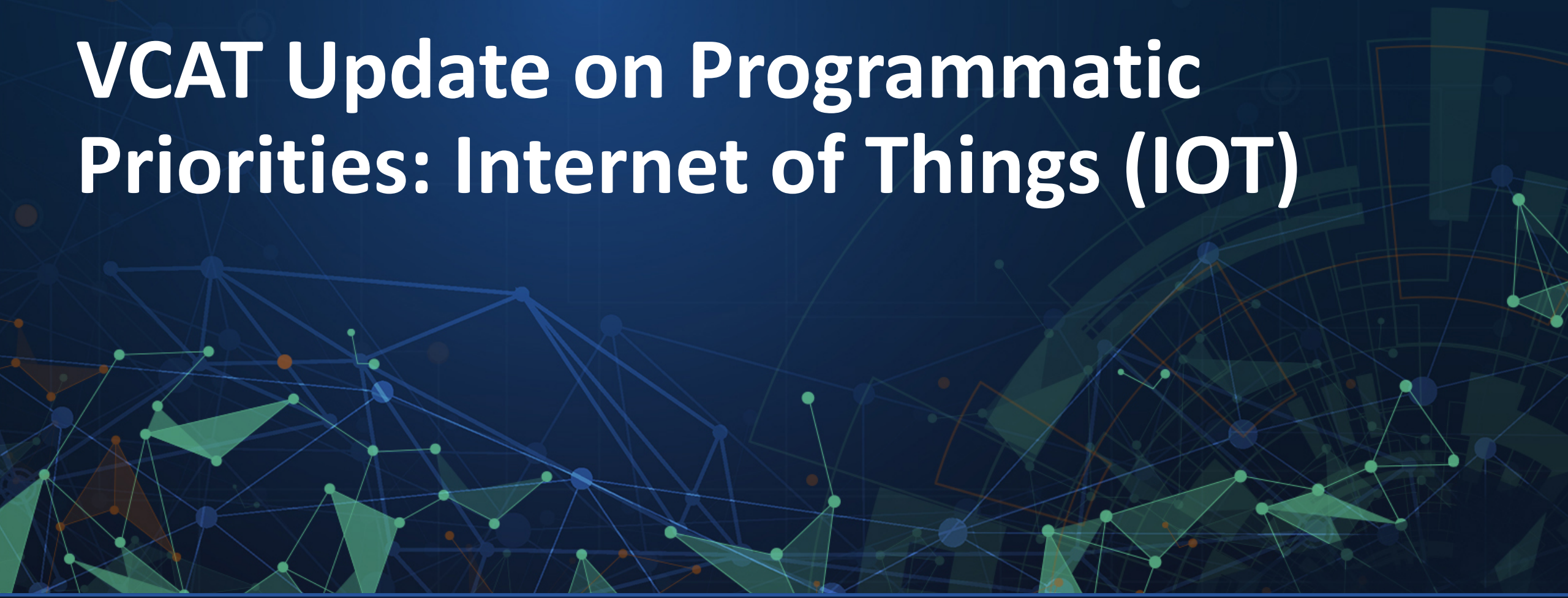
VCAT Update on Programmatic Priorities: Internet of Things (IOT)



National Institute of Standards and Technology
U.S. Department of Commerce

NIST Gaithersburg

February 12, 2020

IOT: NIST Role

*Assuring the **trustworthiness** of IoT systems by developing quantitative metrics, standards, and guidelines.*

Figures of merit for trustworthy IoT systems include: *reliability, resilience, security, privacy, and safety.*

NIST will initially focus on Industrial IoT (IIoT) applications where confidence in trustworthy IoT solutions would prove most beneficial.

Measurements, research, and standards to support reliability, resilience, and safety

Research, standards and guidelines for improving security, privacy

Strategic partnerships to realize the full potential of IIOT and prioritize areas of greatest need.

IOT at NIST

ENGINEERING LABORATORY

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ITL

CTL Communications Technology Laboratory

What is IOT?

