Identifying Minimum Cybersecurity Features for IoT Devices used by the Federal Government

November 19, 2019

Michael Fagan, Senior Technical Lead to the Cybersecurity for IoT Program, NIST

The NIST Cybersecurity for IoT Program coordinates across NIST on IoT cybersecurity.

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

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
- Projects at National Cybersecurity Center of Excellence (NCCoE), some examples:
  - IoT-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, etc.
- Privacy Engineering Program

Cybersecurity for IoT Program Principles

Outcome-Based Approach

Embrace the Cybersecurity Framework's outcome-based approach. Specify desired cybersecurity outcomes, not necessarily how to achieve those outcomes, which allows organizations to choose the best solution for each IoT device and/or their enterprise environment.

Risk-Based Understanding

IoT capabilities, behaviors, deployment environments, and other characteristics can affect cybersecurity risk. Our approach to managing this risk is rooted in an understanding of how IoT can affect it.

No One Size Fits All

Each organization has its own risk tolerance and mission needs, and no one set of controls will address the wide range of cross-industry and cross-vertical needs and use cases. There is no one-size-fits-all approach to managing IoT cybersecurity risk.

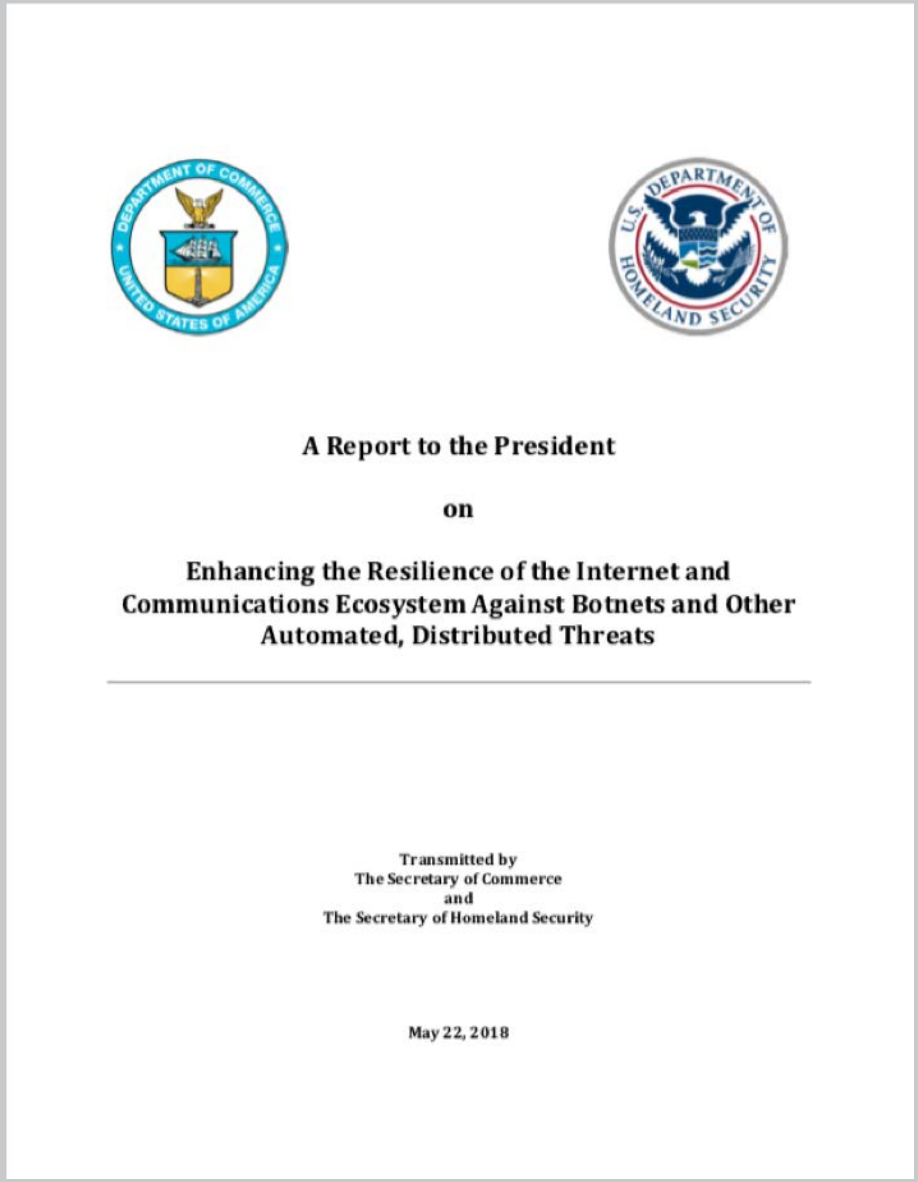
Ecosystem of Things

Recognizing that no device exists in a vacuum, NIST takes an ecosystem approach to IoT cybersecurity. For many devices, much of the functionality happens outside the device—not all the security is on the device itself. As such, we look at the entire ecosystem, not just endpoints.

