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

Keynote

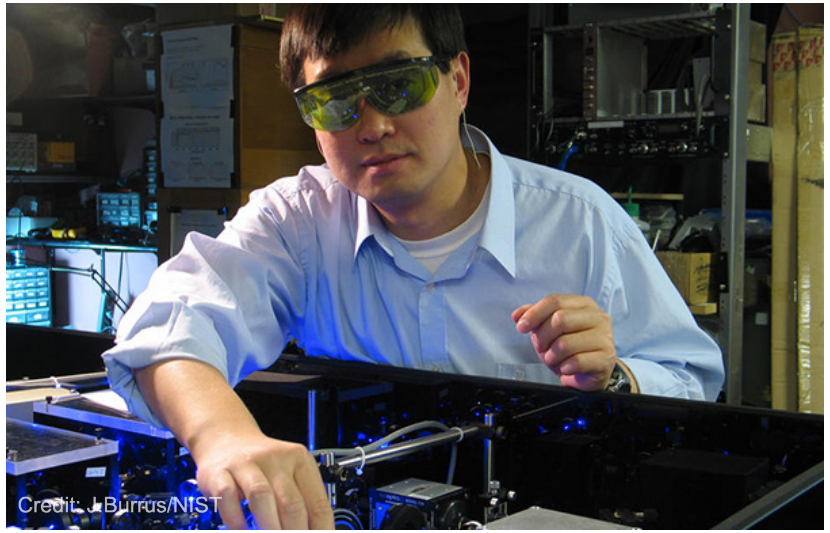
Overview of Current U.S. IoT Legislation and Outlook for the Future

Paul Watrobski | NIST

14 April 2022

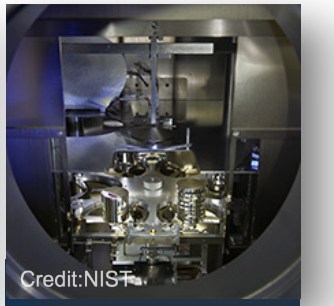
NIST Mission

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

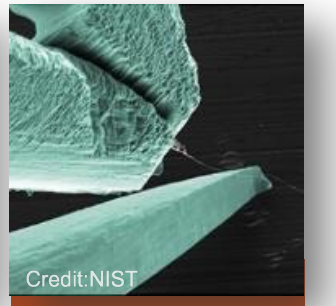


Physical Measurement Laboratory

Engineering Laboratory

Information Technology Laboratory

Communication Technology Laboratory



Center for Nanoscale Science and Technology

NIST Center for Neutron Research

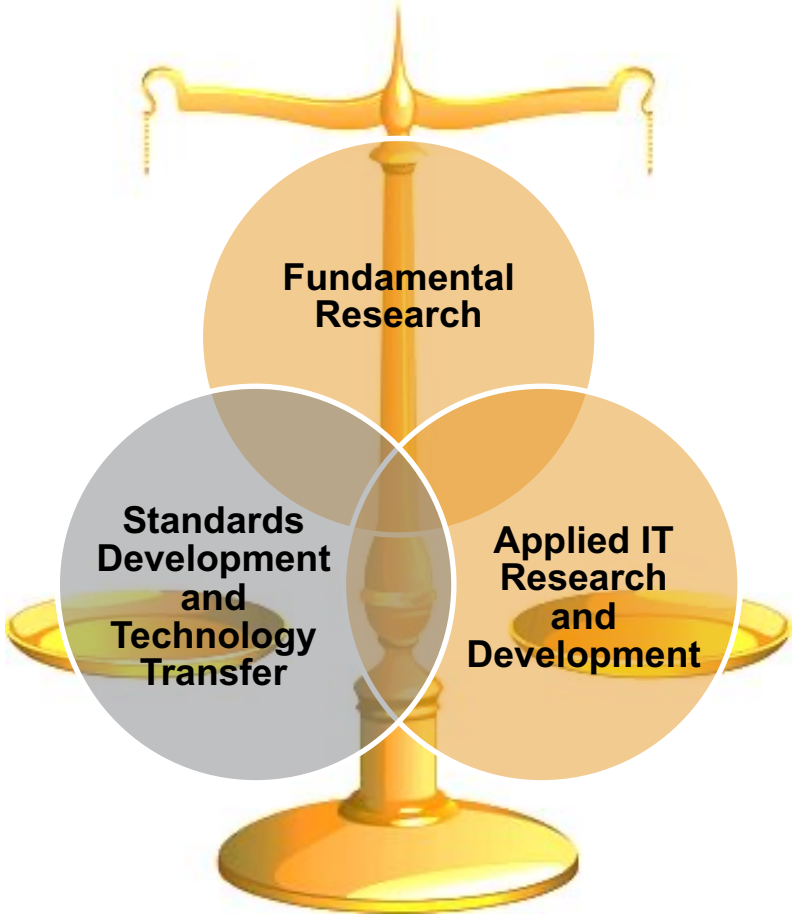
Information Technology Laboratory – itl.nist.gov