Engineered, physical systems integrated with networking, data, and computational systems linked via transducers

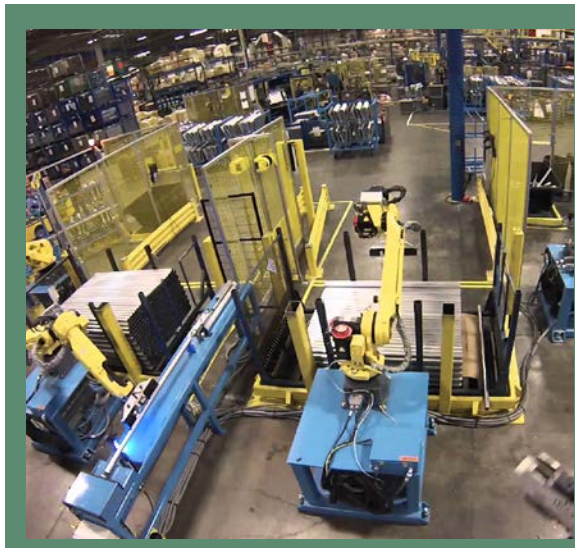
IOT Quick Facts

- By 2015 there were about 15.4B connected IoT devices
- By 2020 the number is expected to grow to 20.4B [1]
- By 2025, 75.4 billion.
- The global IoT market was worth over $150 billion in 2018.
- By 2025 it is expected to exceed $1.5 trillion.
- IoT saves money too. The city of Barcelona saves $37 million a year due to smart lighting.

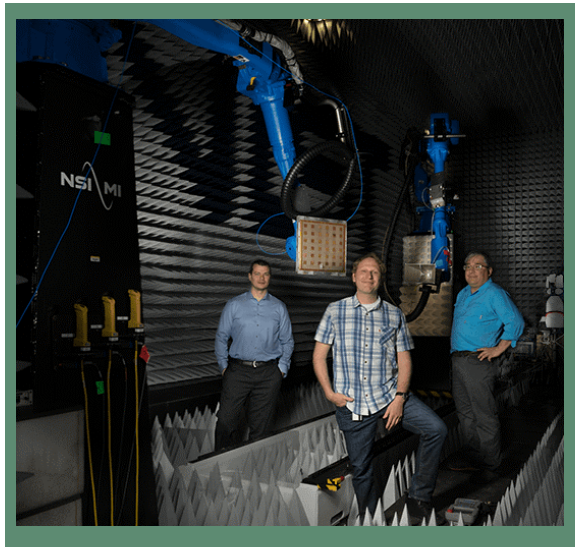
NIST has many programs that can support IOT. Most of these programs reside in ***Communications Technology Laboratory, Engineering Laboratory,*** and ***Information Technology Laboratory.***

[1] Gartner (January 2017).

IOT: Charting a Cohesive Program



NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

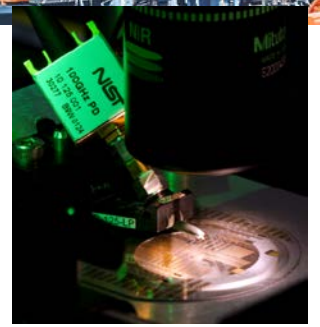


NIST's IoT portfolio includes projects addressing:

- **Measurement capabilities**, including sensor technologies, uncertainty methods, formal methods for assurance, interoperability, virtual and composite methods and more
- **Standards,** including connectivity, data, interoperability, composability, performance measurement guidelines, architectures, etc.
- **Applications,** including advanced manufacturing, automated vehicles, intelligent buildings, smart grid, and smart cities.