Stakeholder Engagement

NIST works with diverse stakeholders to advance IoT cybersecurity. This includes collaborating with stakeholders to provide the necessary tools, guidance, standards, and resources.

Executive Order 13800: A Roadmap Toward IoT Security



A Report to the President

on

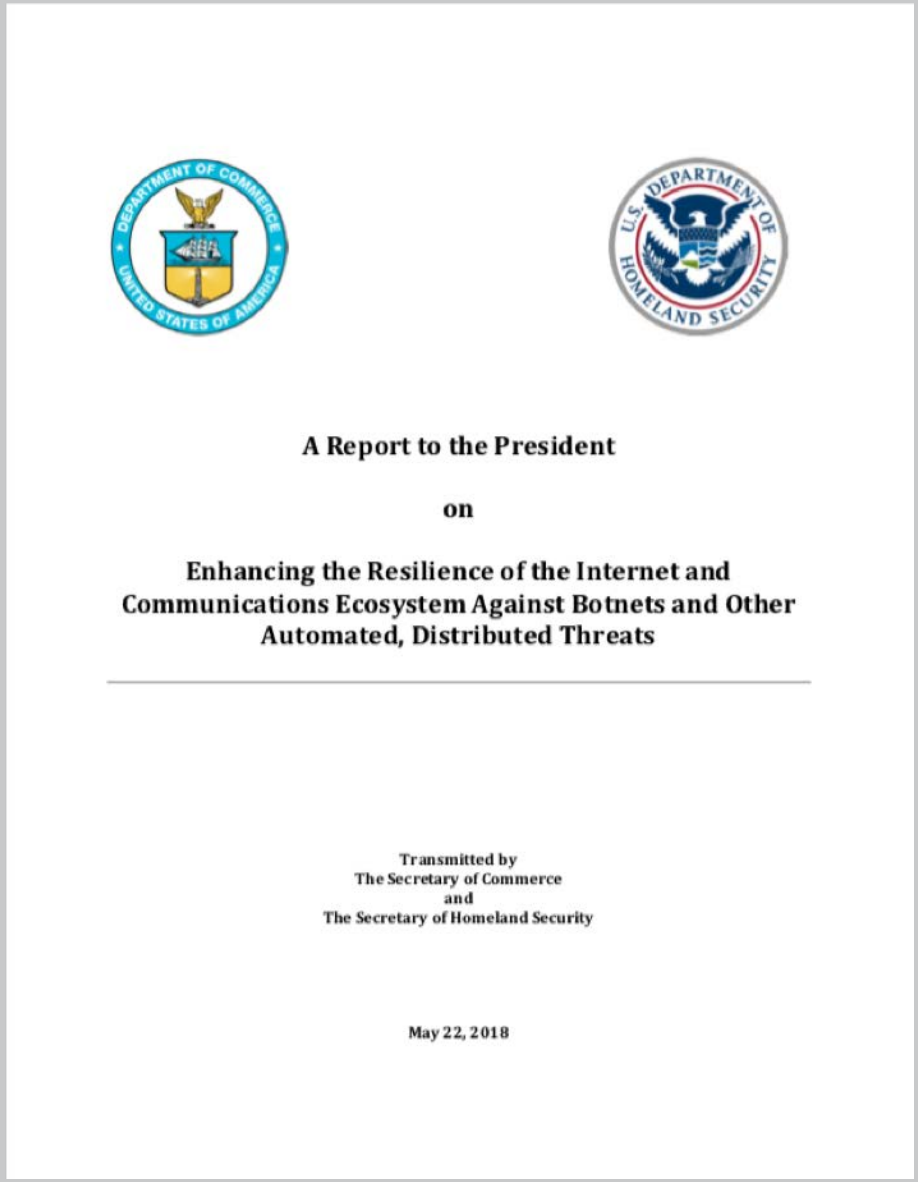
Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Transmitted by
The Secretary of Commerce
and
The Secretary of Homeland Security

May 22, 2018

- In response to Executive Order 13800 issued by the President on May 11, 2017, DoC and DHS delivered a report to the President in May, 2018 on the Resilience of the Internet against Botnet and other threats
- IoT security identified as a key unpinning component
- The Roadmap **charts a path** forward and **sets out a series of tasks** and deadlines laid out in the Report to the President
- The roadmap is a **plan for coordinating efforts among government, civil society, technologists, academics, and industry** sectors to develop a comprehensive strategy for fighting these threats
- One key objective of the roadmap is to establish a widely adopted security capability baseline for federal IoT products with high product availability and strong customer recognition.