Cultivating Trust in IT and Metrology

Standards and Guidelines Development – csrc.nist.gov

- Cryptographic Development – AES, SHA-3, PQC, etc.
- Cryptographic Validation – FIPS 140-3
- Risk Management Framework – Cybersecurity Framework, FISMA, SP 800-53, SP 800-171, etc.
- Technology Guidelines – Virtualization, Containers, Security Automation, etc.
- Framework for cybersecurity, privacy, workforce, and secure software development
- Identity Management

Cybersecurity Program



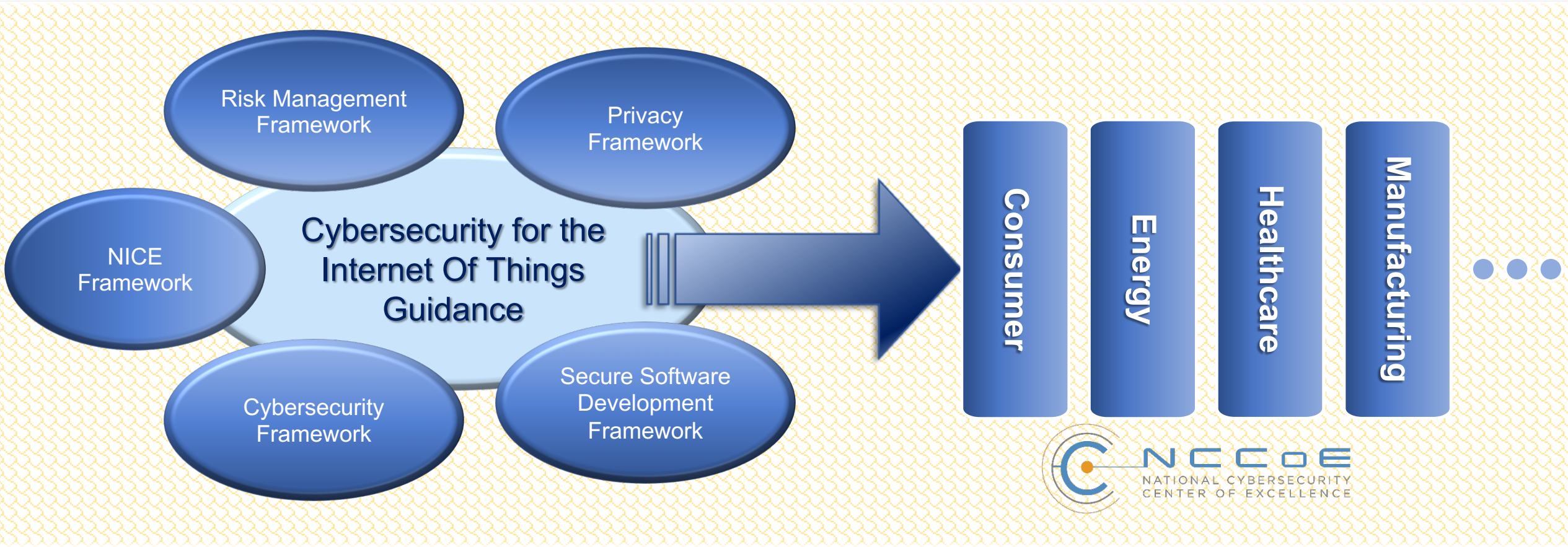
National Cybersecurity Center of Excellence (NCCoE) – nccoe.nist.gov

