Welcome to NIST

Conference Housekeeping Slides

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Agenda

Day 1 | Tuesday, March 31, 2026

9:00am – 3:30pm ET

Day 2 | Wednesday, April 1, 2026

9:00am – 3:45pm ET

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Colloquium on Cybersecurity for IoT: Future Directions

Day 1

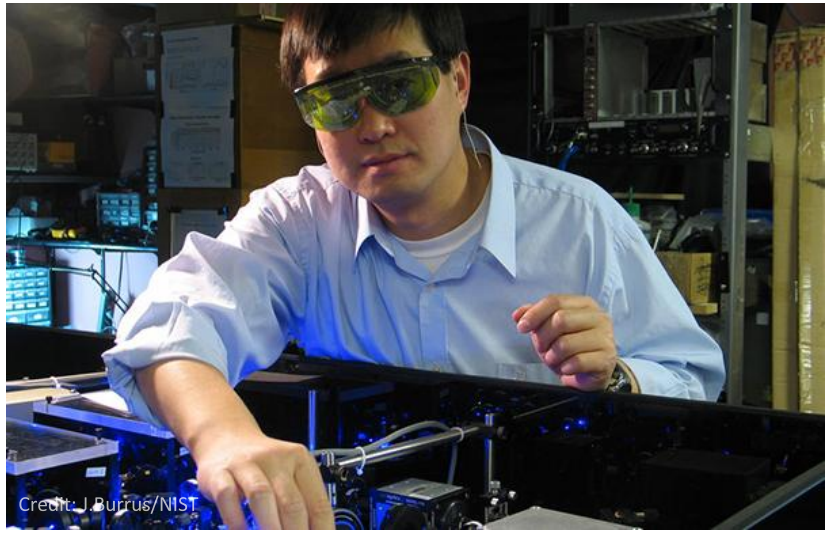
3/31/26

Welcome & Opening!

A bit about NIST…

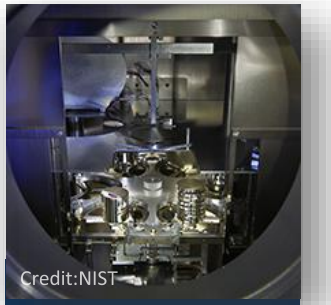
NIST Mission

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



NIST Laboratory Programs

Material Measurement Laboratory



Physical Measurement Laboratory

Engineering Laboratory

Information Technology Laboratory

Communication Technology Laboratory

NIST Center for Neutron Research

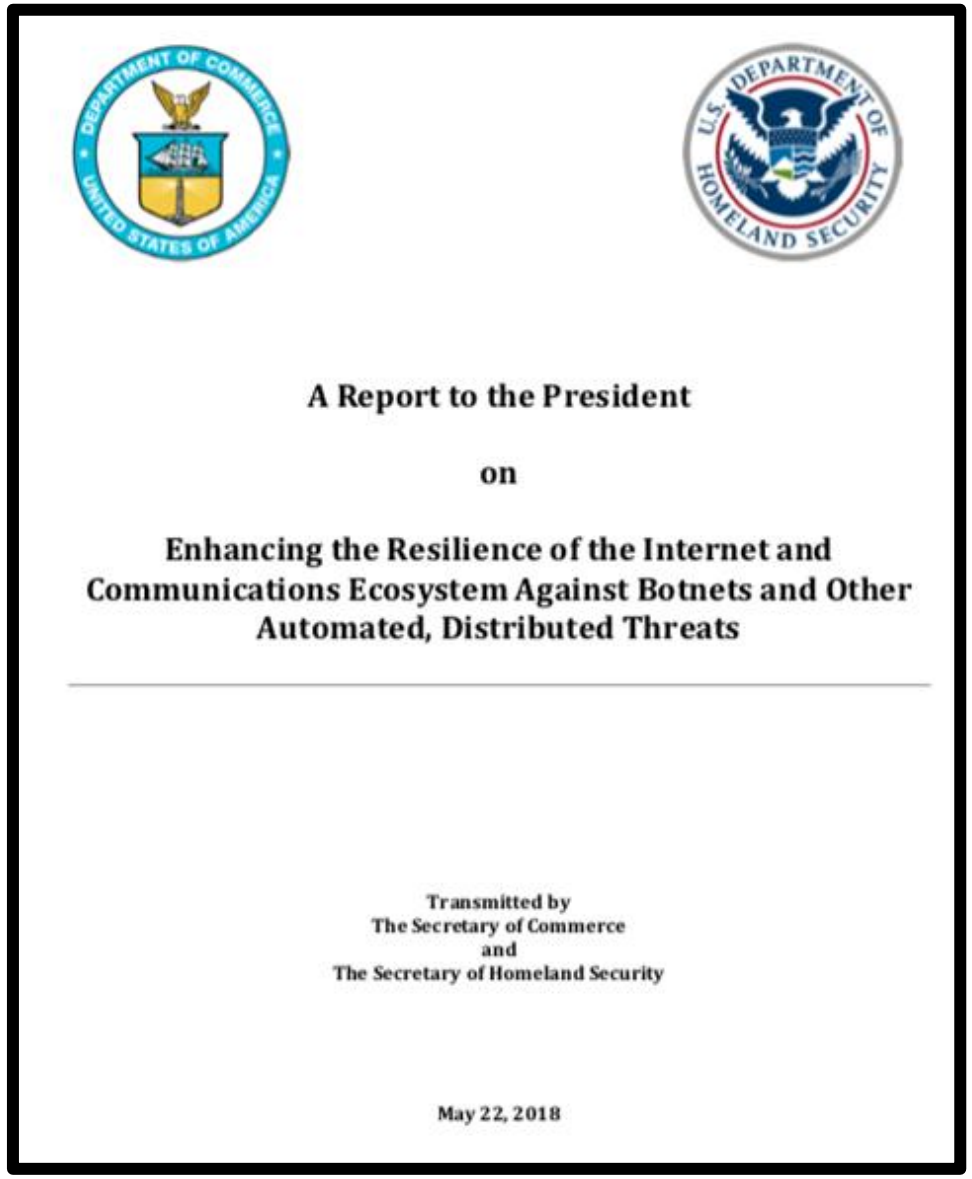
About the Information Technology Laboratory

- NIST Information Technology Lab (ITL) mission is to **cultivate trust in information technology**. ITL priority areas: **1) cybersecurity, 2) the Internet of Things**, 3) artificial intelligence, 4) reliable computing, and 5) future computing technologies.
- In accordance with the Federal Information Security Modernization Act (FISMA), NIST **develops information security standards and guidelines** for federal information systems.
- Agency within the U.S. Department of Commerce

NIST IoT Cybersecurity: Core Principles and Future Directions

Kat Megas, NIST

It started with Executive Order 13800



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

- A national strategy for securing IoT was taken from President Trump's 2017 EO 13800, ***Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.***
- The report and subsequent roadmap laid out a series of actions for both private sector and government for securing the IoT ecosystem.
- Since then NIST has:
  - published 20+ documents
    - With 500K+ downloads including all pubs
  - held 12+ public workshops
  - engaged with 3500+ stakeholders
  - processed 2200+ comments

Core Principles Guiding Our Efforts

Focus on how IoT characteristics affect system and organizational cybersecurity risk

Risk-Based Understanding

No One-Size-Fits-All

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

Ecosystem of Things

Cybersecurity for IoT Program Principles

Stakeholder Engagement

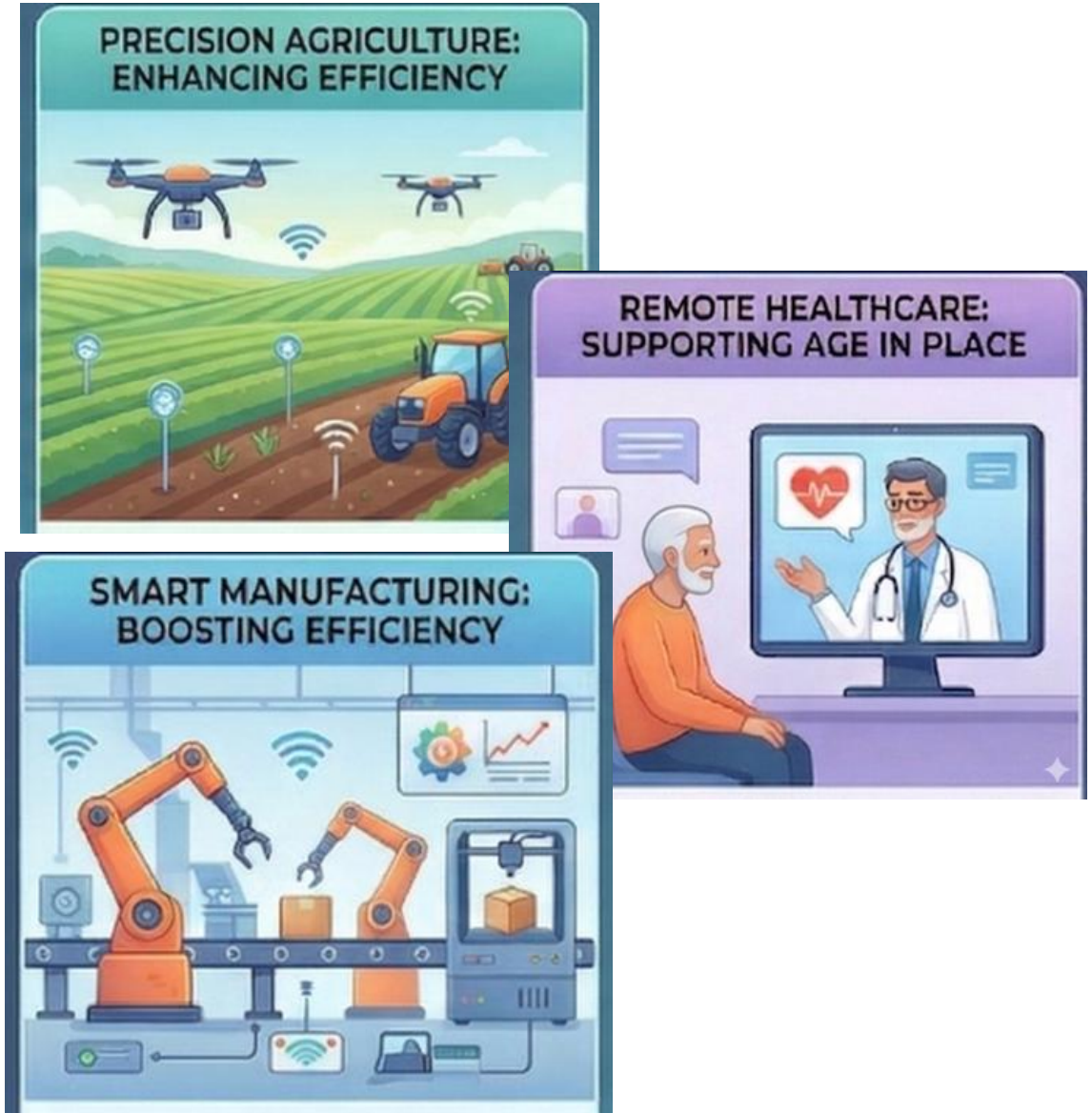
No device exists in a vacuum, so look at entire ecosystem not just IoT endpoints

Outcome-Based Approach

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

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

Looking ahead IoT will continue to play a critical role in the future in tandem with emerging technology