Executive Order 13800: A Roadmap Toward IoT Security



A Report to the President

on

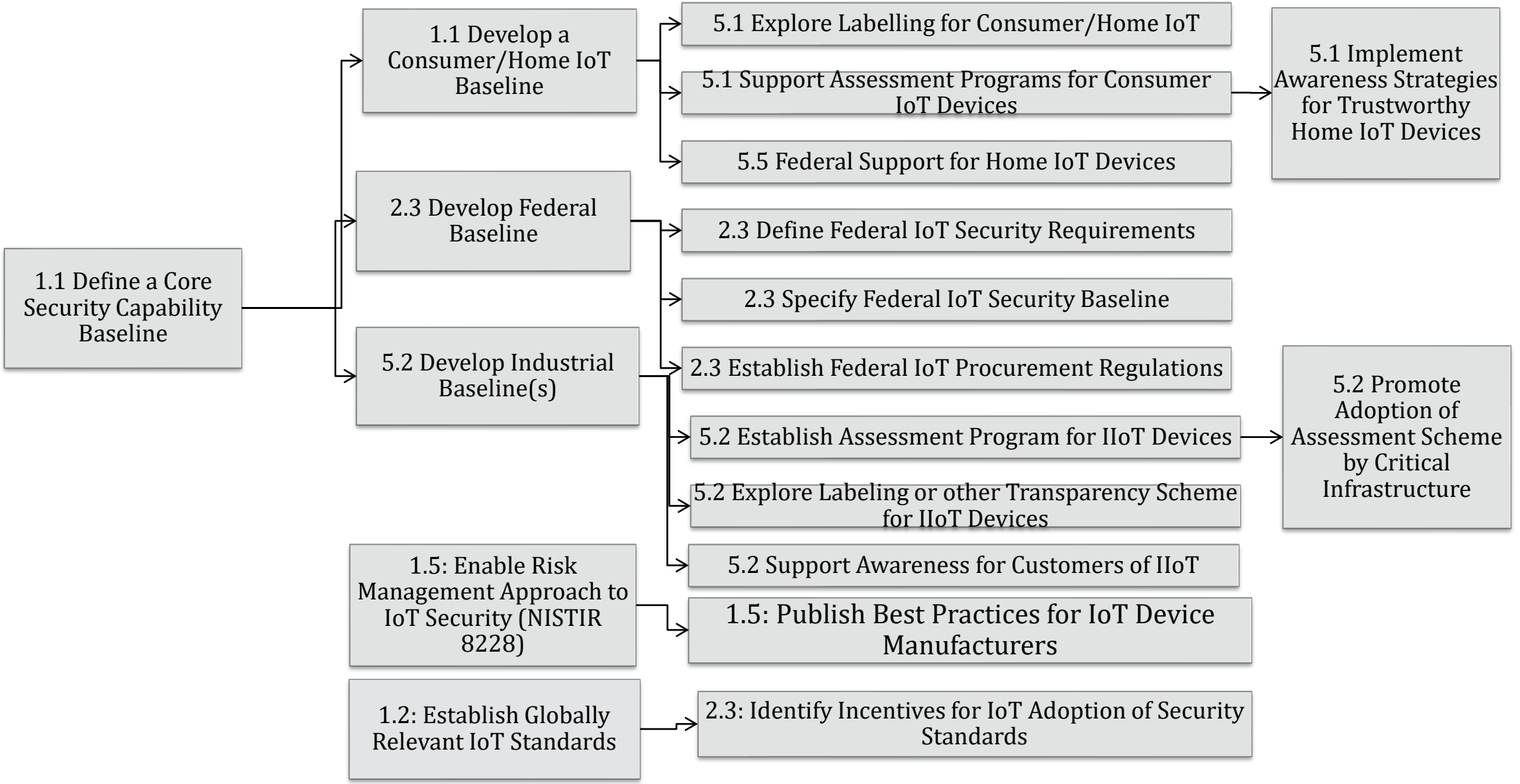
Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Transmitted by
The Secretary of Commerce
and
The Secretary of Homeland Security

May 22, 2018

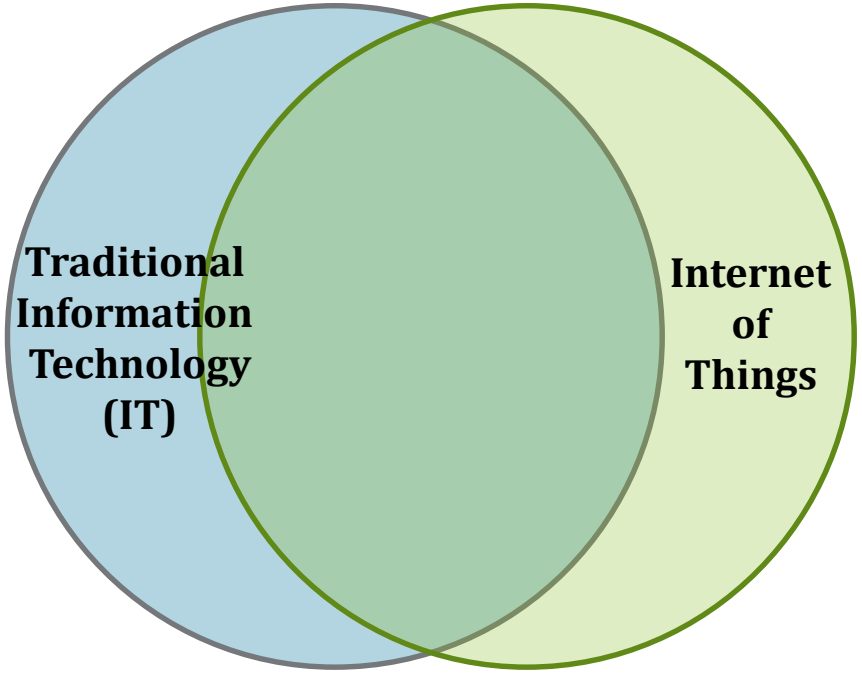
- Our national strategy for securing IoT comes from President Trump's 2017 EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.
- EO tasked DoC & DHS to "identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks."
- In May 2018, DoC and DHS delivered a report to the President, calling for the federal government to clearly delineate priorities for action. This initial roadmap lays out actions that could dramatically reduce the threat of botnets and similar attacks consistent with Administration priorities as set forth in the National Cyber Strategy.