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

- DEFINE
- ASSEMBLE
- BUILD
- ADVOCATE

Collaboration with Industry, Federal/State/Local Governments, and Academia

Example Implementations of Guidance



Key publications and external drivers for the NIST IoT Cybersecurity Program

8200: International Standardization Status

8201: IoT Colloquium Report

8228: Considerations for Managing IoT Security & Privacy Risks

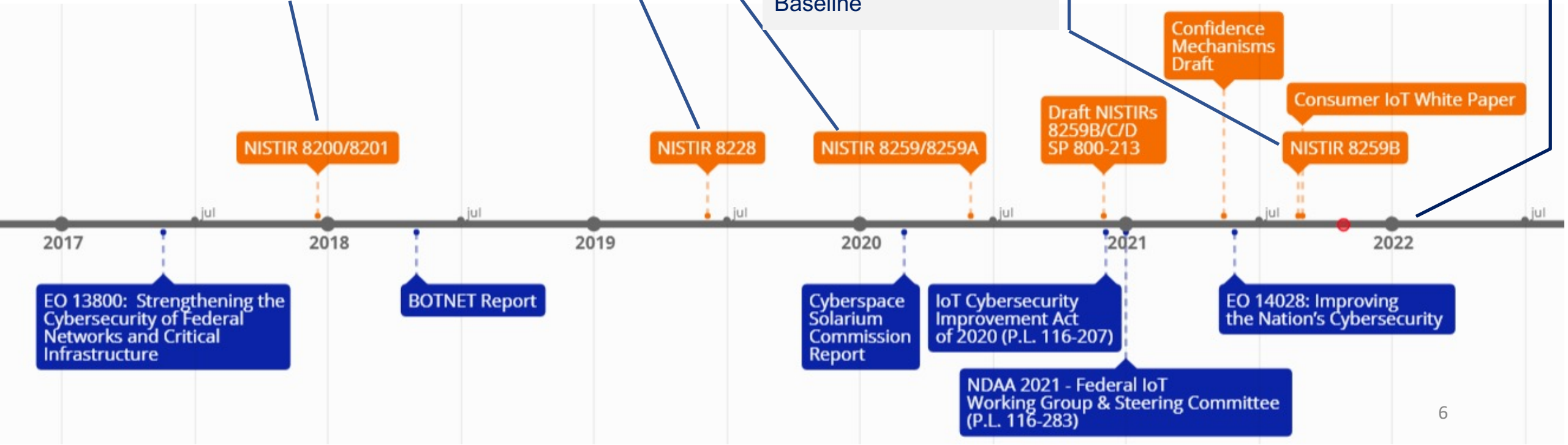
8259: Recommendations for Manufacturers

8259A: Core Device Cybersecurity Baseline

8259B: Non-Technical Supporting Capability Core Baseline

Recent:

- **SP 800-213 / -213A** (Nov 2021)
- **Consumer IoT Criteria** (Feb 2022)



Description of IoT Products

An IoT product is an **IoT device** and any additional **product components** that are necessary to using the IoT device beyond basic operational features.

