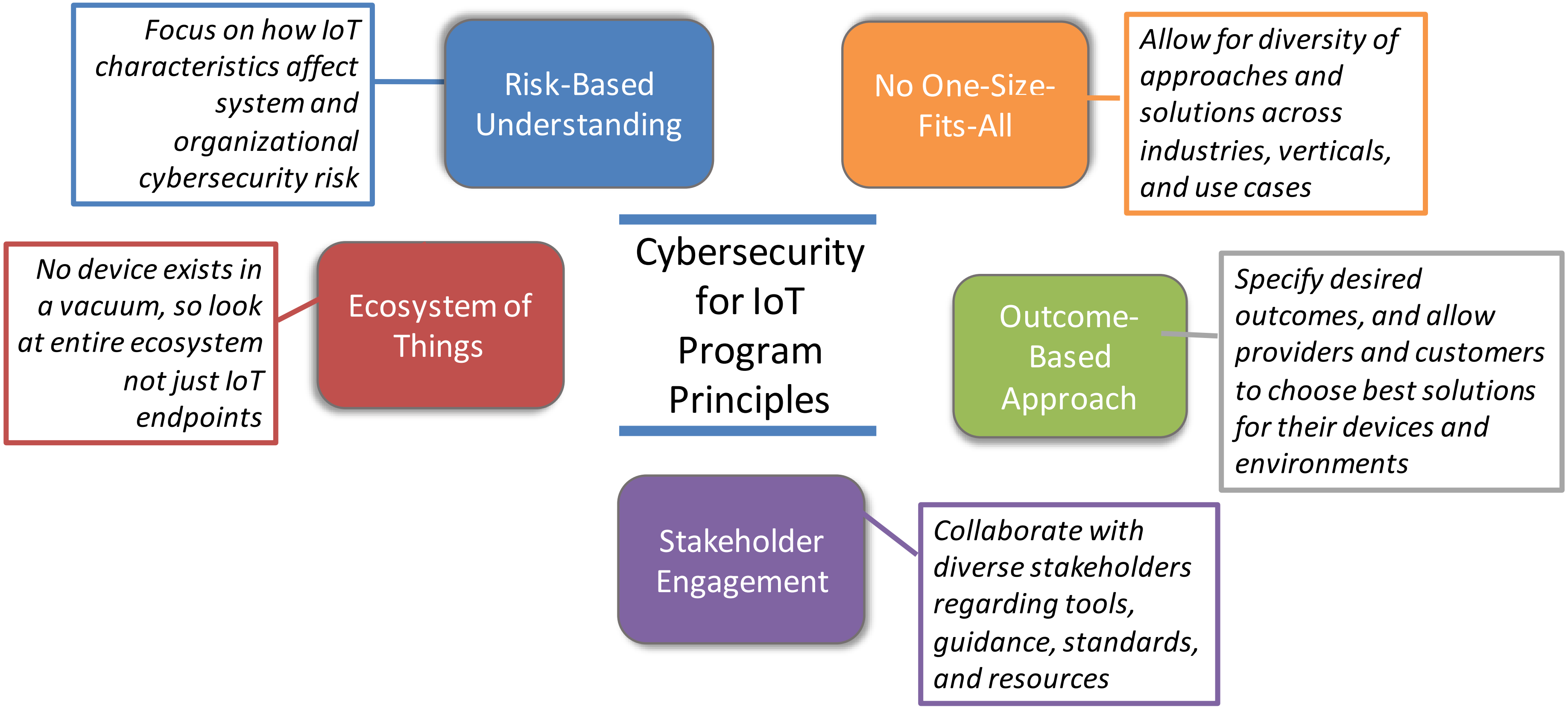
Figure 1: IoT Trustworthiness - IIC Industrial Internet Security Framework - source IIC IISF

Organizations need to consider all 5 aspects of Trustworthiness: Safety, Security, Privacy, Resilience and Reliability