IOT: Communications Technology Laboratory

- **SI traceability for communications**
  - Scattering parameters
  - RF power & noise
  - Antenna parameters
  - Dielectric constant
  - Cross-frequency phase
- **New challenges:**
  - Over-the-Air testing
  - Dynamic measurements
  - System-level metrology
  - Component-level testing
  - Traceable standards for 5G and beyond



5G Millimeter-Wave Channel Model Alliance

IOT Highlight: Over-the-Air (OTA) Testing

Defining new certifications for connector-less devices with OTA

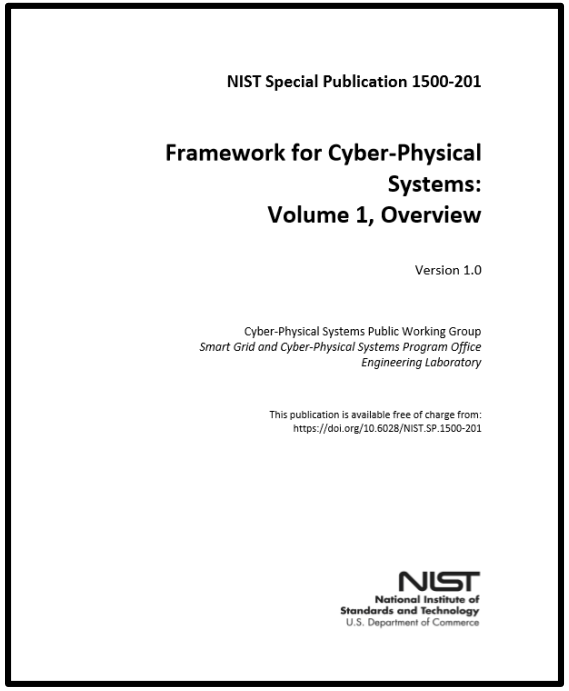
- Handset and base-station performance verified under radiated conditions
  - Total Radiated Power, Receiver Sensitivity
  - Isotropic quantities
- NIST has led development of efficient, rigorous OTA tests for large-form-factor IoT devices
  - CTIA Certification Test Plan released June 2019
  - *Every new IOT device is tested OTA!*

IOT: Engineering Laboratory

Trustworthy Systems, Components, and Data for Smart Manufacturing Program

Cyber Physical Systems Framework and Testbed

Industrial Wireless Testbed



NIST Special Publication 1500-201

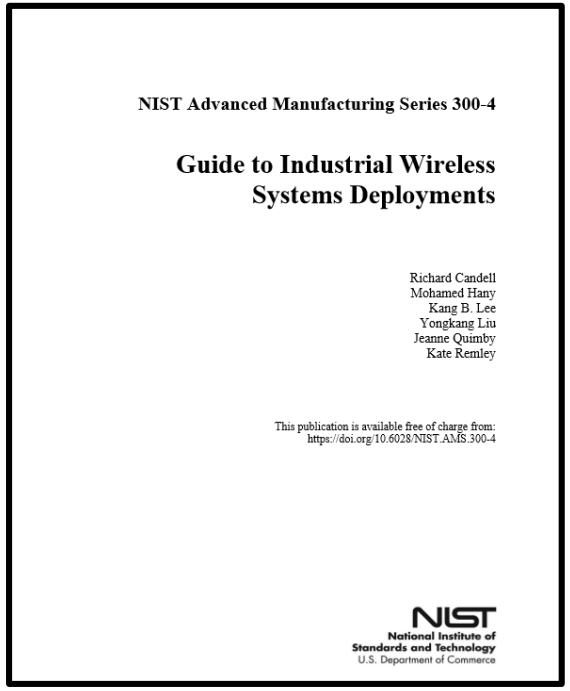
Framework for Cyber-Physical Systems:
Volume 1, Overview

Version 1.0

Cyber-Physical Systems Public Working Group
Smart Grid and Cyber-Physical Systems Program Office
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-201

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



NIST Advanced Manufacturing Series 300-4

Guide to Industrial Wireless Systems Deployments

Richard Candell
Mohamed Hany
Kang B. Lee
Yongkang Liu
Jeanne Quimby
Kate Remley

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AMS.300-4

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Industrial Wireless Technical Working Group