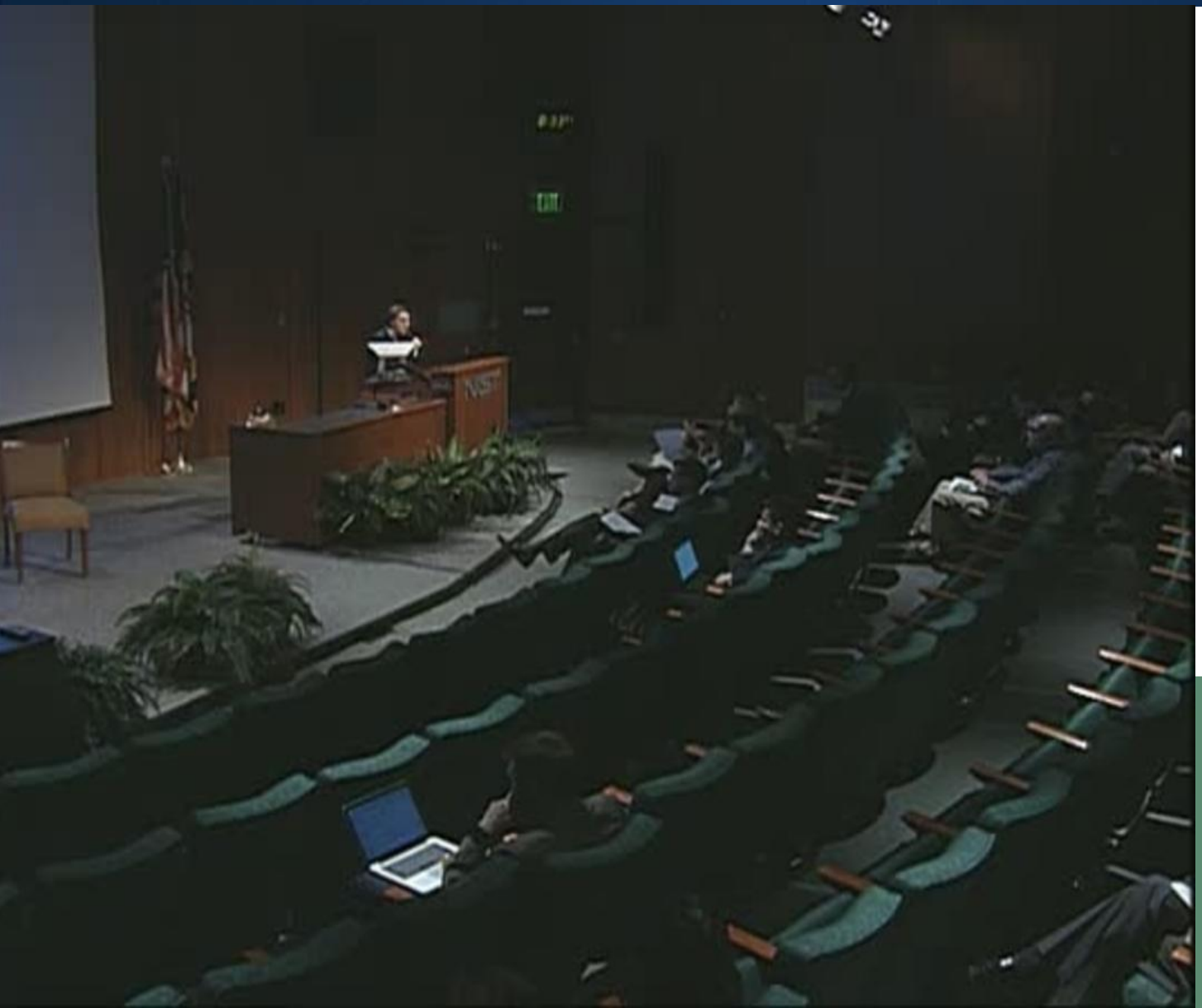
- IoT will continue to enhance productivity in manufacturing through data driven optimization such as: predictive maintenance reducing downtime; optimizing supply chains and improving quality control.
- In areas such as precision agriculture it has the ability to enhance efficiencies by enabling smart irrigation systems, soil health monitoring and nutrient sensors and crop disease prediction through early environmental change alerts
- IoT has the promise of improving our lives when at home whether it be through wearables that track vitals such as heart rate and blood pressure to safety alerts

But also new challenges from emerging tech

- AI enabled cyber attacks may require us to rethink defenses
- Deployment of AI in IoT may have implications for risk
- Quantum resistant cryptography and crypto agility may present unique challenges for IoT

Setting the Stage

Why are we here?



- As the Program has evolved, we've stayed active to keep our work responsive and up-to-date.
- In that mind, we are here today and tomorrow to:
  - Hear your thoughts and suggestions on what NIST should consider as we update SP 800-213.
  - Learn about the current state of IoT cybersecurity and emerging topics.
  - Understand future directions for our Program that will help us support innovation in the United States.

We have 2 days to dig into all these topics!

- Day 1 will focus on SP 800-213 and feedback from the community to support its update.
- Day 2 will widen the aperture to all IoT cybersecurity and future directions for the program

Today's Agenda (Day 1)

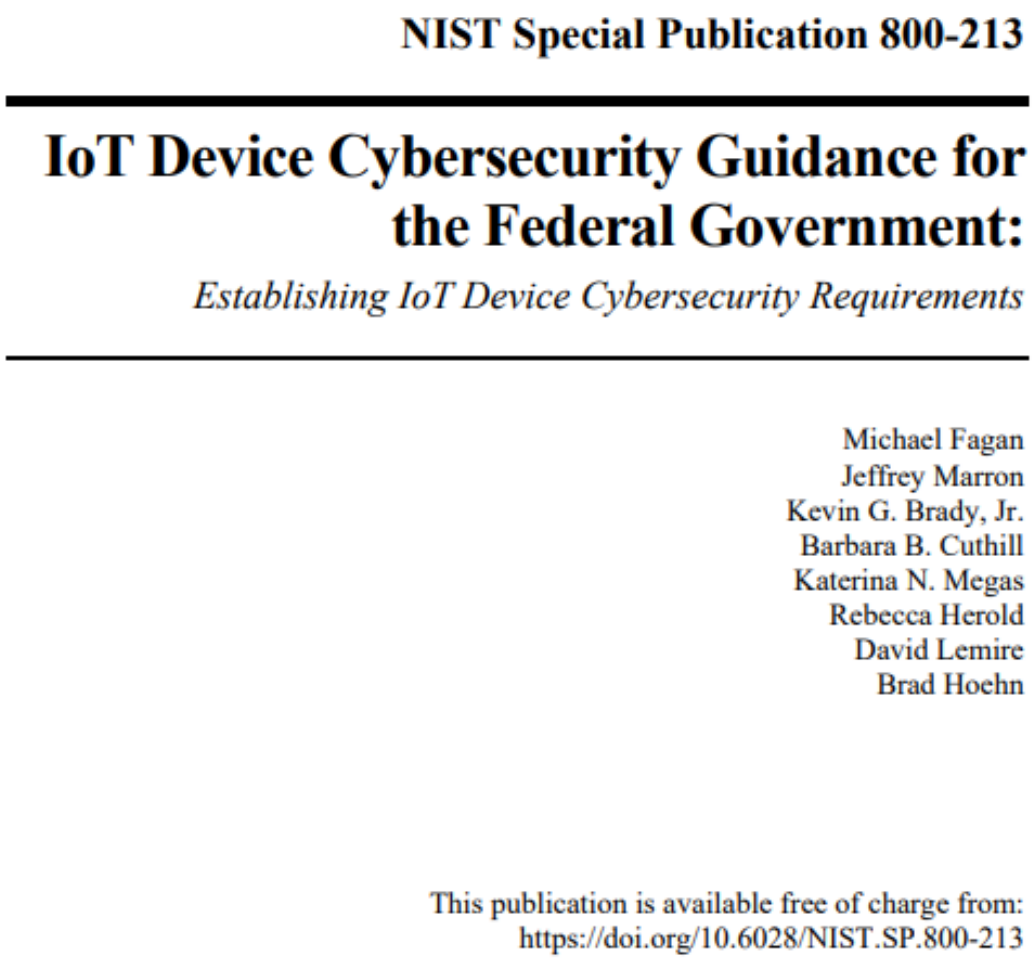
Time	Topic	Speaker(s)
9:00-9:30	Welcome & Opening [Green Auditorium]	Mike Fagan (NIST)
9:30-9:45	NIST IoT Cyber & DoC Priorities [Green Auditorium]	Kat Megas (NIST)
9:45-10:00	Setting the Stage [Green Auditorium]	Mike Fagan (NIST)
10:00-10:45	Identity of Things [Green Auditorium]	Nick Allott (NQuiring Minds)
10:45-11:00	*Break*	
11:00-12:00	Fireside Chat: Cryptography [Green Auditorium]	Mike Fagan (NIST), Moderator Kerry McKay (NIST) Colin Soutar (Deloitte Cyber)
12:00-1:30	*Lunch*	
1:30–3:30	Breakout Sessions: SP 800-213 Feedback [Portrait, Heritage, Lecture Room A]	

Tomorrow's Agenda (Day 2)

Time	Topic	Speaker(s)
9:00-9:30	Welcome & Focus on the Future [Green Auditorium]	Mike Fagan (NIST)
9:30-9:35	Introduction for Strategy of Things [Green Auditorium]	Kathleen McTigue (NIST)
9:30-10:30	Strategy of Things [Green Auditorium]	Benson Chan (Strategy of Things)
10:30-11:45	Healthcare Considerations Panel [Green Auditorium]	Jeff Marron (NIST), Moderator Nadia Elkaissi (Veteran's Hospitals) Nastassia Tamari (FDA) Connor Walsh (Siemens)
11:45-1:00	*Lunch*	
1:00-2:00	Fireside Chat: IoT Risk In Context [Green Auditorium]	Mike Fagan (NIST), Moderator Ian Fleming (Deloitte) Rishabh Das (Ohio University)
2:00-3:30	Breakout Session: IoT Risk Considerations [Portrait, Heritage, Lecture Room A]	
3:30-3:45	Wrap-up & Conclusion [Green Auditorium]	Mike Fagan (NIST)

Today's Focus:
All Things SP 800-213!

Guidelines for the Federal Government



NIST Special Publication 800-213

IoT Device Cybersecurity Guidance for the Federal Government:

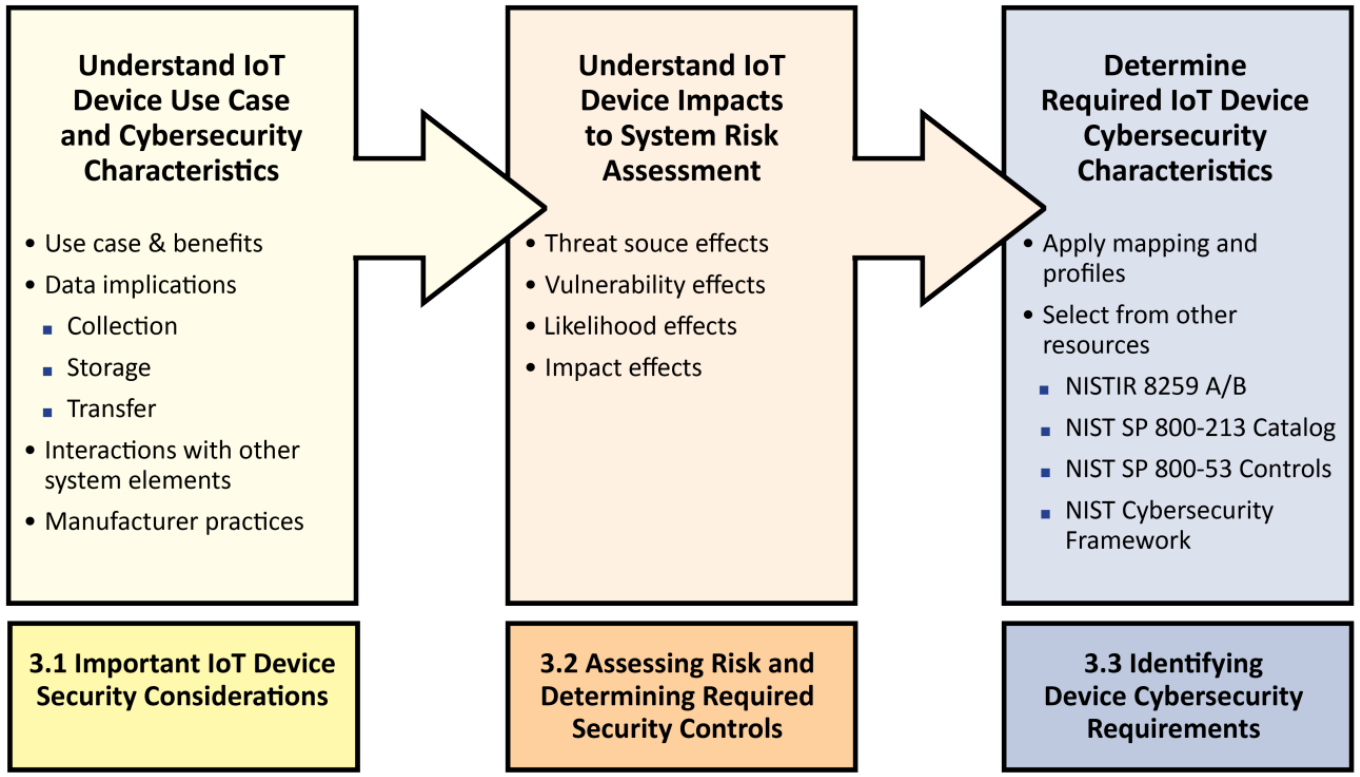
Establishing IoT Device Cybersecurity Requirements

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Rebecca Herold
David Lemire
Brad Hoehn

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-213

Today is focused on engaging in important IoT security topics, sharing our thoughts for the updated SP 800-213 document, and hearing from you on these developments.