The Roadmap's IoT Line of Effort lays out an action plan to establish a robust market for trustworthy IoT devices



NISTIR 8228: Considerations for Managing IoT Cybersecurity and Privacy Risks

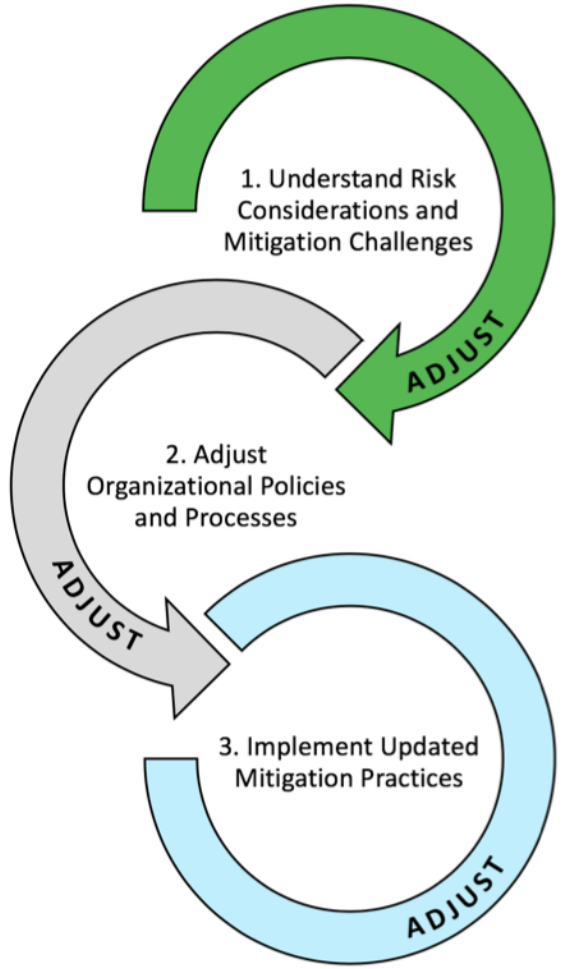
- Addresses the realm of IoT cybersecurity and privacy risk not addressed in existing IT guidance and **provides considerations for applying existing guidance.**
- The primary audience is federal agencies, but the publication is intended to be **useful to any organization interested in managing their security and privacy risks associated with using IoT.** Stakeholders from federal agencies, industry, and academia provided input throughout the process.
- It includes **possible solutions for addressing cybersecurity and privacy risks.** These are not requirements: IoT devices and their uses are so varied that we wanted to allow for flexibility so the guidance can be applicable across various use cases, levels of risk, and device types.



NISTIR 8228: Navigating the Process of Identifying and Addressing IoT Cybersecurity and Privacy Risks

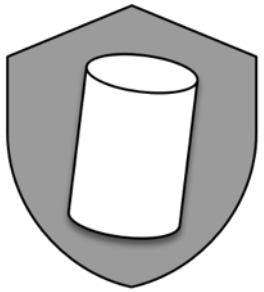
Walks readers through the process of considering IoT cybersecurity and privacy risks, by:

1. Defining capabilities IoT devices can provide, particularly those with most potential to affect cybersecurity and privacy risk.
2. Describing considerations that may affect the management of cybersecurity and privacy risks for IoT devices.
3. Exploring how the risk considerations may affect mitigating cybersecurity and privacy risk for an organization's IoT devices.
4. Providing organizations recommendations on how to address the risk considerations for their IoT devices.



Three goals discussed for IoT risk mitigation

Protect Device Security
Prevent a device from being used to conduct attacks, including participating in distributed denial of service (DDoS) attacks against other organizations, and eavesdropping on network traffic or compromising other devices on the same network segment. This goal applies to all IoT devices.



Protect Data Security
Protect the confidentiality, integrity, and/or availability of data (including PII) collected by, stored on, processed by, or transmitted to or from the IoT device. This goal applies to each IoT device with one or more data capabilities unless it is determined that none of the device's data needs its security protected.

Protect Individuals' Privacy
Protect individuals' privacy impacted by PII processing beyond risks managed through device and data security protection. This goal applies to all IoT devices that process PII or directly impact individuals.