Depending on the risk the 'view' of the trustworthiness will be different



Five principles guide how we approach solutions and program direction



Cybersecurity for IoT Program Principles

Risk-Based Understanding

Focus on how IoT characteristics affect system and organizational cybersecurity risk

No One-Size-Fits-All

Allow for diversity of approaches and solutions across industries, verticals, and use cases

Ecosystem of Things

No device exists in a vacuum, so look at entire ecosystem not just IoT endpoints

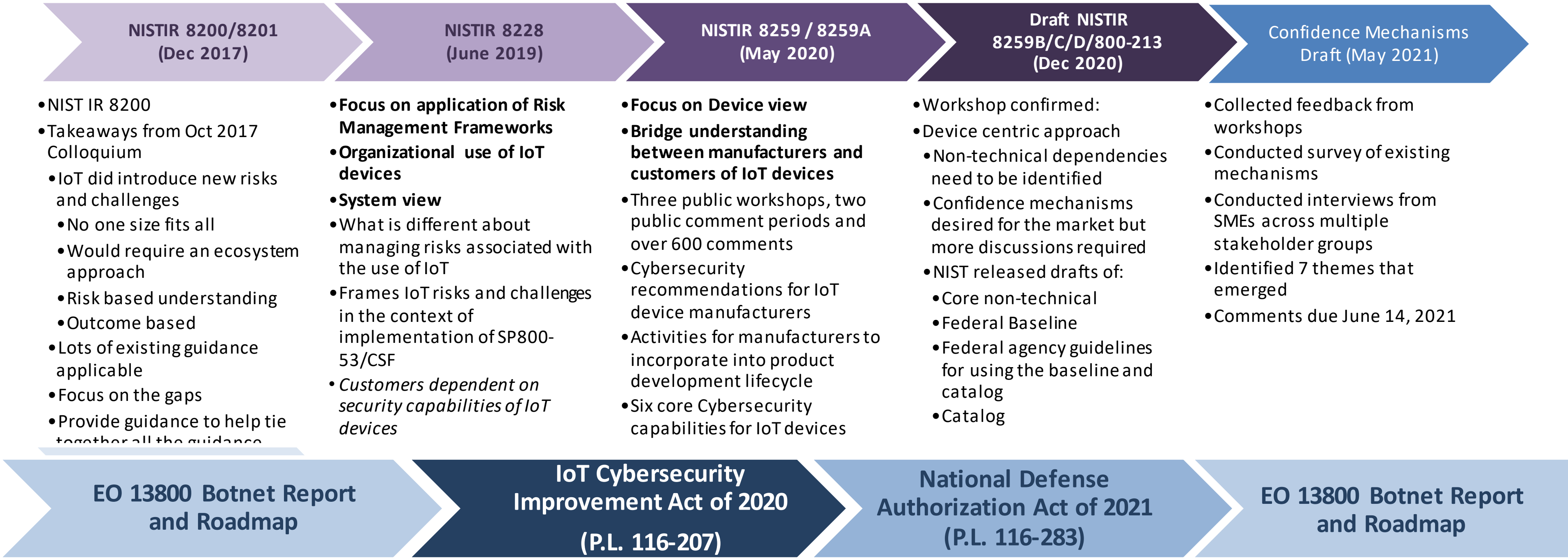
Outcome-Based Approach

Specify desired outcomes, and allow providers and customers to choose best solutions for their devices and environments

Stakeholder Engagement

Collaborate with diverse stakeholders regarding tools, guidance, standards, and resources

Key events and drivers for the NIST IoT Cybersecurity Program



NISTIR 8200/8201 (Dec 2017)

- NIST IR 8200
- Takeaways from Oct 2017 Colloquium
  - IoT did introduce new risks and challenges
    - No one size fits all
    - Would require an ecosystem approach
    - Risk based understanding
    - Outcome based
  - Lots of existing guidance applicable
  - Focus on the gaps
  - Provide guidance to help tie together all the guidance

NISTIR 8228 (June 2019)