A Solid Foundation for Revision



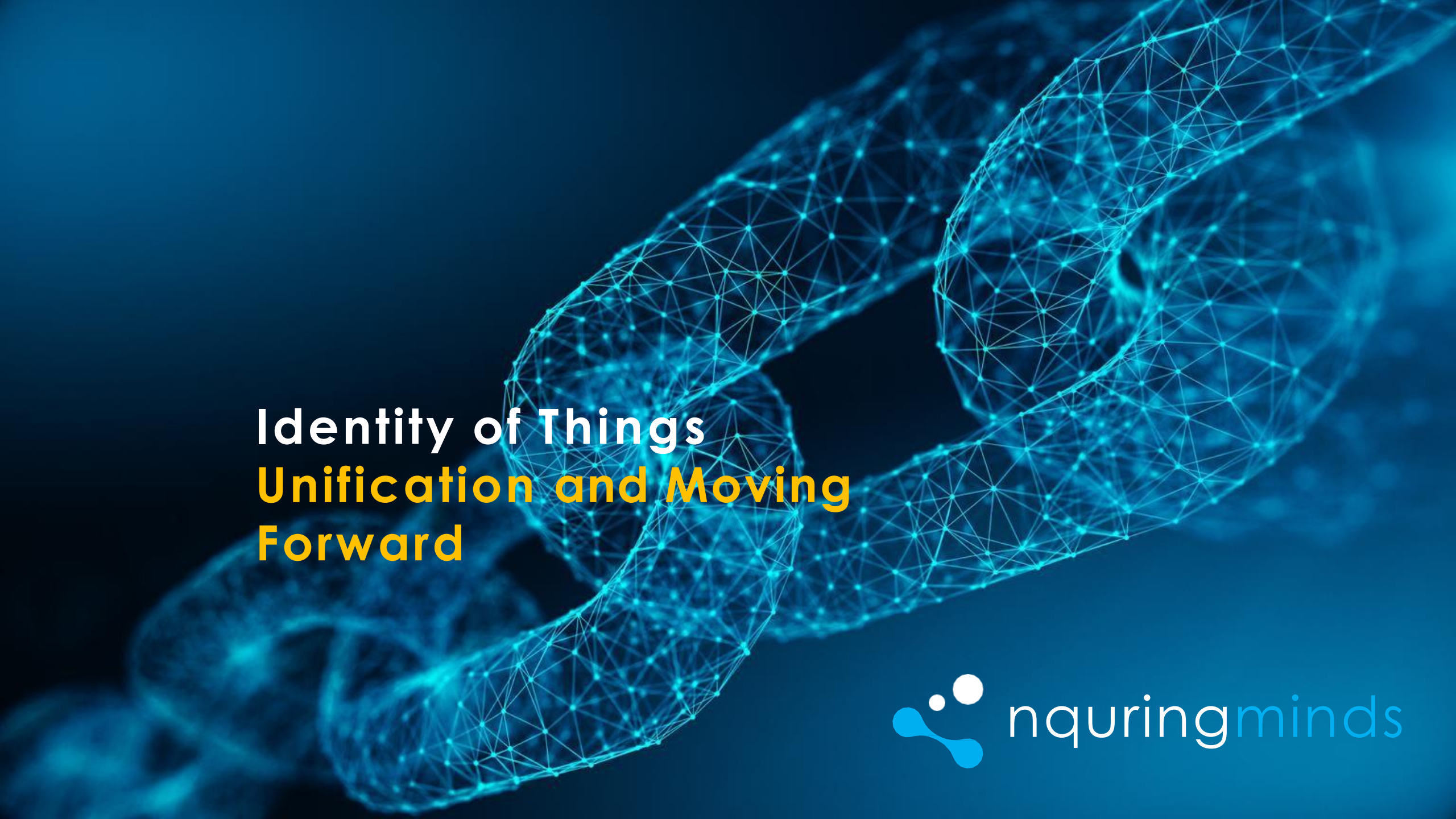
Looking at the last 5 years, we remain confident that the framework established in 2021's SP 800-213 and its basis in the RMF remain useful for approaching the topic by Federal agencies and beyond!

But updates are needed.

The Path Forward

- We're considering switching to product-based language, allowing us to better speak to components, and how they fit into the larger ecosystem.
- We are also thinking about technological changes and convergences and how SP 800-213 can best consider them.

- We need your insights and thoughts as well!
- This will be interactive: please challenge assumptions, share what you're seeing in practice, and help us identify what to keep, what to clarify, and what to change.


Identity of Things
Unification and Moving Forward
nquringminds

Topics to cover

nquiringminds

- Identity: some definitions
- IOT Identity and NIST Onboarding
- AI identity
- Pressures…
- What's next….

Identity Definitions

nquiringminds

Identity Definitions

- In security, identity is defined as the set of unique physical, behavioral, or digital attributes that distinguish an entity—person, machine, or application—within a system. It acts as a digital "key" allowing systems to verify users and authorize access to resources. Identity security protects these identities through authentication and lifecycle management

https://gemini.google.com/

- The set of physical and behavioral characteristics by which an individual is uniquely recognizable.
- The distinguishing character or personality of an entity.
- The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.

https://csrc.nist.gov/glossary/term/identity

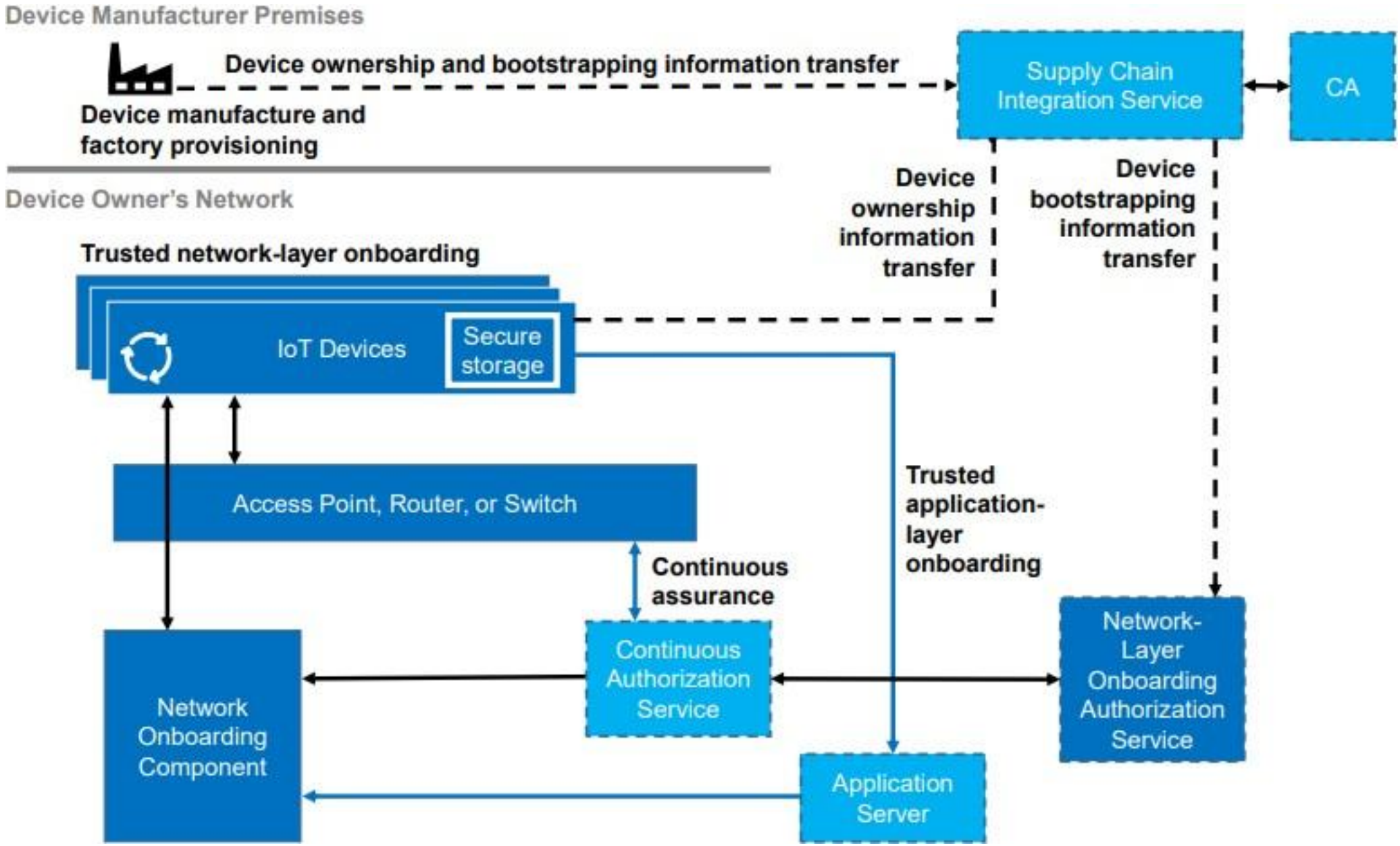
IOT Identity

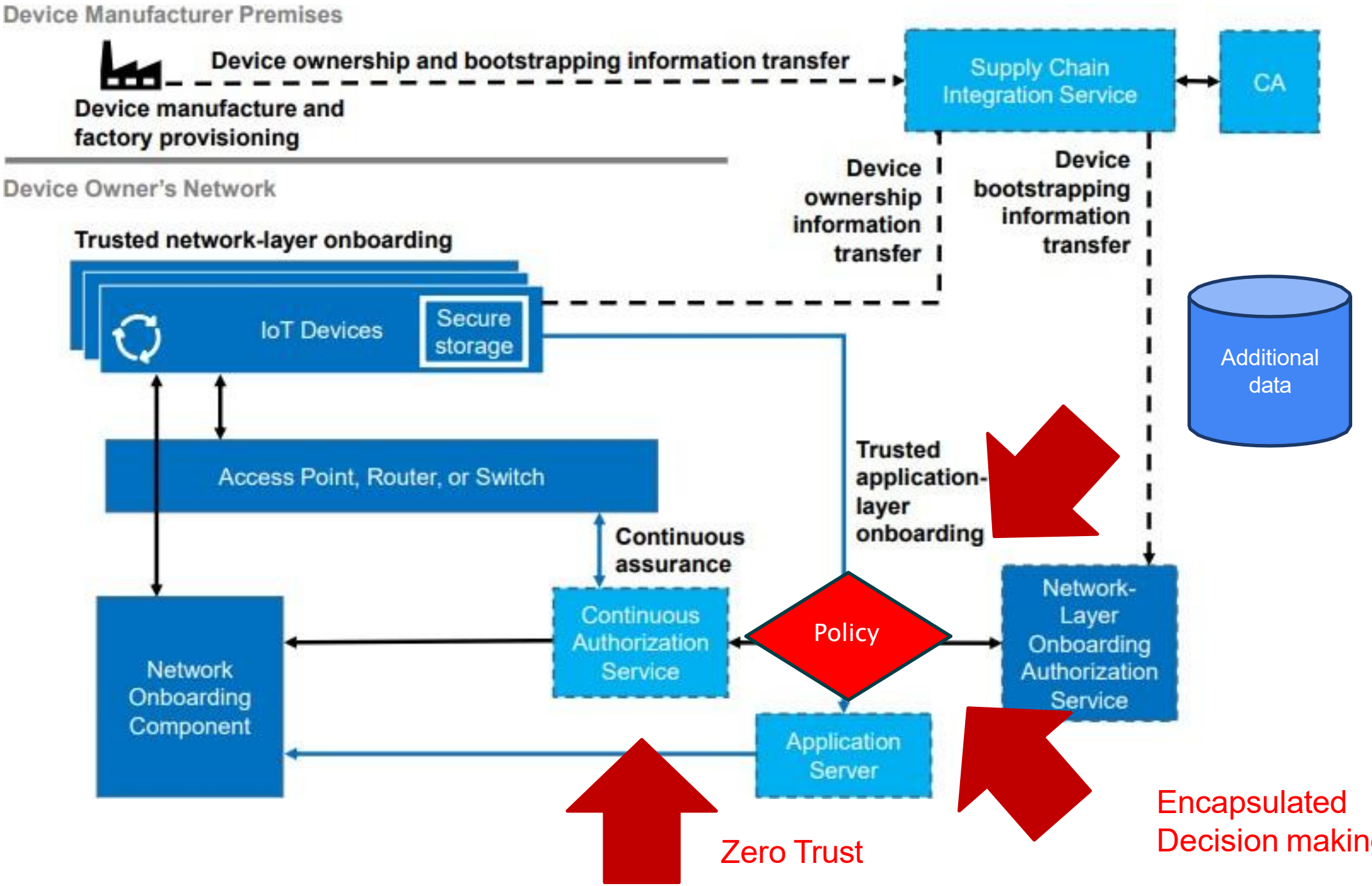
Trusted IOT Lifecycle

Big Picture – why is this important

- No shared passwords (security)
- Low touch provisioning (usability)
- Policy encapsulation (flexibility)
- Supply chain integration (business + security)

Something better than MAC address!!