8228 identifies potential implications for the organization and affected controls and framework subcategories

Protect Device Security

- Asset Management
- Vulnerability Management
- Access Management
- Device Security Incident Detection:

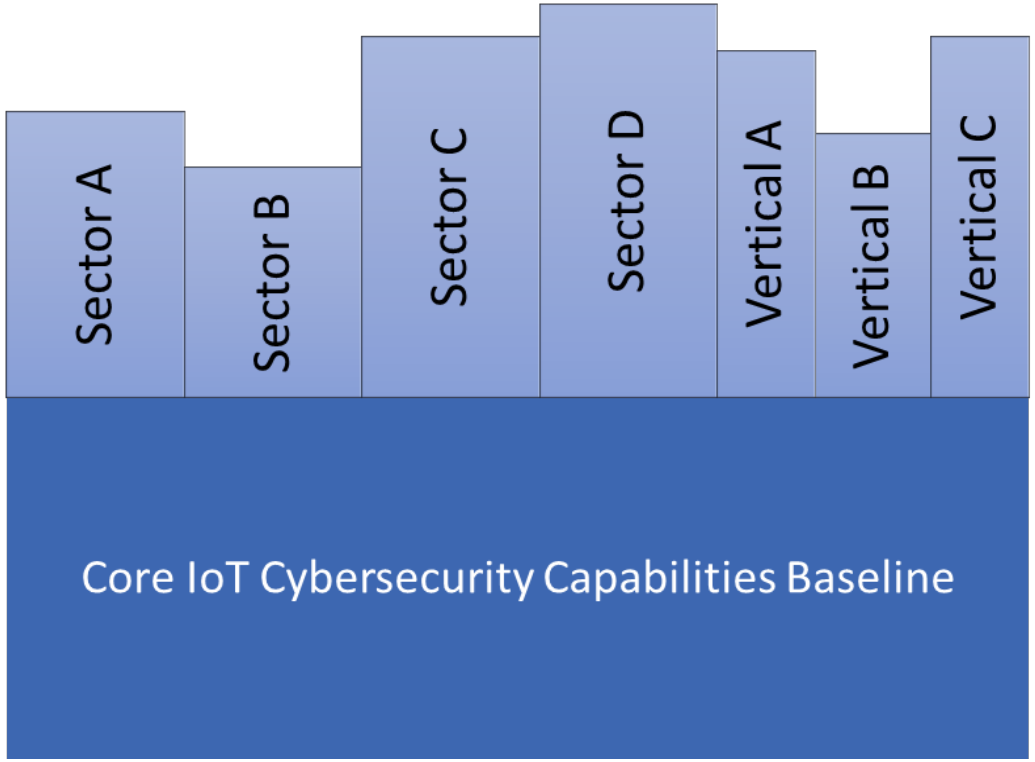
Protect Data Security

- Data Protection
- Data Security Incident Detection

Protect Individuals' Privacy

- Information Flow Management
- PII Processing Permissions Management
- Informed Decision Making
- Disassociated Data Management
- Privacy Breach Detection

Identifying a core baseline of security capabilities for devices



Draft NISTIR 8259, Core Cybersecurity Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers