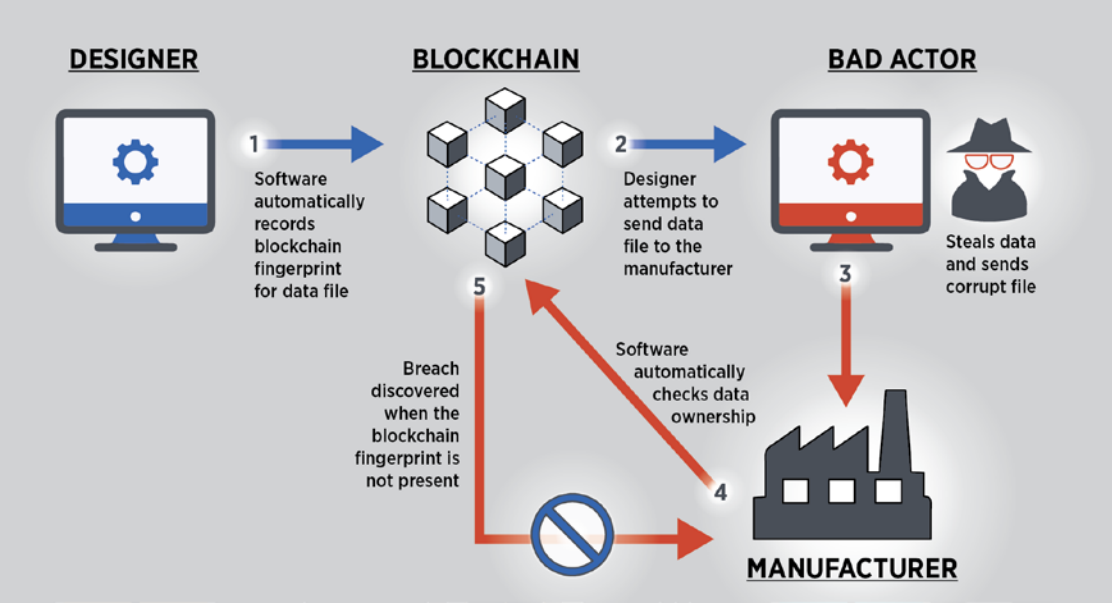
IEEE
Advancing Technology for Humanity

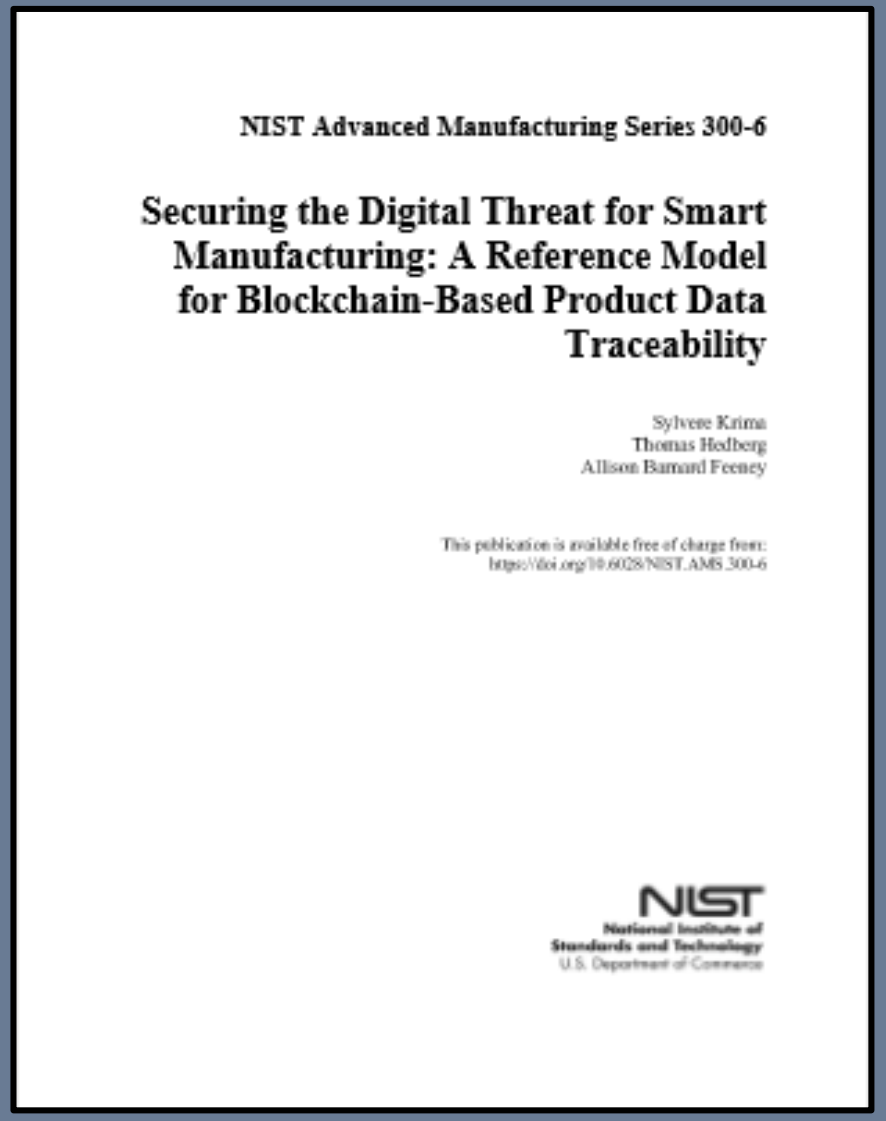
IOT Highlight: Blockchain for Smart Manufacturing

Building trustworthiness into digital manufacturing networks

Tamper-proof transmission of manufacturing data

➔ *Data traceability for all participants in production process*





NIST Advanced Manufacturing Series 300-6

Securing the Digital Threat for Smart Manufacturing: A Reference Model for Blockchain-Based Product Data Traceability

Sylvere Krima
Thomas Hedberg
Allison Barnard Feeney

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AMS.300-6

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

IOT: Information Technology Laboratory

Wide range of ITL IOT research - eg:

- **Cybersecurity for IoT**
  - Standards, guidelines, and related tools
- **Networking Protocols**
  - E.g., Intra-vehicle networking protocols
- **Usability**
  - Research to improve human IoT interactions
- **Cloud for IoT**
  - Edge computing (e.g., fog computing)
- **Architecture for IoT**
  - Standards (ISO/IEC, IEEE, IIC)
- **Information modeling**
  - Category theory for IoT

The NCCoE has developed cybersecurity guidance to help healthcare delivery organizations protect their networks and data.

IOT Highlight: Baseline for Securable IOT Devices

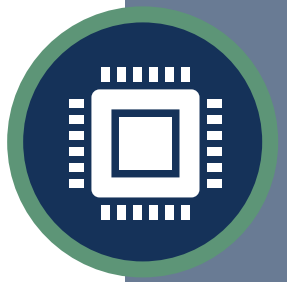
NIST 8228: Considerations for Managing IOT Cybersecurity and Privacy Risk (July 2019)