Device Manufacturer Premises
Device ownership and bootstrapping information transfer
Supply Chain Integration Service
CA
Device manufacture and factory provisioning
Device ownership information transfer
Device bootstrapping information transfer
Device Owner's Network
Trusted network-layer onboarding
IoT Devices
Secure storage
Access Point, Router, or Switch
Trusted application-layer onboarding
Continuous assurance
Network Onboarding Component
Continuous Authorization Service
Network-Layer Onboarding Authorization Service
Application Server


Device Manufacturer Premises
Device ownership and bootstrapping information transfer
Supply Chain Integration Service
CA
Device manufacture and factory provisioning
Device ownership information transfer
Device bootstrapping information transfer
Device Owner's Network
Trusted network-layer onboarding
IoT Devices
Secure storage
Additional data
Access Point, Router, or Switch
Trusted application-layer onboarding
Continuous assurance
Continuous Authorization Service
Policy
Network-Layer Onboarding Authorization Service
Network Onboarding Component
Application Server
Zero Trust
Encapsulated Decision making

Levels of identity in IOT

- Identity of device (iDevID)

IEEE 802.1

Working Group Policies and Procedures
- 802.1 Email Lists
- 802.1 Working Group Leadership
- 802.1 Working Group Membership

Future Sessions

Documents
- Public Documents
- Committee Documents
- Active Ballots
- Incoming and Outgoing Liaisons
- Management Information Base (MIB) Modules

Search

802.1AR: Secure Device Identity

Full title: IEEE Standard for Local and metropolitan area networks–Secure Device Identity

Local Area Networks (LANs) are often deployed in networks that provide publicly accessible services or cannot be completely physically secured. Protocols that configure, manage, and regulate access to these networks typically run over the networks themselves. Secure and predictable network operation depends on authenticating each device attached to and participating in the network, so that the degree of trust and authorization to be accorded to that device by its communicating peers can be determined. Authentication of a human user, through a credential known to or possessed by that user, is often used to authenticate devices such as laptop personal computers, but many network devices are designed for unattended autonomous operation and do not support user authentication.

This standard specifies Secure Device Identifiers (DevIDs) designed to be used as interoperable secure device authentication credentials with Extensible Authentication Protocol (EAP) and other industry standard authentication and provisioning protocols. A standardized device identity facilitates interoperable secure device authentication and simplifies secure device deployment and management.

A device with DevID capability incorporates a globally unique manufacturer provided Initial Device Identifier (IDevID), stored in a way that protects it from modification. The device may support the creation of Locally Significant Device Identifiers (LDevIDs) by a network administrator. Each LDevID is bound to the device in a way that makes it infeasible for it to be forged or transferred to a device with a different IDevID without knowledge of the private key used to effect the cryptographic binding. LDevIDs can incorporate, and fully protect, additional information specified by the network administrator to support local authorization conventions.

The 2018 revision of this standard added the ECDSA P-384/SHA-384 signature suite to align with the Suite B Certificate

in

Search Search

Agendas and Minutes List Archive

Recent Posts
- May 2026 Interim Session in Munich, Germany
- YANGsters Electronic Meeting Agenda – March 24, 2026
- Maintenance TG Electronic Meeting Agenda – March 31, 2026
- Draft Agenda: IEEE 802 Nendica Meeting 2026-04-02
- Agenda: IEEE 802.1 / 802.15 joint meeting 2026-03-10
- March 2026 Plenary Session – Maintenance TG Agenda
- March 2026 Plenary Session – Security TG Agenda

Categories
- Joint WG Agendas
- Latest News

But its not that easy

nquiringminds

- Identify of device (iDevID)
- Identity of network
- Identity of device manufacturer
- Identity of device type
- Identity of device owner
- Identity of network owner
- Identity of the software
- Identity of the application services

Methods for authentication

Policy for authorization

nquiringminds

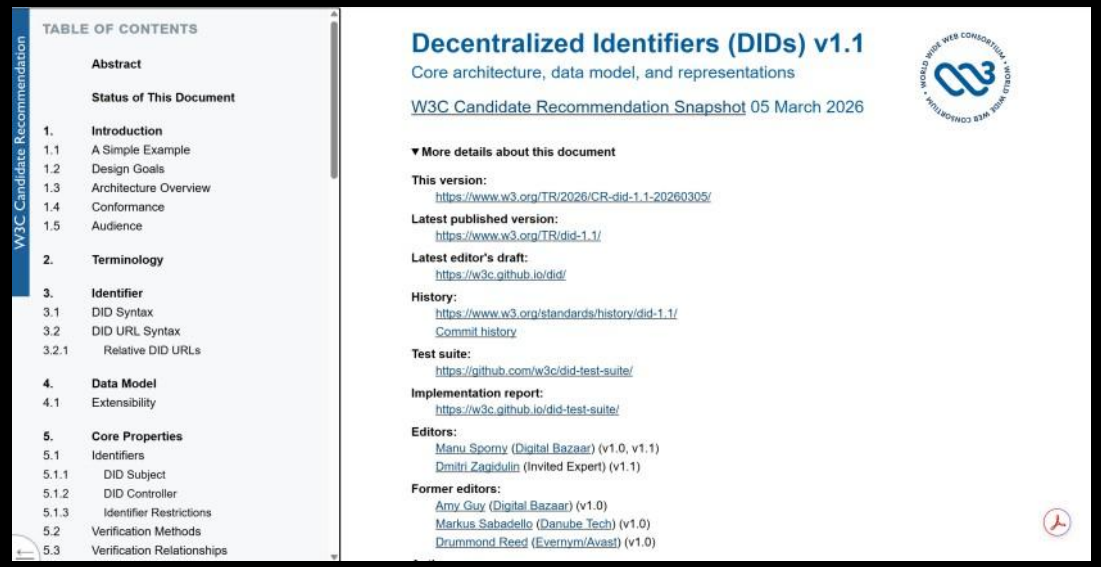
Incremental Challenge…..

Continuous assurance

- Lifecyle management!
- Reacts to changes in environment & information
- Reuses same policy framework
- Simple Radius server extension implementation
- Can be extended to other “Policy decisions"

A unifying approach

DIDs and VCs



W3C Candidate Recommendation

TABLE OF CONTENTS

Decentralized Identifiers (DIDs) v1.1

Core architecture, data model, and representations

W3C Candidate Recommendation Snapshot 05 March 2026

▾ More details about this document

This version:
https://www.w3.org/TR/2026/CR-did-1.1-20260305/

Latest published version:
https://www.w3.org/TR/did-1.1/

Latest editor's draft:
https://w3c.github.io/did/

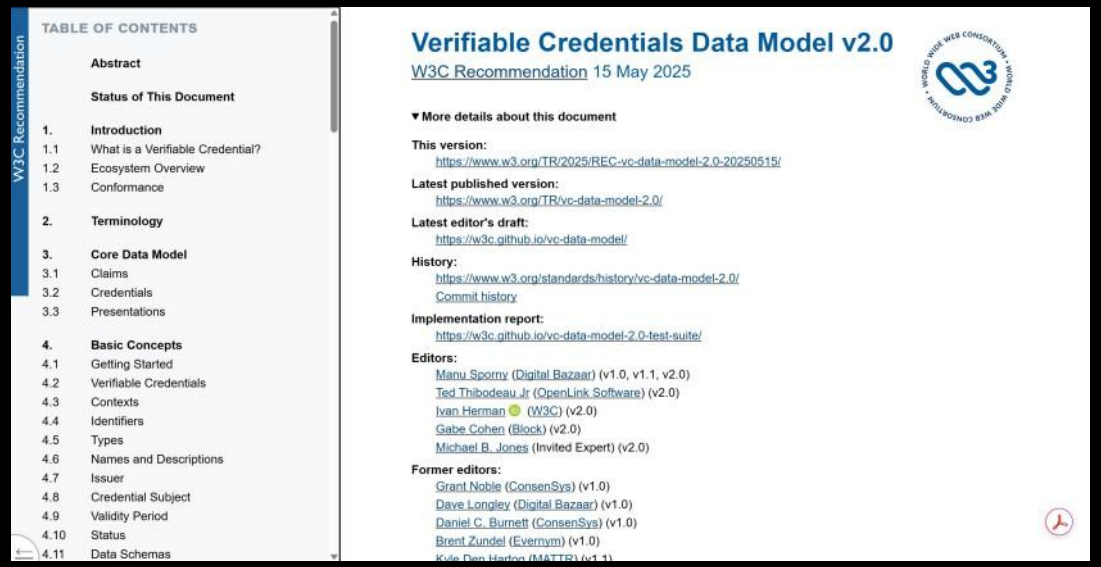
History:
https://www.w3.org/standards/history/did-1.1/
Commit history

Test suite:
https://github.com/w3c/did-test-suite/

Implementation report:
https://w3c.github.io/did-test-suite/

Editors:
Manu Sporny (Digital Bazaar) (v1.0, v1.1)
Dmitri Zagidulin (Invited Expert) (v1.1)

Former editors:
Amy Guy (Digital Bazaar) (v1.0)
Markus Sabadello (Danube Tech) (v1.0)
Drummond Reed (Evernym/Avast) (v1.0)



W3C Recommendation

TABLE OF CONTENTS

Verifiable Credentials Data Model v2.0

W3C Recommendation 15 May 2025

▾ More details about this document

This version:
https://www.w3.org/TR/2025/REC-vc-data-model-2.0-20250515/

Latest published version:
https://www.w3.org/TR/vc-data-model-2.0/

Latest editor's draft:
https://w3c.github.io/vc-data-model/

History:
https://www.w3.org/standards/history/vc-data-model-2.0/
Commit history

Implementation report:
https://w3c.github.io/vc-data-model-2.0-test-suite/

Editors:
Manu Sporny (Digital Bazaar) (v1.0, v1.1, v2.0)
Ted Thibodeau Jr (OpenLink Software) (v2.0)
Ivan Herman (W3C) (v2.0)
Gabe Cohen (Block) (v2.0)
Michael B. Jones (Invited Expert) (v2.0)

Former editors:
Grant Noble (ConsenSys) (v1.0)
Dave Longley (Digital Bazaar) (v1.0)
Daniel C. Burnett (ConsenSys) (v1.0)
Brent Zundel (Evernym) (v1.0)
Kyle Den Hartog (MATTR) (v1.1)

A unifying approach

DIDs and VCs

- **Identity:** DIDs provide an extensible method to identity
- **Interoperable:** interworking standard for all aspects of the stack. More "explicit" than digital certs. Common expression for all crypto artefacts.
- **Data centric security** reduces API/ integration complexity. Integrity, provenance (identity) and revocation baked in.
- **Policy evidence:** better foundation for policy decisions. Explicit trust base. Easy to extend and integrate
- **Composable:** VCs can be combined and reasoned over

Welcome to the IoTSF Device Identity Forum Working Group landing page

What is this group?

This is the Device Identity Forum. It was formed on May 15, 2025. This WG deals with device trust. Every device must reliably declare, “I am who I say I am,” and “I’m safe to connect.” Device identities—unique, hardware-rooted identifiers—provide this foundation, enabling a “chain of trust” that spans from silicon to cloud.

This WG exists to provide technical and marketing guidance to make device identities and and ubiquitous. The Forum meets approximately once a month online, and will produce a number of white papers (see below), as well as various other market guidance.

Key Information

Chair: Michael Richardson, Sandelman Software Works / email: mcr+iotsf@sandelman.ca

Vice-Chair: open

- The inaugural meeting of the group was held on May 15th, 2025 – see the press release
- The inaugural white paper can be found here: Building a System of Trust

Public Slides from previous meetings

Welcome to the IoTSF Device Identity Forum Working Group landing page

What is this group?

This is the Device Identity Forum. It was formed on May 15, 2025. This WG deals with device trust. Every device must reliably declare, “I am who I say I am,” and “I’m safe to connect.” Device identities—unique, hardware-rooted identifiers—provide this foundation, enabling a “chain of trust” that spans from silicon to cloud.

This WG exists to provide technical and marketing guidance to make device identities and and ubiquitous. The Forum meets approximately once a month online, and will produce a number of white papers (see below), as well as various other market guidance.