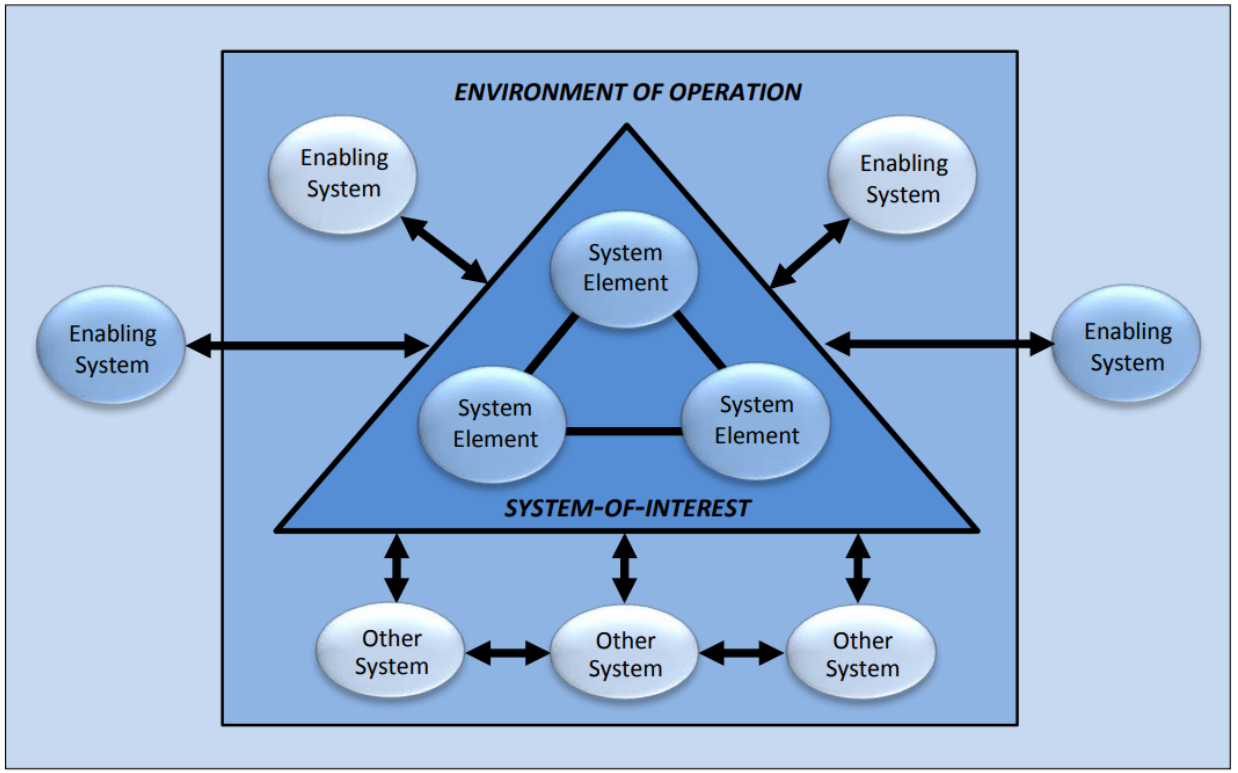
- Intended to help IoT device manufacturers understand how to identify the cybersecurity risks their customers face so **IoT devices can provide cybersecurity features that make them at least minimally securable.**
- Defines a **core baseline of cybersecurity features that manufacturers may voluntarily adopt for IoT devices they produce**.
- Provides information to help manufacturers **review their device's function and identify and implement capabilities beyond the core baseline most appropriate for their customers.**
- Because many customers will benefit from manufacturers communicating more clearly about cybersecurity risks involving their IoT devices, Draft NISTIR 8259 **includes examples of the types of information that may be beneficial to communicate to customers.**
- Comments received in last comment period are being processed and **a new draft is forthcoming**.

Next Initiative: Develop Federal Baseline

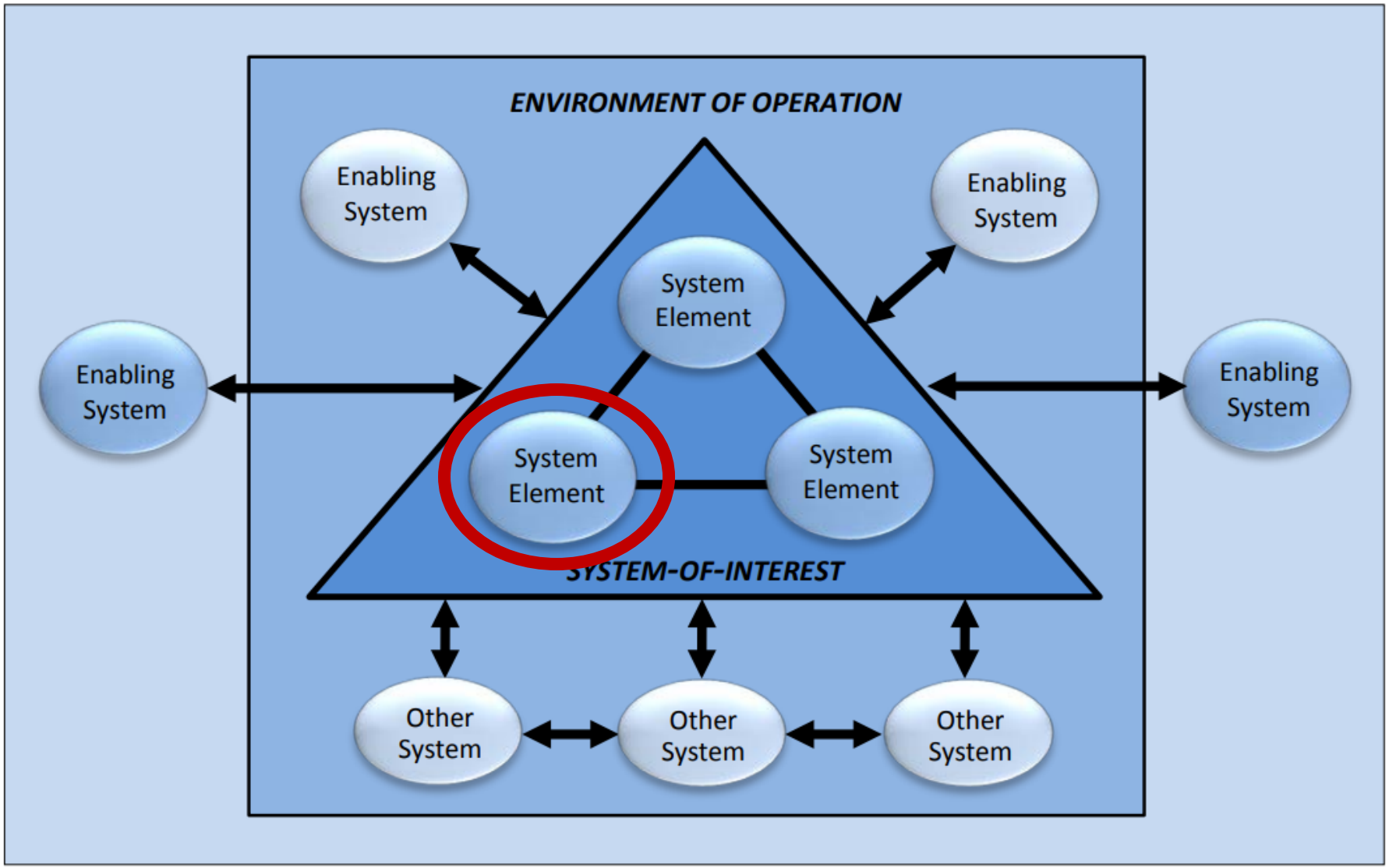
- Focus turns to the needs of Federal Agencies to augment the core security capability baseline with requirements specific to the federal IoT market
- Federal baseline will support downstream activities to encourage acquisition and deployment of conforming devices by established federal procurement regulations that reference a federal baseline.