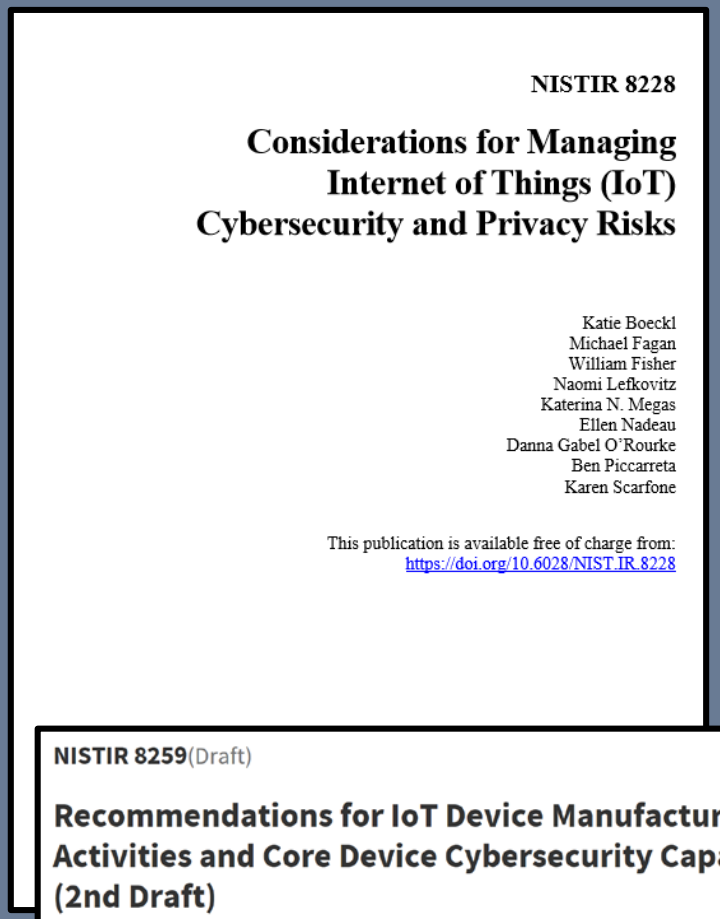
Approaches risk management from organization use of IOT

NIST 8259: Recommendations for IOT Device Manufacturers (2nd draft)

Guidance for manufacturers to address cybersecurity features that make IOT devices at least minimally securable by end users.

Public comments closed Feb. 7, 2020.





NISTIR 8228

Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

Katie Boeckl
Michael Fagan
William Fisher
Naomi Lefkovitz
Katerina N. Megas
Ellen Nadeau
Danna Gabel O'Rourke
Ben Piccarreta
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8228

NISTIR 8259(Draft)

Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft)

Date Published: January 2020
Comments Due: February 7, 2020
Email Comments to: iotsecurity@nist.gov

Author(s)
Michael Fagan (NIST), Katerina Megas (NIST), Karen Scarfone (Scarfone Cybersecurity), Matthew Smith (G2)

DOCUMENTATION

Publication:
NISTIR 8259 (Draft) (DOI)
Local Download

Supplemental Material:
None available

Coordinates activities across NIST related to cybersecurity and privacy concerns for IOT

IOT: Supporting Industries of the Future

ENGINEERING LABORATORY

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ITL

CTL Communications Technology Laboratory

NIST will undertake multifaceted approach to addressing critical factors comprising *trustworthiness*

1. Measurements, research, and standards to support reliability, resilience, and safety
2. Research, standards and guidelines for improving security, privacy
3. Strategic partnerships to realize the full potential of IIOT and prioritize areas of greatest need.

[1] Gartner (January 2017).