- **Focus on application of Risk Management Frameworks**
- **Organizational use of IoT devices**
- **System view**
- What is different about managing risks associated with the use of IoT
- Frames IoT risks and challenges in the context of implementation of SP800-53/CSF
- *Customers dependent on security capabilities of IoT devices*

NISTIR 8259 / 8259A (May 2020)

- **Focus on Device view**
- **Bridge understanding between manufacturers and customers of IoT devices**
- Three public workshops, two public comment periods and over 600 comments
- Cybersecurity recommendations for IoT device manufacturers
- Activities for manufacturers to incorporate into product development lifecycle
- Six core Cybersecurity capabilities for IoT devices

Draft NISTIR 8259B/C/D/800-213 (Dec 2020)

- Workshop confirmed:
- Device centric approach
  - Non-technical dependencies need to be identified
  - Confidence mechanisms desired for the market but more discussions required
  - NIST released drafts of:
    - Core non-technical
    - Federal Baseline
    - Federal agency guidelines for using the baseline and catalog
    - Catalog

Confidence Mechanisms Draft (May 2021)

- Collected feedback from workshops
- Conducted survey of existing mechanisms
- Conducted interviews from SMEs across multiple stakeholder groups
- Identified 7 themes that emerged
- Comments due June 14, 2021

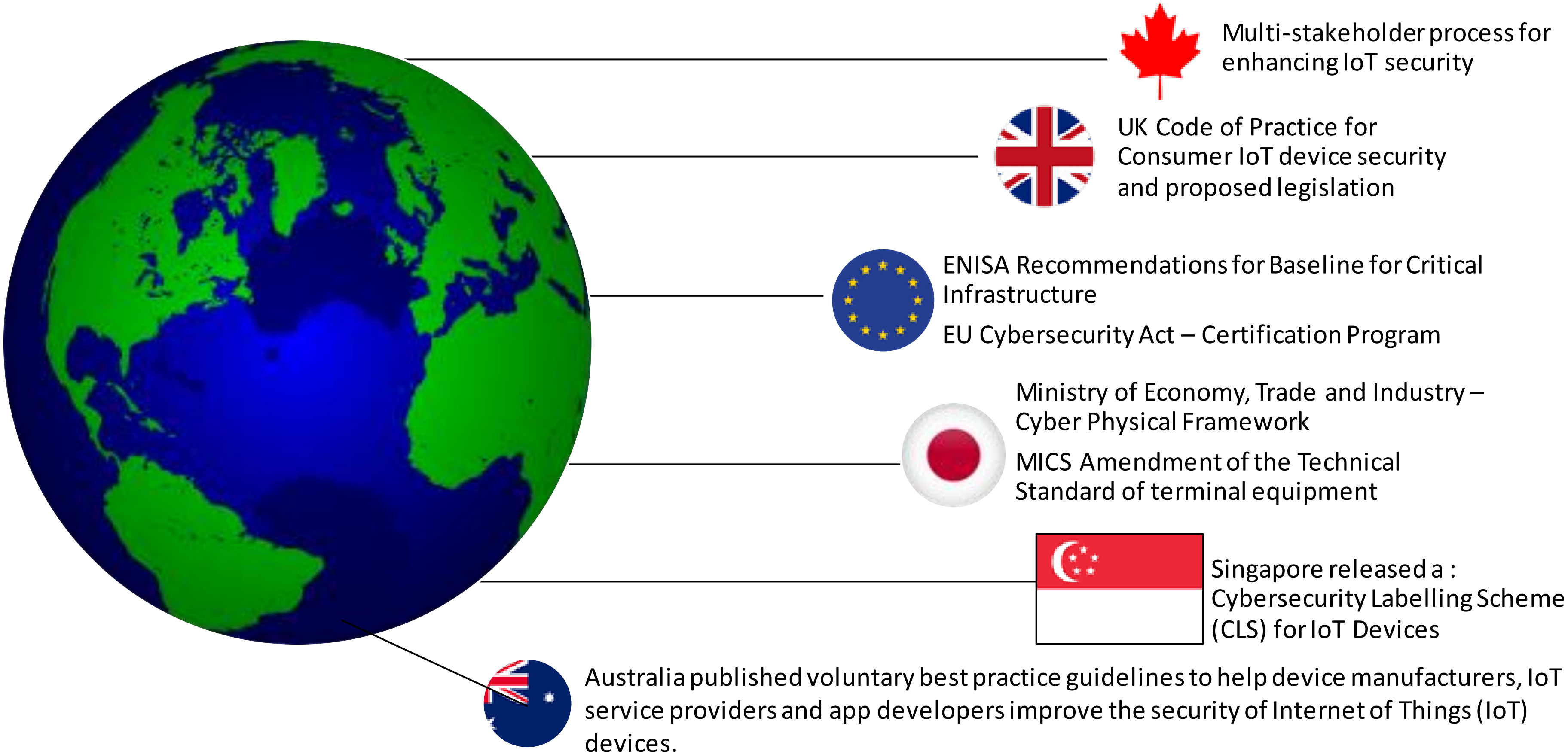
EO 13800 Botnet Report and Roadmap

IoT Cybersecurity Improvement Act of 2020 (P.L. 116-207)

National Defense Authorization Act of 2021 (P.L. 116-283)

EO 13800 Botnet Report and Roadmap

IoT security is a global concern evidenced by multiple countries approaching security of devices



Multi-stakeholder process for enhancing IoT security