Key Information

Chair: Michael Richardson, Sandelman Software Works / email: mcr+iotsf@sandelman.ca

Vice-Chair: open

- The inaugural meeting of the group was held on May 15th, 2025 – see the press release
- The inaugural white paper can be found here: Building a System of Trust

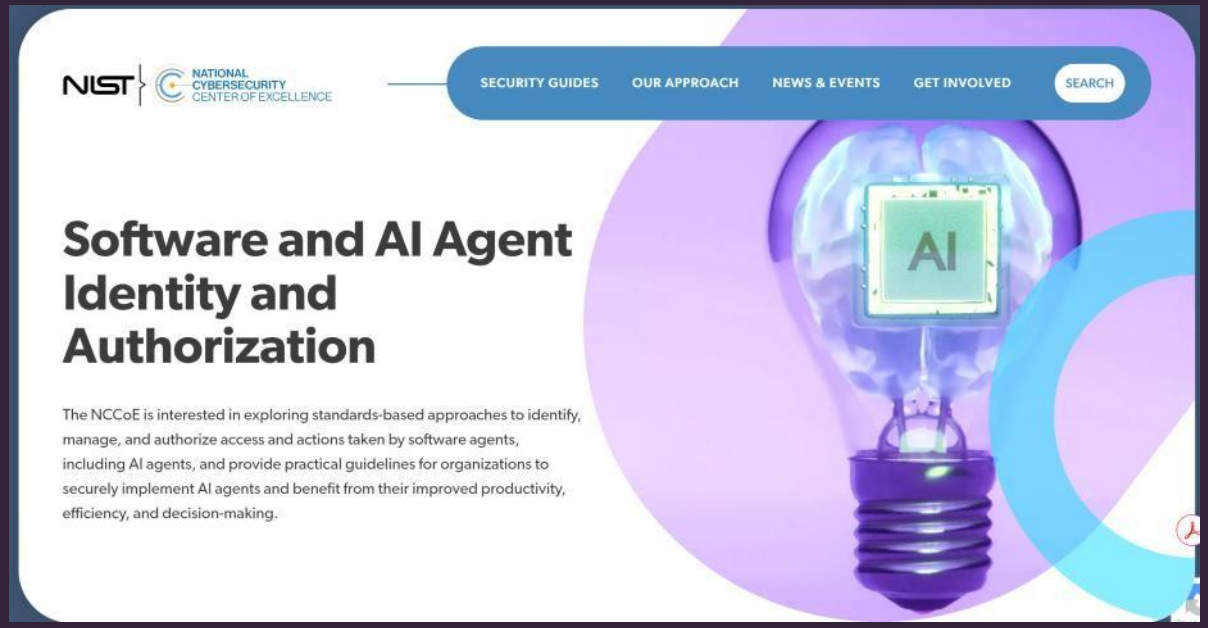
Public Slides from previous meetings

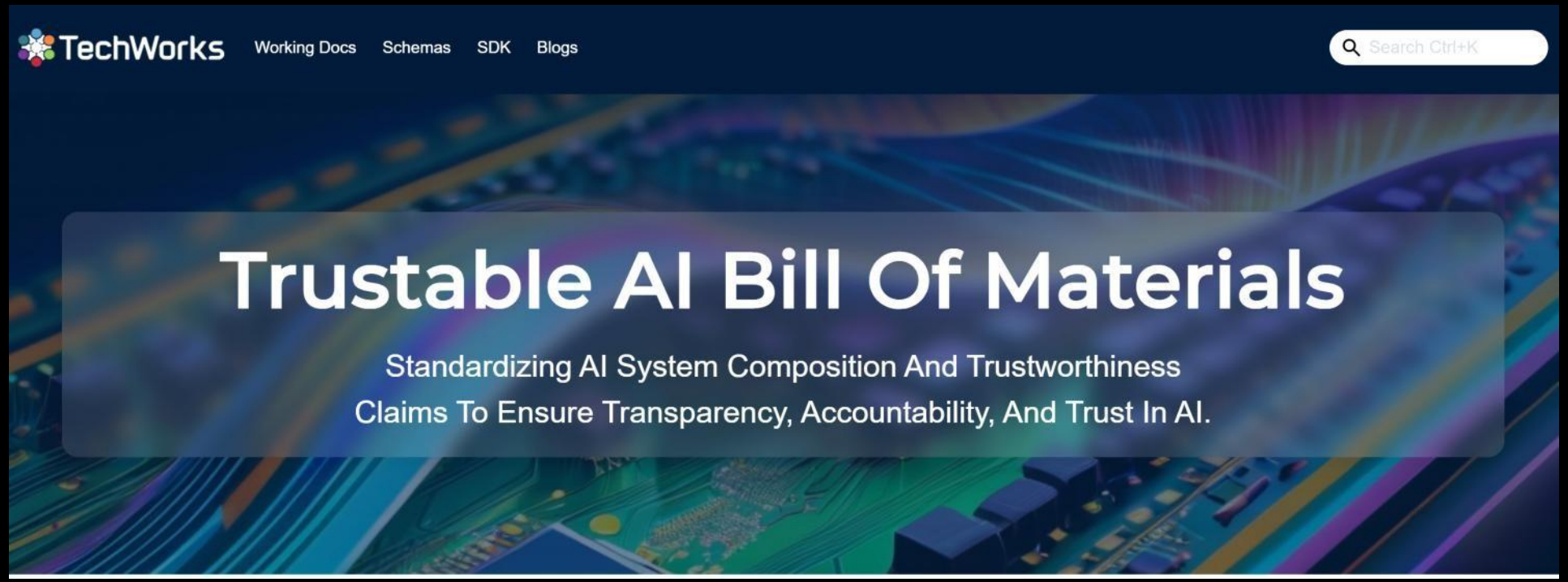
nquiringminds

AI Identity

nquiringminds

Is AI different?

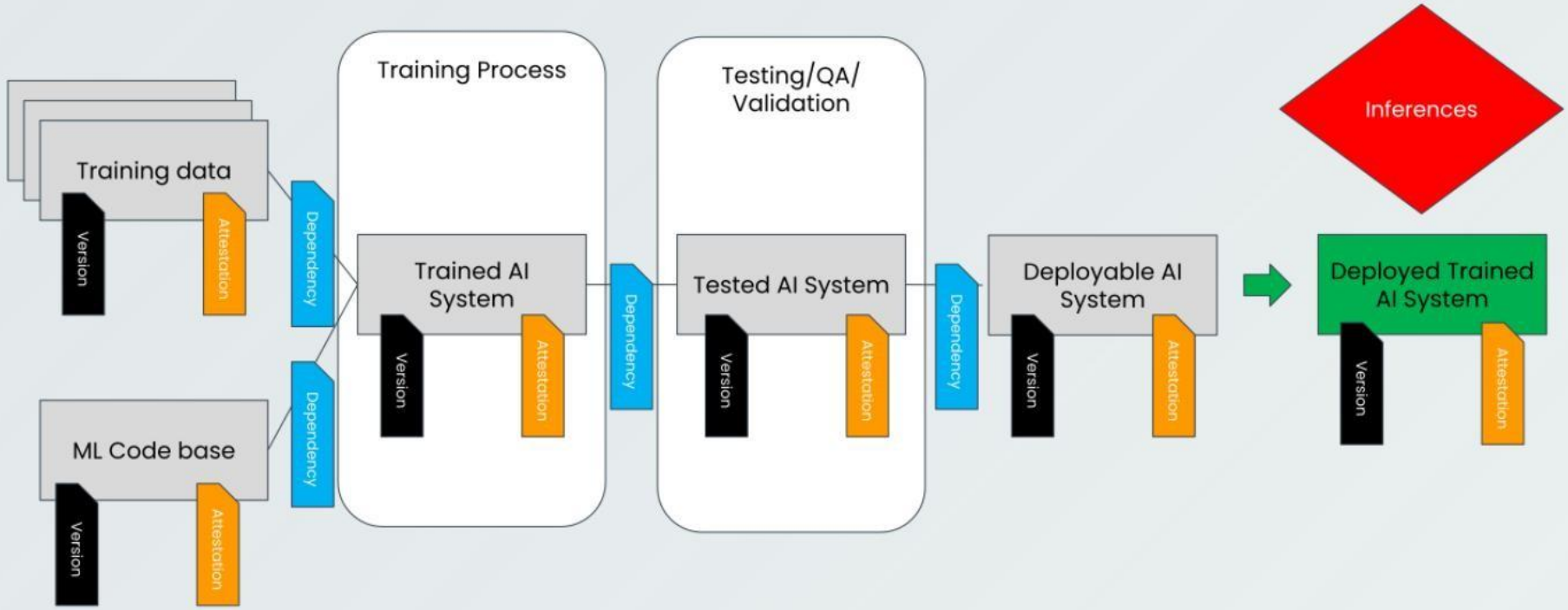



TechWorks
Working Docs
Schemas
SDK
Blogs
Search Ctrl+K
Trustable AI Bill Of Materials
Standardizing AI System Composition And Trustworthiness
Claims To Ensure Transparency, Accountability, And Trust In AI.

Technical Building Blocks

TAIBOM is underpinned by the W3C verifiable credential interoperable standard, and provides:

- **Identity:** A formal method of naming, versioning and validating the constituent parts of an AI system
- **Dependencies:** A method of describing the (complex) system depenencies in AI. It describes how systems are made from parts and how one component has an implied risk dependency on another.
- **Annotation:** A method of annotating components and systems with security, licensing and broader attributes, including positive and negative risk implication
- **Inferencing:** A method of reasoning about the inherent risk in an AI system by transitively propagating risk

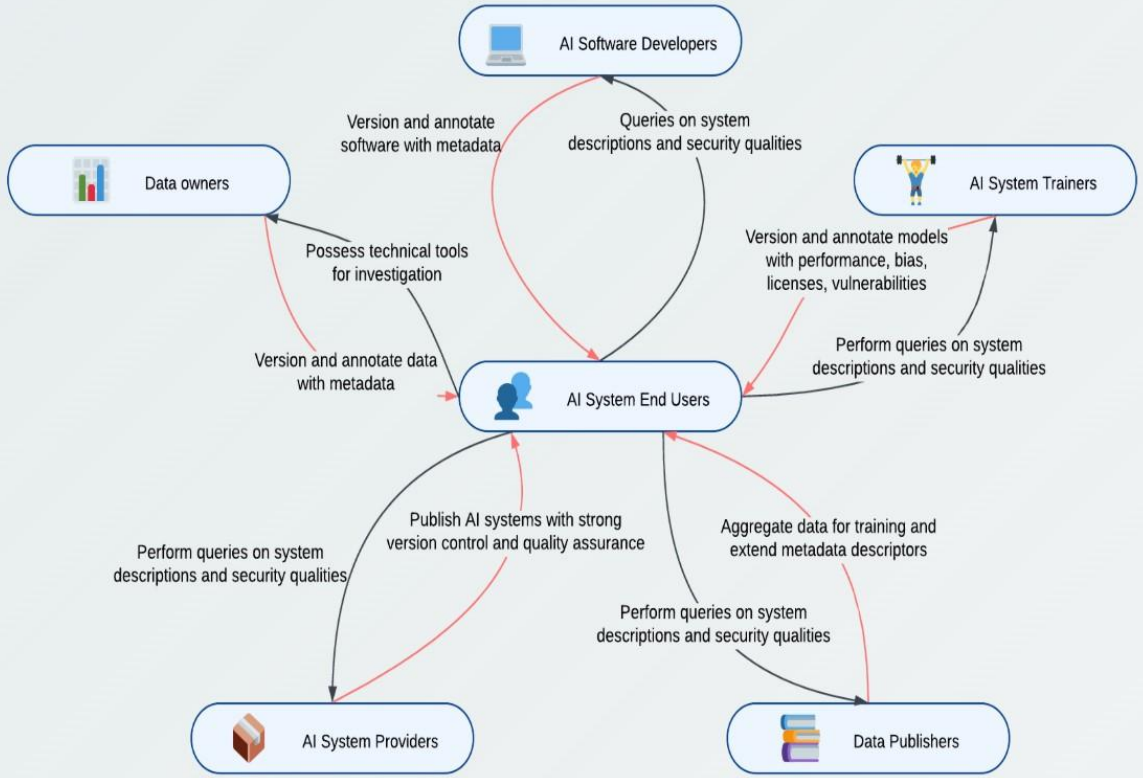


Who Can Use Use TAIBOM

TAIBOM is distributed by nature, to reflect the complex supply chain of AI systems. Likewise the technology can be used by many stakeholders.