Strategic Leverage Through Partnerships

NARUC
National Association of Regulatory Utility Commissioners

5G Millimeter-Wave
Channel Model Alliance

A Sempra Energy utility

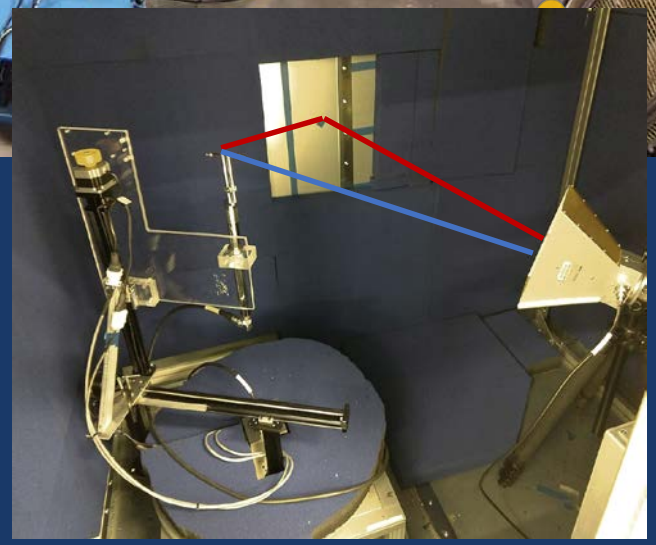
AT&T

IOT: Charting a Cohesive Program

Communications Technology Laboratory	Engineering Laboratory	Information Technology Laboratory
• NIST 5G mmWave Channel Model Alliance • Over-the-Air Testing • Component ➔ Systems Characterization • Chip-scale standards and probes for RF and mmWave measurements	• Cybersecurity for Smart Manufacturing • Smart Manufacturing Testbed • Wireless Systems for Factory Automation • Trustworthy Systems for Smart Manufacturing	• Cybersecurity Standards for IOT • National Cybersecurity Center of Excellence • Securing Industrial Control Systems • Healthcare IOT

Identifying synergistic opportunities across NIST to support Industries of the Future

IOT: NIST Grand Challenge



Industrial IOT Testbed

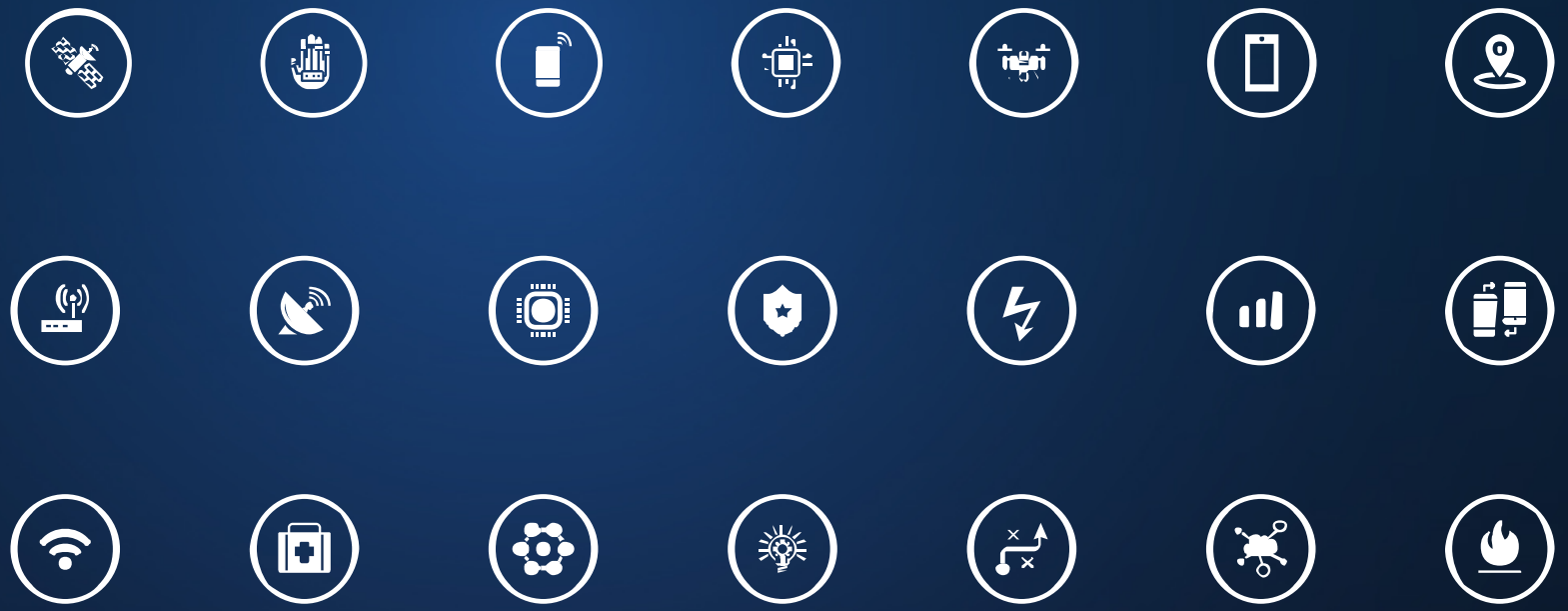
NIST will create a metric-based IIOT testbed uniting NIST expertise in wireless comms, manufacturing, and artificial intelligence.