UK Code of Practice for Consumer IoT device security and proposed legislation

ENISA Recommendations for Baseline for Critical Infrastructure

EU Cybersecurity Act – Certification Program

Ministry of Economy, Trade and Industry – Cyber Physical Framework

MICS Amendment of the Technical Standard of terminal equipment

Singapore released a : Cybersecurity Labelling Scheme (CLS) for IoT Devices

Australia published voluntary best practice guidelines to help device manufacturers, IoT service providers and app developers improve the security of Internet of Things (IoT) devices.

•International standards can provide means to satisfy
•government and market needs while supporting confidence

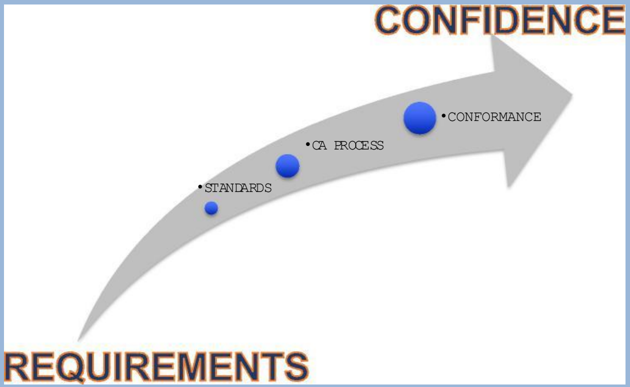
NIST

•ISO/IEC JTC 1 27400 – Cybersecurity – IoT security and privacy – Guidelines: currently in 2nd committee
•draft

•ISO/IEC JTC1 27402 - Cybersecurity – IoT Security and Privacy – Device Baseline Requirements: 1st
•committee draft (US/France/Israel co-editors)

•Multiple other efforts relating to sector specific and
•protocol specific efforts such as:

- IEEE/UL P2933 – Standard for clinical internet of
  •things
- ETSI 303 645 - Cyber Security for Consumer
  •Internet of Things: Baseline Requirements
- IETF – MUD and Device Onboarding
- IEC 62443- Industrial Control System (ICS) security
  •including minimizing exposure of ICS networks to
  •cyberthreats.



U.S. Cyberspace Solarium Commission

Robert Morgus

Privacy+ Security Forum

Federal Trade Commission

James Trilling

May 25, 2021

Developments in IoT Security

Katerina Megas
National Institute of Standards & Technology

Robert Morgus
U.S. Cyberspace Solarium Commission

James Trilling
Federal Trade Commission

Erik Jones
Venable LLP

Privacy+ Security Forum