- Data owners: owners of the data on which AI systems are trained can version and annotate their data with things like copyright licenses
- AI software developers: can version the software, and annotate this software with licenses or vulnerabilities.
- AI system trainers: can version the trained models and annotate these systems with think like: performance metrics, bias metrics, licences or vulnerabilities
- Data publishers: can aggregate data for training, using or extending the meta data descriptors
- AI system providers: can publish AI systems with strong version control and extended meta data descriptors and quality assurance measures

But the main users are the AI system end users. With TAIBOM the AI system user possess the technical tools to do detailed investigation and quires on the system descriptions and security qualities



nquiringminds

AI Agents are harder

- **Delegation:** working on behalf of who
- **Intent:** what are you asking it to do
- **Least privilege:** what are the bounding conditions
- **Dynamic:** highly dynamic behaviours with external tooling
- **Communications:** How do they interconnect in a trustworthy way
- **Dependencies:** and all of this depends on everything above

Defence

- Digital targeting web
- Next generation targeting
- Combined Joint All-Domain Command and Control

Summary

- **Interoperable:** we need a unifying technology – there's too many specs doing the same thing
- **Policy** drive through the policy use case: Can I – Can you…?.
- **Defence:** defence application are the hardest policy use case

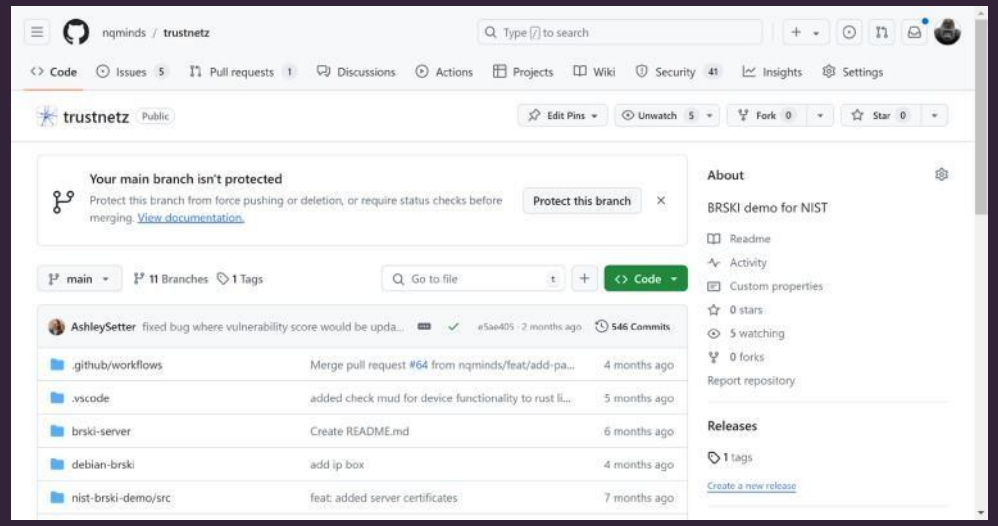
nquiringminds

Open source assets

https://trustnetz.org
https://github.com/nqminds/trustnetz
https://taibom.org/

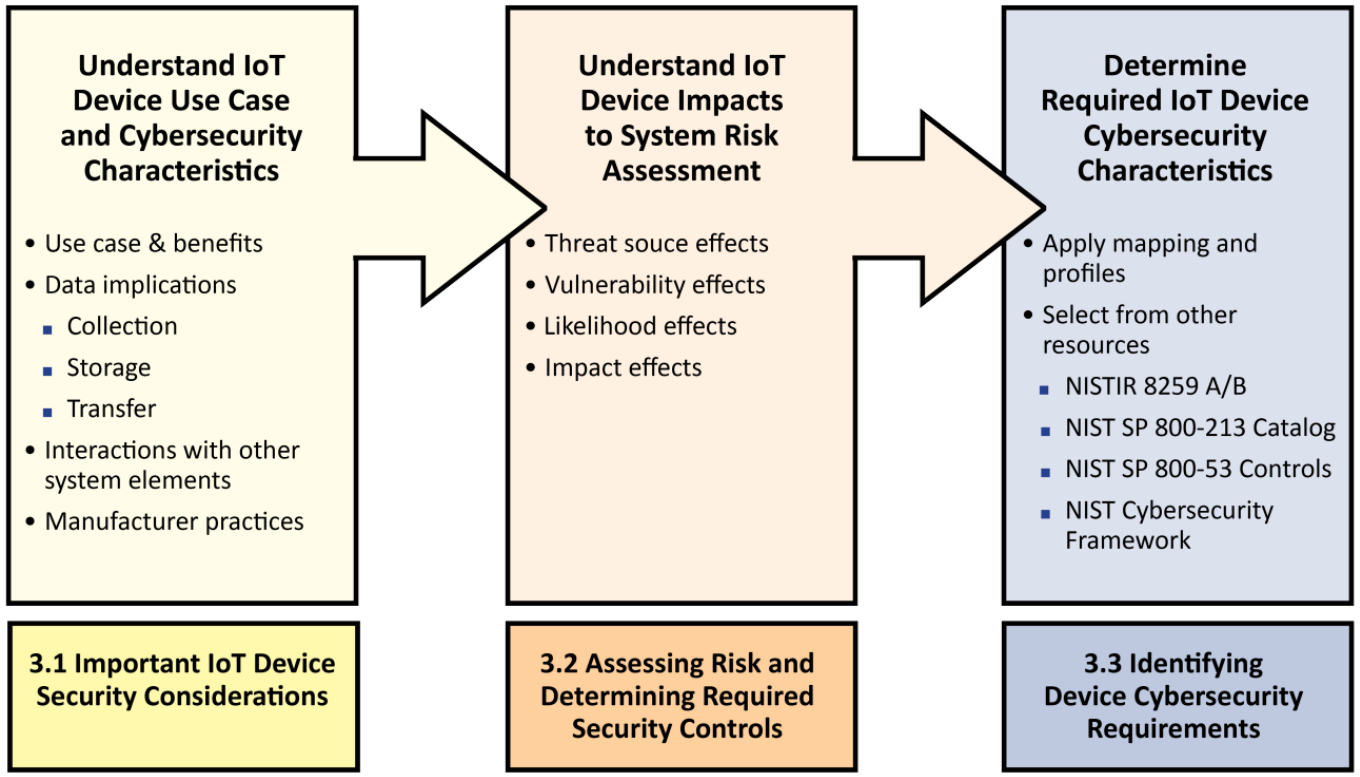
Questions

nick@nquiringminds.com
Nick Allott



Breakout: SP 800-213

A Solid Foundation for Revision



Looking at the last 5 years, we remain confident that the framework established in 2021's SP 800-213 and its basis in the RMF remain useful for approaching the topic by Federal agencies and beyond!

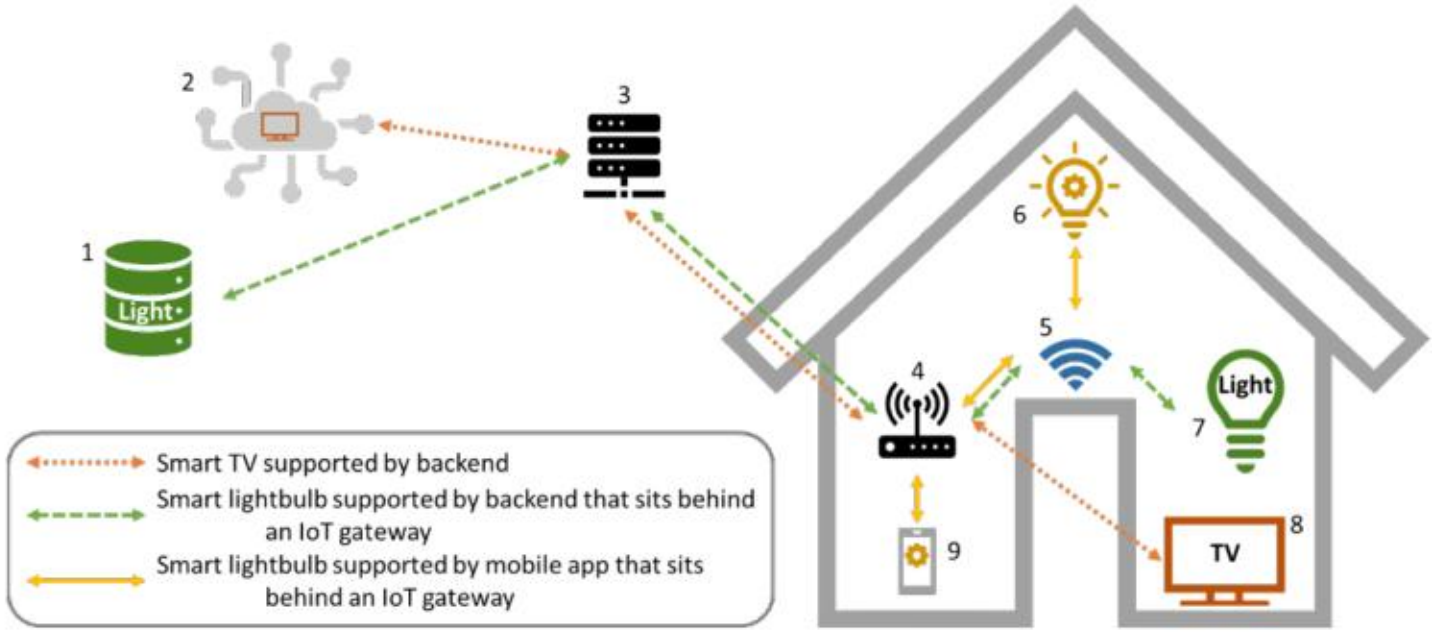
But updates are needed.

The Path Forward

- We're considering switching to product-based language, allowing us to better speak to components, and how they fit into the larger ecosystem.
- We are also thinking about technological changes and convergences and how SP 800-213 can best consider them.

- We need your insights and thoughts as well!
- This will be interactive: please challenge assumptions, share what you're seeing in practice, and help us identify what to keep, what to clarify, and what to change.

What is an IoT ‘Product’?

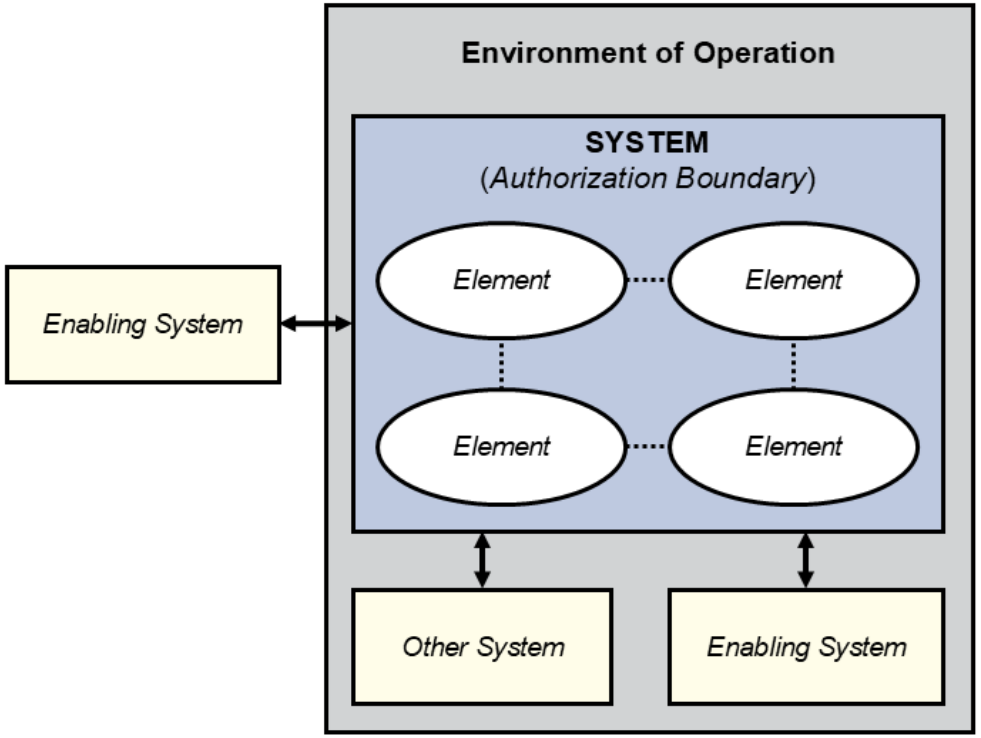


1. Backend for a lightbulb IoT product
2. Cloud service hosting a smart television product application
3. Internet infrastructure
4. Home Wi-Fi router
5. Third-party IoT gateway
6. Locally managed IoT lightbulb
7. Remotely managed IoT lightbulb
8. Smart Television
9. Smartphone app for lightbulb IoT product (running on an individual’s smartphone)

Example from Draft NIST CSWP 33

- IoT products are digital equipment or systems that sense or actuate on the physical world while being connected or connectable to the Internet.
- IoT products may be comprised of a single IoT device and nothing else or they may be comprised of the IoT device and additional IoT product components (e.g., backends, companion applications, and specialty networking/gateway hardware).
- An IoT device has at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface for interfacing with the digital world.

Impact on SP 800-213



The guidelines in SP 800-213 are focused on helping identify requirements to connect IoT products to systems.

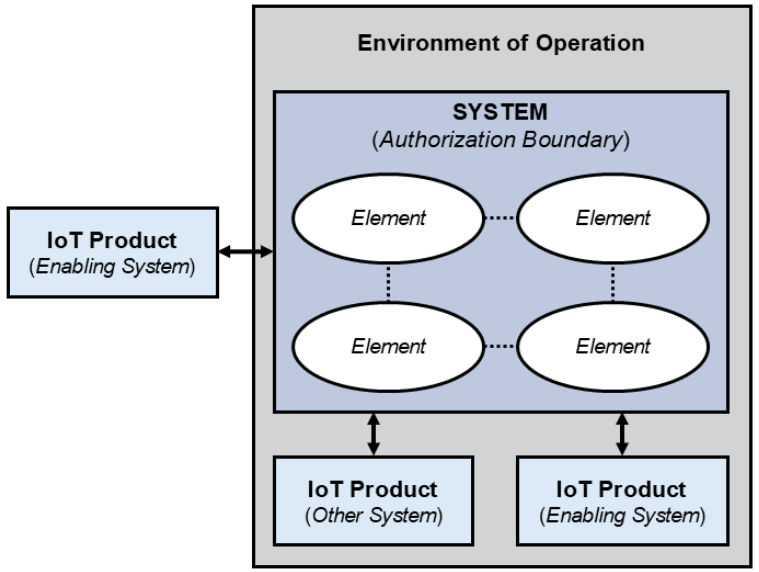
In the current version of SP 800-213, which discusses IoT *devices*, the perspective is of this equipment as an *element* of a system.