Standards-based security controls for manufacturers in NIST Cybersecurity Practice Guide

National Cybersecurity Center of Excellence, NIST 5G Alliance, NIST Industrial Wireless Technical Working Group, NSF Platforms for Advanced Wireless Research, & Manufacturing USA Institutes .

DISCUSSION

Copy and paste icon to desired slide. To change color, double click on icon, select color from drop down. For consistency, please use colors in the template. *Due to licensing restrictions, you can only use these icons for NIST PowerPoints.*



IOT: Information Technology Laboratory

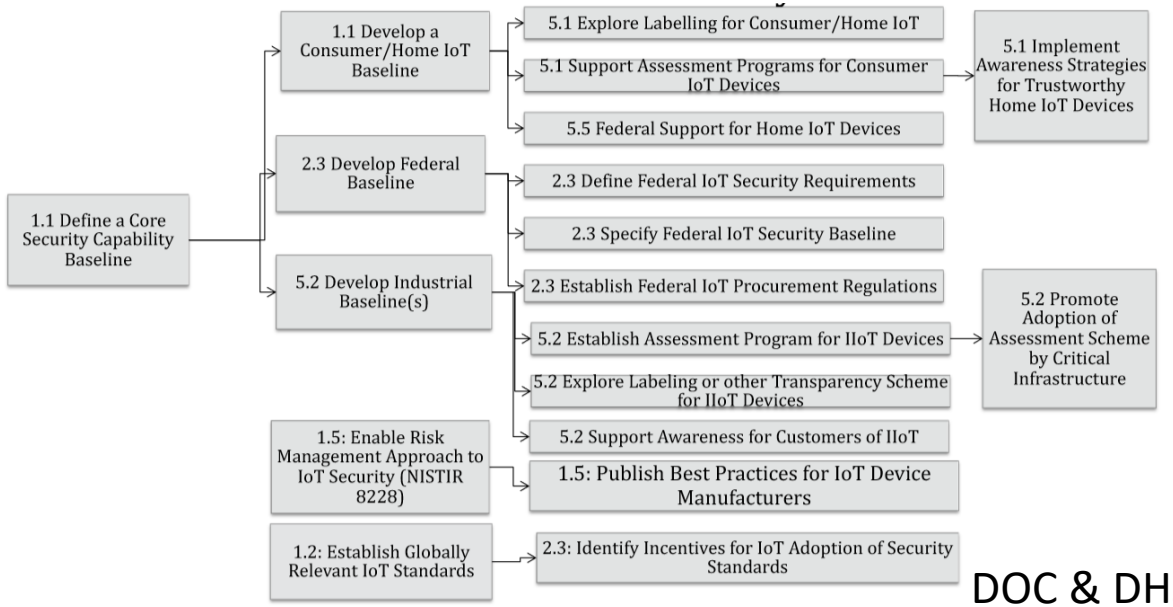
Cybersecurity for IOT Program

Fostering cybersecurity for devices and data in the IoT ecosystem, across industry sectors and at scale

Ecosystem approach to IOT cybersecurity to address functionality that happens outside of individual IOT device

- *No One Size Fits All*
- *Outcome-Based Approach*
- *Risk-Based Understanding*
- *Stakeholder Engagement*

Roadmap Toward IOT Security



DOC & DHS (2018)

Amazon, Boeing, Chamber of Commerce, CTA, CTIA, ITI, Microsoft, Raytheon, Symantec, and many more.