There exists extensive guidance for Federal IT systems

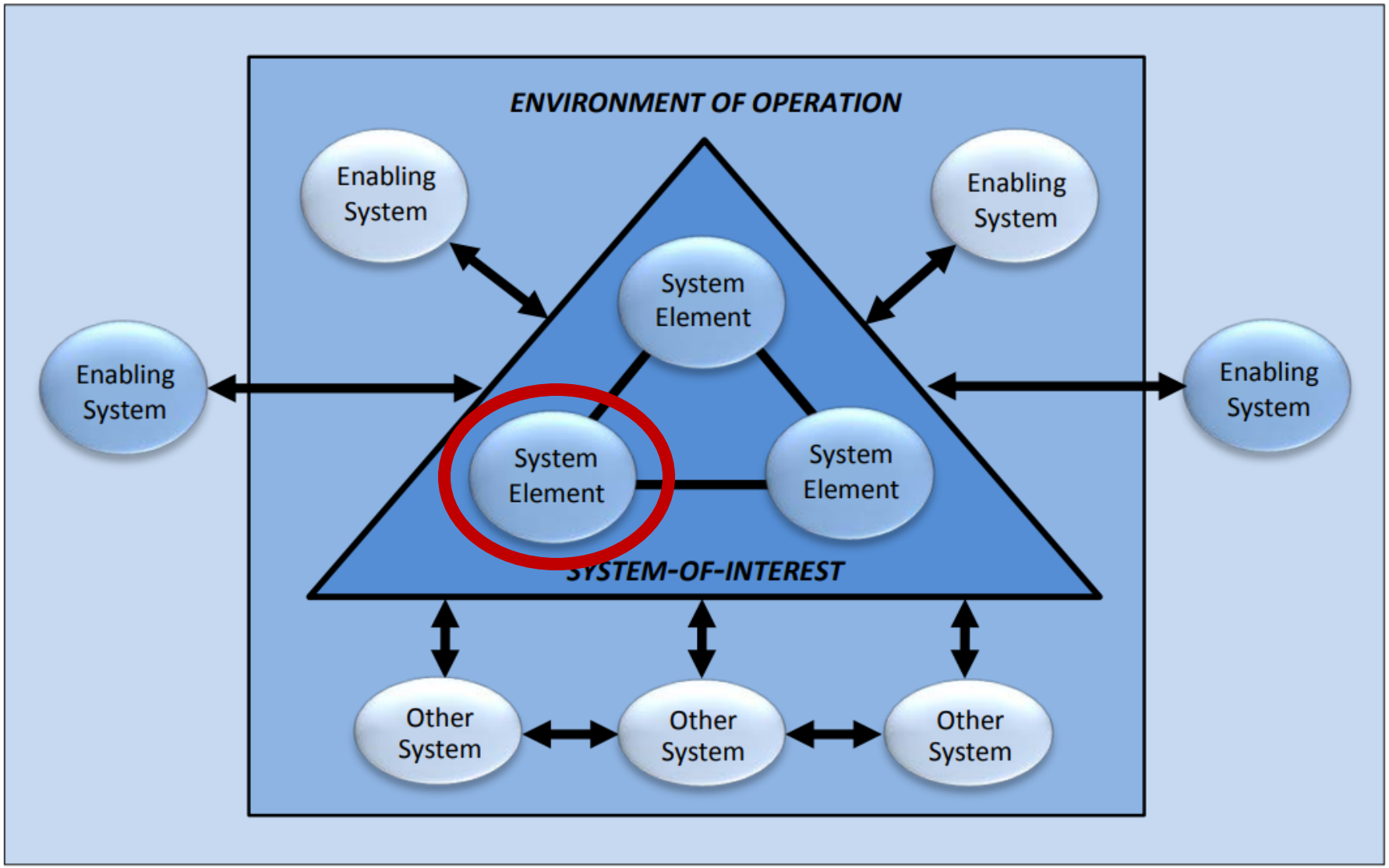
- Risk Management Framework
- Cybersecurity Framework
- FIPS Standards for Security Categorization of Federal Information and Information Systems
- Cybersecurity Framework
- NIST SP 800-53 Security and Privacy Controls
- Guidance needed on applying existing body of knowledge to IoT and IoT devices
  - Surfacing cybersecurity assumptions of IT (NISTIR 8228)
  - Special considerations for different risk levels of Federal systems
  - Special tailoring of implementing controls may be needed