When updating to discuss IoT products, we have more potential views of how the IoT product and its components will relate to the system.

Potential System Views

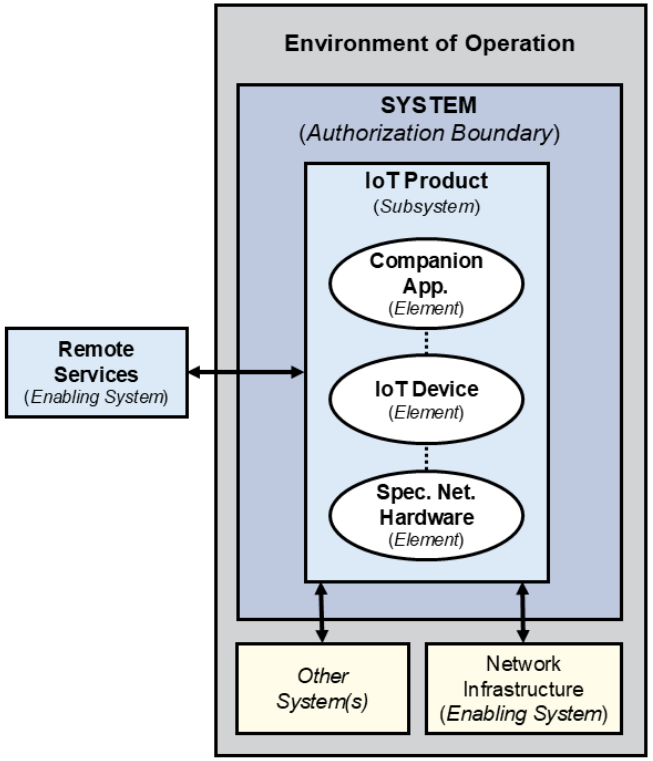
Outside the System

IoT products could be considered entirely outside the system, as *enabling* or *other* systems.



As a Standalone System

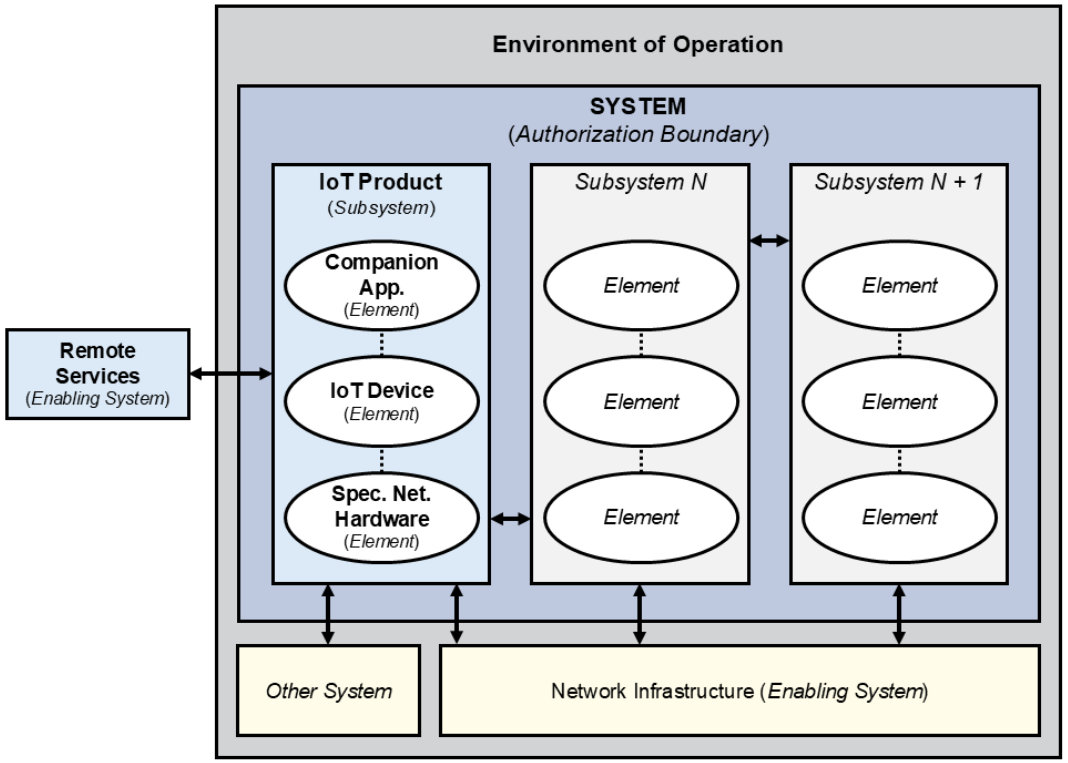
All locally managed IoT product components could be seen as a 'standalone' system.



Potential System Views

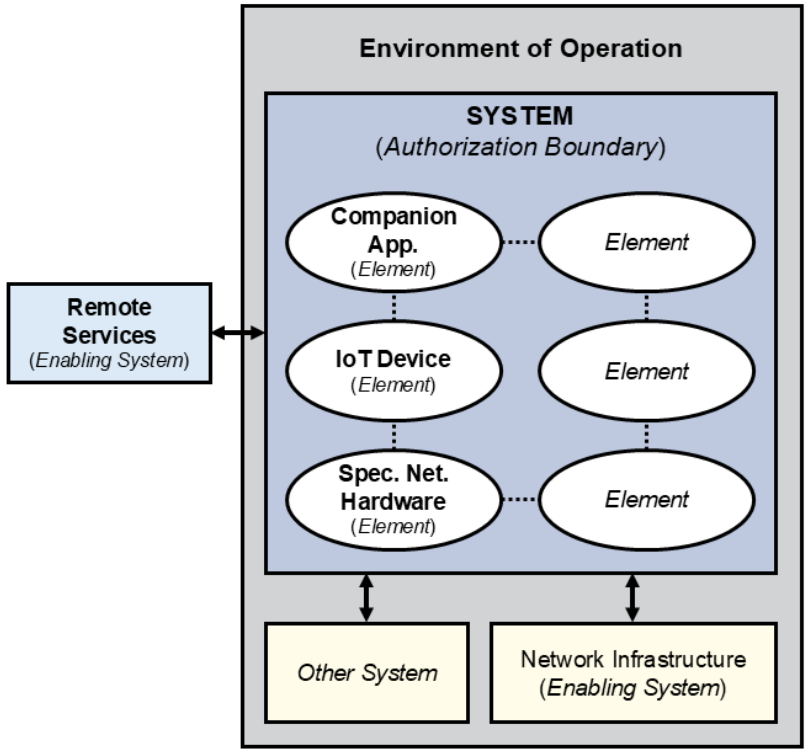
Beside other Systems

IoT products could be considered as a subsystem that will operate beside other subsystems.



Integrated in the System

All locally managed IoT product components could be seen as elements of the system.



Points to Consider for Feedback

1 IoT Products

Were these views of IoT products and how they can relate to the system meaningful?

What considerations could root from these perspectives?

2 Technological Changes

What new developments in technology apply to IoT and should be considered in this update?

How has technology adoption in the Federal Government changed?

3 New Guidelines

What new guidelines and other publications should NIST consider when working on this update?

4 Your Thoughts!

We welcome discussion or any other pertinent topics that can help NIST update SP 800-213!

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Colloquium on Cybersecurity for IoT: Future Directions

Day 2

4/1/26

Next Steps

Within these core principles, the Program must grow and adapt to changes and developments. Today, we will explore how IoT has been adopted for modern applications and what cybersecurity topics can help support further innovation.

Where is IoT technology and adoption today?

What does the future hold in store for IoT?

How can NIST support continued IoT innovation?

Technology Management (HTM)

Medical Device Protection Program

Nadia ElKaissi

Networking & Cybersecurity | Office of HTM

Agenda | Medical Device Protection Program

1 VA AND MEDICAL DEVICE SECURITY OVERVIEW

2 VA MEDICAL DEVICE PROTECTION PROGRAM

Overview | Mission and Vision

U.S. Department of Veterans Affairs

HTM

Healthcare Technology Management

MISSION

Honor Veterans by developing and guiding comprehensive management of healthcare technologies to assure safe, available, and innovative medical technology used to deliver exceptional health care for Veterans.

VISION

Be an efficient, innovative and customer-oriented Center of Excellence that continually enhances VHA's ability to deliver world class health care for our nation's Veterans through exceptional management of healthcare technology as well as position VHA as the national leader healthcare technology management in the healthcare industry.

US Department of Veterans Affairs (VA) Healthcare Technology Management (HTM)

Overview | VA HTM by the Numbers

1 CENTRAL OFFICE

18 VETERAN INTEGRATED SERVICE NETWORKS

171 MEDICAL CENTERS

$10 billion
of healthcare technology

900,000
medical devices and clinical systems

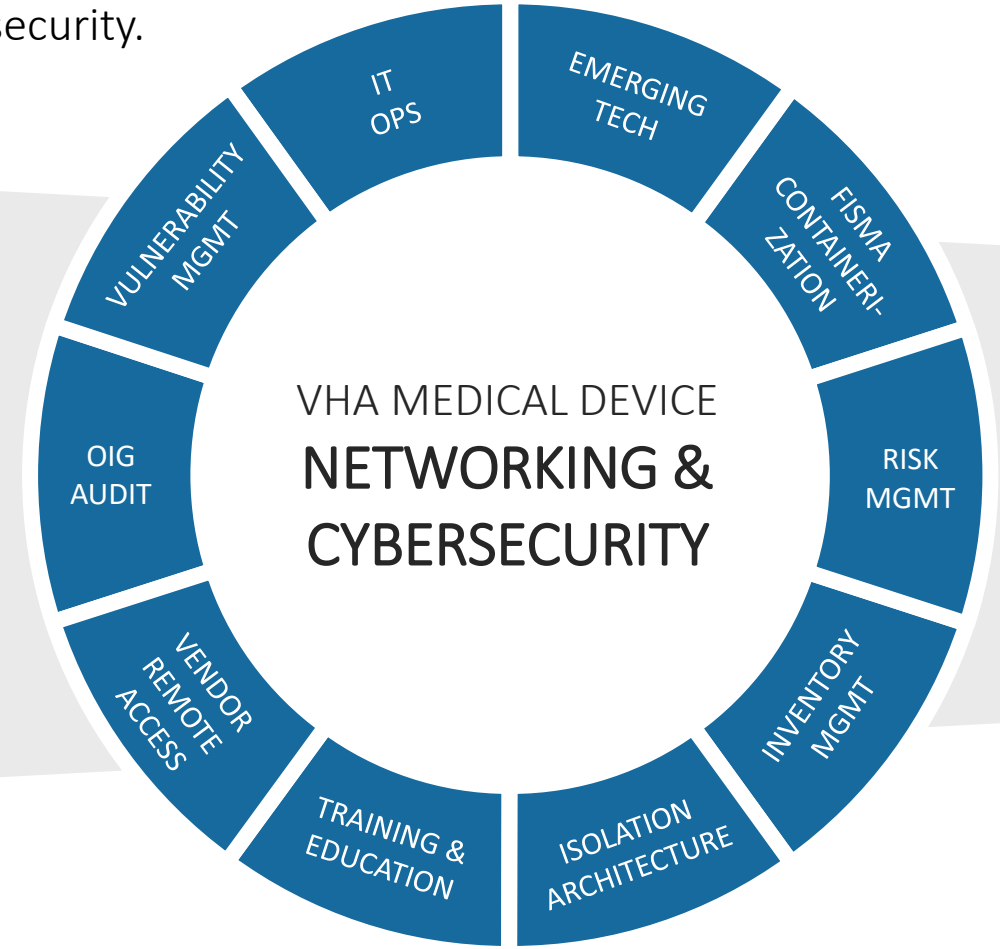
155,000
network connected medical devices

2,200
Biomedical Engineering professionals

Overview | Medical Device Protection Program

VA's MDPP is a comprehensive security initiative intended to better safeguard network-connected medical devices and mitigate risks to patient safety and cybersecurity.

MDPP
Medical Device Protection Program



Overview | Medical Device Protection Program

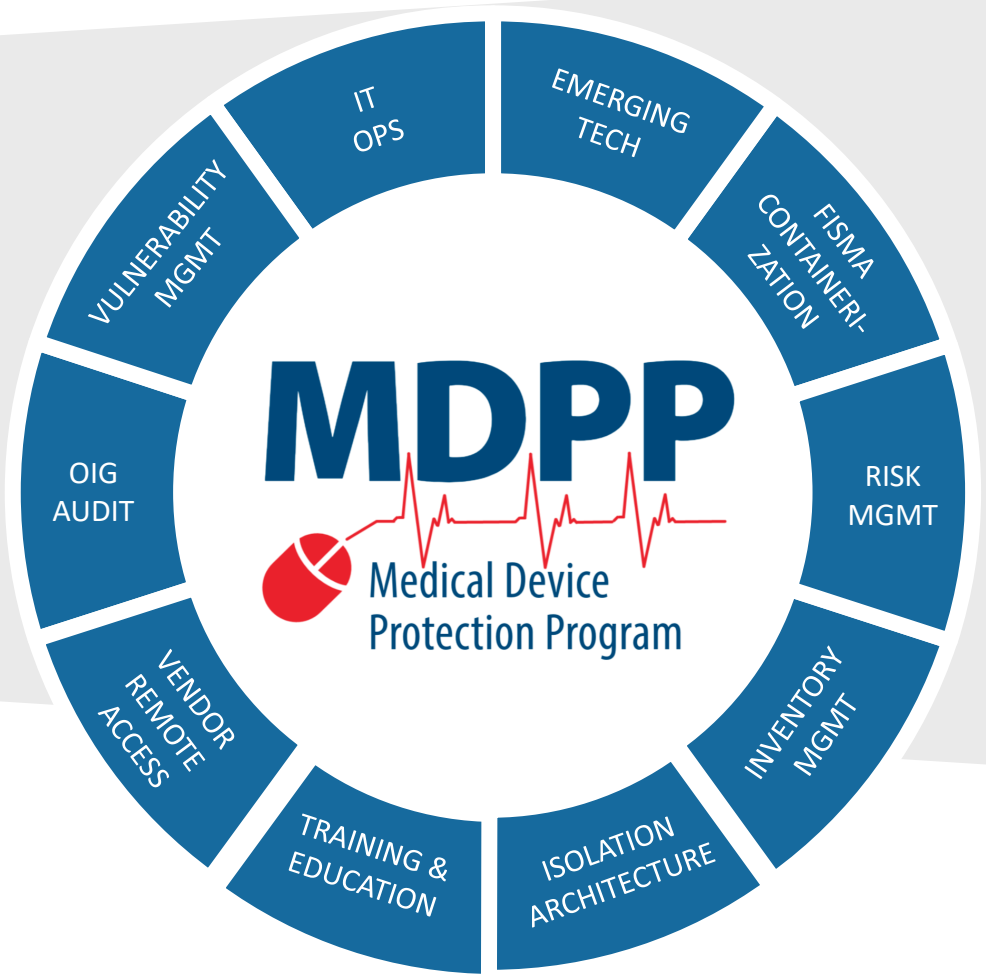
VHA HTM relies on the **field-based subject matter experts** who volunteer as members of the MDPP

2 Office of HTM FTEE

10 subgroups

90+ members

60+ unique members



Centralized **patch approval repository** with 7,000 entries

Standardized inventory of networked devices and clinical systems

Full suite of **medical device standards and policies**

Robust **tracking and reporting** of **vulnerabilities**

Annual cybersecurity **audit readiness program**

Medical Device Protection Program | Risk Management

ENTERPRISE RISK ANALYSIS

Requires VA HTM and manufacturer input for all VA networked medical devices and systems

- Identifies the inherited risk and impact to the VA
- Documents and addresses system specific security controls
- Manages and addresses vulnerabilities

1 VA 6550 APPENDIX A

VA-specific pre-procurement assessment form for cybersecurity features, such as FIPS 140-2 or 140-3 certification, antivirus and OS patching, data encryption capabilities and electronic health record compatibility.

2 MANUFACTURER DISCLOSURE

Standard document -- Manufacturer Disclosure Statement for Medical Device Security (MDS2) -- for manufacturers to communicate cybersecurity information about their equipment.

3 INVENTORY LIST

Listing of device name, type, model, operating system, operating system version, and software application name and versions for all networked devices and peripherals within the system.

4 PORTS & PROTOCOLS

Listing of Ports, Protocols, and Services (PPS) to record communication service (SMTP, DNS, DICOM, Custom Comms, etc.), port numbers, protocol (TCP, UDP, IP), communication direction, external IP communications, and reason for use.

5 NETWORK TOPOLOGY

Diagram showing Accreditation Boundary of the system, all directional communication services as identified by the PPS, and any communications to systems outside of the VA network.

6 Additional Vendor Documentation

Letter of attestation, vulnerability scan, SBOM.

Medical Device Protection Program | Risk Management

ENTERPRISE RISK ANALYSIS

Requires VA HTM and manufacturer input for all VA networked medical devices and systems

- Identifies the inherited risk and impact to the VA
- Documents and addresses system specific security controls
- Manages and addresses vulnerabilities

- Evaluate the device, network architecture, additional vendor documentation
- Assess vulnerabilities and exposure pathways
- Determine clinical criticality and usage
- Assign risk level based on impact and likelihood
- Define path forward:
  - Mitigate
  - Accept with justification
  - Recommend Alternatives

Medical Device Protection Program | FISMA Containerization

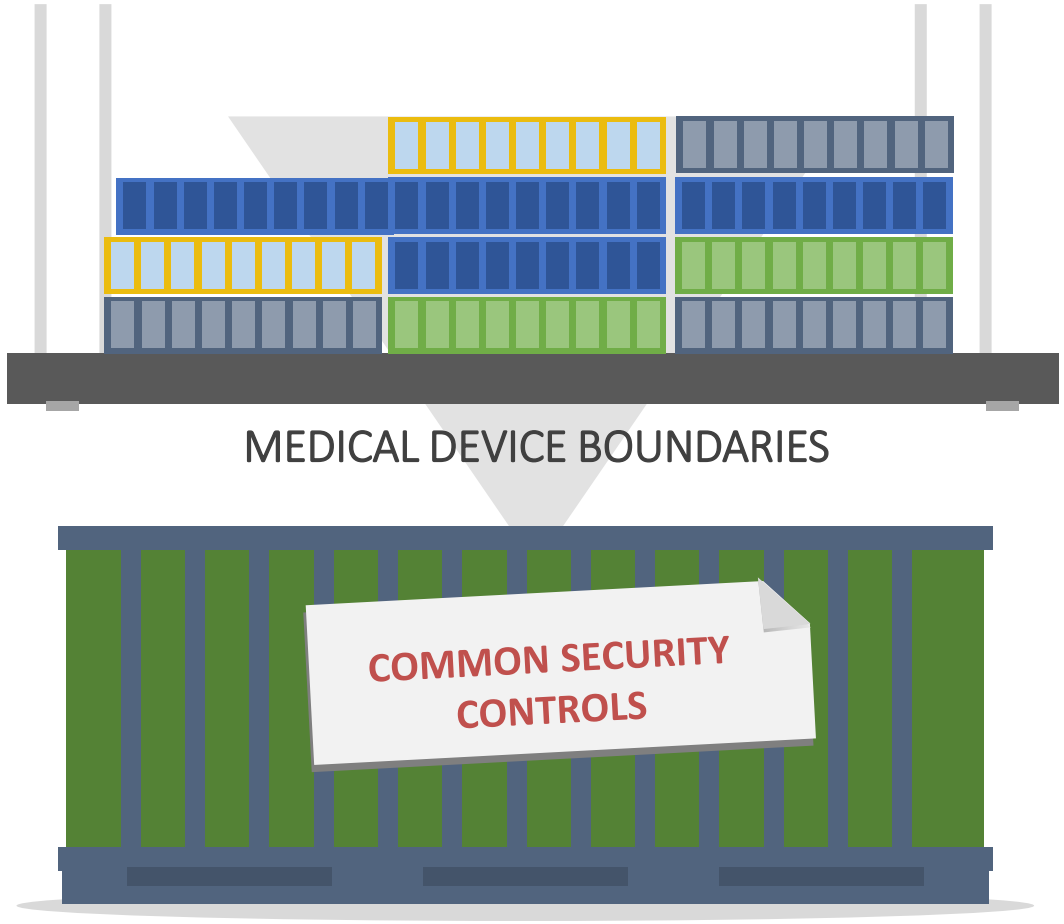
FISMA

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

Requires each federal agency to develop, document, and implement an information security program

All networked devices must be included in the Continuous Authorization Monitoring (CAM) for inventory tracking and reporting.

Assets are assigned to different boundaries within CAM and require documentation to demonstrate compliance with the security controls and achieve authorization to connect.



Streamline Security Processes

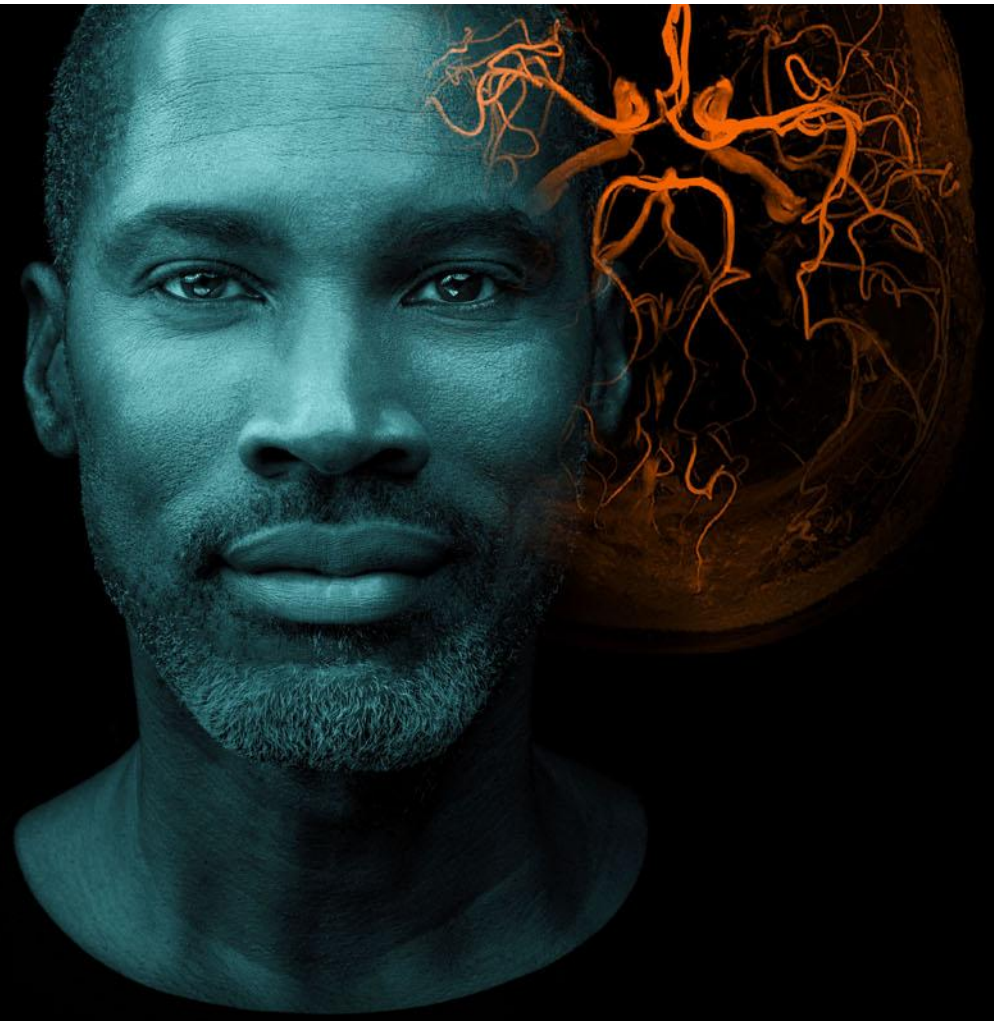
Improve Governance

Allow For Enterprise-level Plans of Actions & Milestones POA&Ms

SIEMENS Healthineers

NIST

Cybersecurity for IoT Workshop: Future Directions



Connor Walsh

April 2026

Manufacturer Perspective on Secure Integration of Medical Devices in Clinical Environments

- Medical device manufacturer view
- Intersection of product security, healthcare operations, and regulatory reality
- Focus on practical deployment in clinical environments

- **Goal: secure, safe, and operationally workable device deployment**

What Matters Most in Medical Device Cybersecurity

- Patient Safety
  - Cybersecurity supports safe and reliable care
- Customer Enablement
  - Providers need actionable guidance, not just features
- Shared Responsibility
  - Manufacturers, HDOs, and government each have distinct roles
- Operational Reality
  - Controls must work in live clinical environments

- **The objective is not security in isolation, but secure and safe clinical use.**

How Manufacturers Can Help Enable Secure Adoption

- Secure defaults and reduced attack surface
- Clear deployment and hardening guidance
- Documentation of network requirements and data flows
- Support for segmentation and access control
- Actionable vulnerability communications
- Practical patching and compensating control pathways

Good security guidance reduces ambiguity and helps providers make risk-informed decisions.

Questions?

SIEMENS Healthineers

1. Connor Walsh
    1. Connor.walsh@siemens-Healthineers.com

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity

CONTACT US

NIST.gov/cybersecurity

@NISTcyber

NIST Cybersecurity for IoT Program Home Page