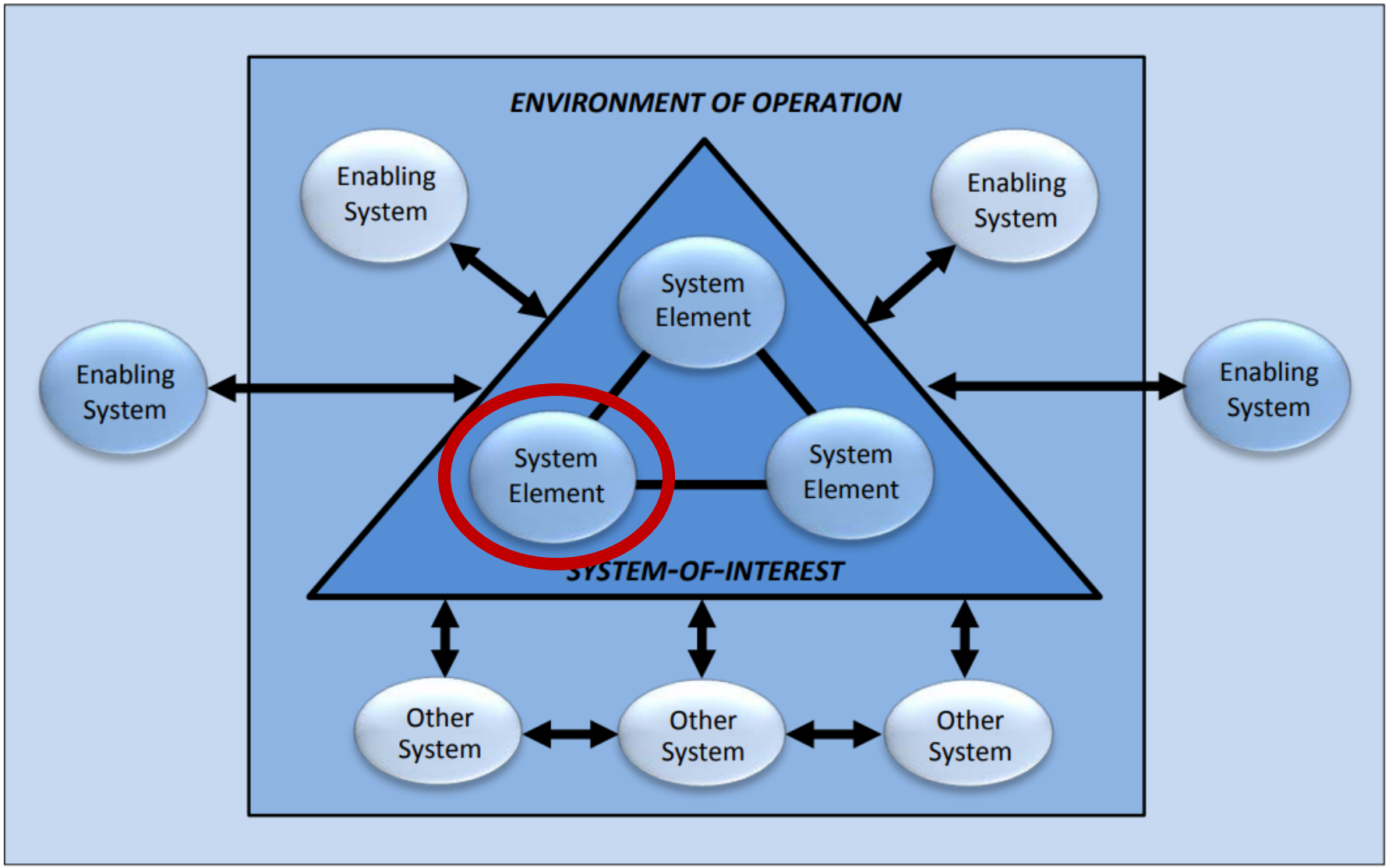
Manufacturers create IoT devices that may become system elements.



These IoT devices then may have to support security controls “out-of-the-box”



Management of risk may depend upon that "out-of-box" support, or require new tailoring of controls/acceptance of risks



Q & A

Have a question or an idea? We want to hear from you!
We're always accepting thoughtful feedback at
iotsecurity@nist.gov

@NISTcyber
#IoTSecurityNIST

We welcome **your** written feedback at:
iotsecurity@nist.gov

iotsecurity@nist.gov

https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this document in order to describe a procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.