An IoT device has…

At least one **transducer** for interacting directly with the **physical world**

(e.g., a sensor or actuator)

&

At least one **network interface** for interfacing with the **digital world**

(e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB])

State Legislation

- California – Internet of Things Cybersecurity Improvement Act of 2017
  - California Civil Code § 1798.91.04 took effect in 2020 – requiring manufacturers of IoT devices to them with “reasonable security” features that are:
    - appropriate to the nature and function of the device
    - appropriate to the information the device may collect, contain, or transmit
    - designed to protect the device and any information contained on the device from unauthorized access, destruction, use, modification, or disclosure
- Oregon – passed a similar law in 2019 (Bill 2395 amending ORS 6456.607) regarding manufacturers of “connected devices”
- Illinois, Kentucky, Massachusetts, Maryland, New York, Rhode Island*, Vermont, and Virginia considered/considering similar legislation

May 2021 E.O. directed NIST to identify IoT Cybersecurity criteria and pilot labeling program

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

Criteria

- *What criteria are products assessed against?*

Label

- *What should the label look like and what should it contain?*

Conformity

- *How is conformity with criteria demonstrated?*

How do we get from drivers to fulfillment?

- Identify drivers & expectations
  - Security properties; consumer understandable; market discriminator; regulation necessary or not
- Develop requirements & standards
  - Meet the expectations and overall drivers; support repeatable and reproducible tests
- Conformity assessment model & information
  - Evidence of requirements met at the desired level of confidence, while being cost-effective and efficient
- How do we get to fulfillment?
  - Adoption based on alignment of drivers/expectations, requirements, and confidence
- Not always a straight line from consensus to fulfillment
- The best standard (technically?) does not always succeed in the market

Responding to E.O. 14028: The path we've traveled ...

- **Establishing Confidence in IoT Device Security: How do we get there?**
  - **Seven broad themes identified** ranging from topics such as fragmentation to expectations around role of customer in security
- **Conducted a landscape review of consumer IoT**
  - Surveyed 28 Informative References
  - Applied IoT Product Perspective
- **DRAFT Baseline Security Criteria for Consumer IoT Devices (31 August)**
  - Include Product Technical Criteria & Non-Technical Supporting Actions
  - Started from Core Baseline (NISTIRs 8259A / 8259B)
  - Added "Product" criteria
  - Over 400 comments received
- **Workshop on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software (14-15 Sept)**
  - Panel discussions and participant input
  - Nearly 550 participants
- **Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward (2 December)**
  - Incorporated formal and informal feedback on 31 August draft
- **Workshop on Cybersecurity Labeling for Consumer IoT and Software: Executive Order Update and Discussion (9 Dec)**

Cybersecurity Criteria were published Feb 2022

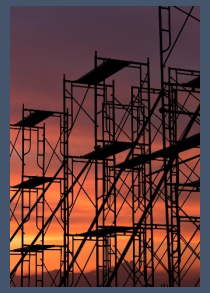
Criteria

- Build on Core Baselines (8259A/B)
  - Starting point to be adapted/tailored for consumer customer needs and goals
- Product Focused
  - Consumer perception
  - Flexibility in implementation

- Outcome based
  - Prescriptive requirements are brittle
  - Focuses on expectation
  - Adoption of standards
- Baseline
  - Consumer cybersecurity risk calculations
  - Profiles to be need/market driven

Focus on Outcomes in Criteria

Flexibility in meeting the criteria to support different approaches to cybersecurity



Allows for a vibrant IoT product conformity and labeling landscape

Easy adaptability as technologies and risks change over time

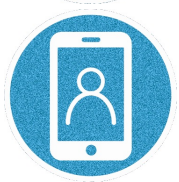
Outcomes speak to the risks they are intended to mitigate

Proposed Baseline IoT Product Criteria


Asset Identification


Product Configuration


Data Protection


Interface Access Control


Software Update


Cybersecurity State Awareness


Documentation


Information and Query Reception


Information Dissemination


Education and Awareness

Labeling & Conformity Considerations published Feb 2022

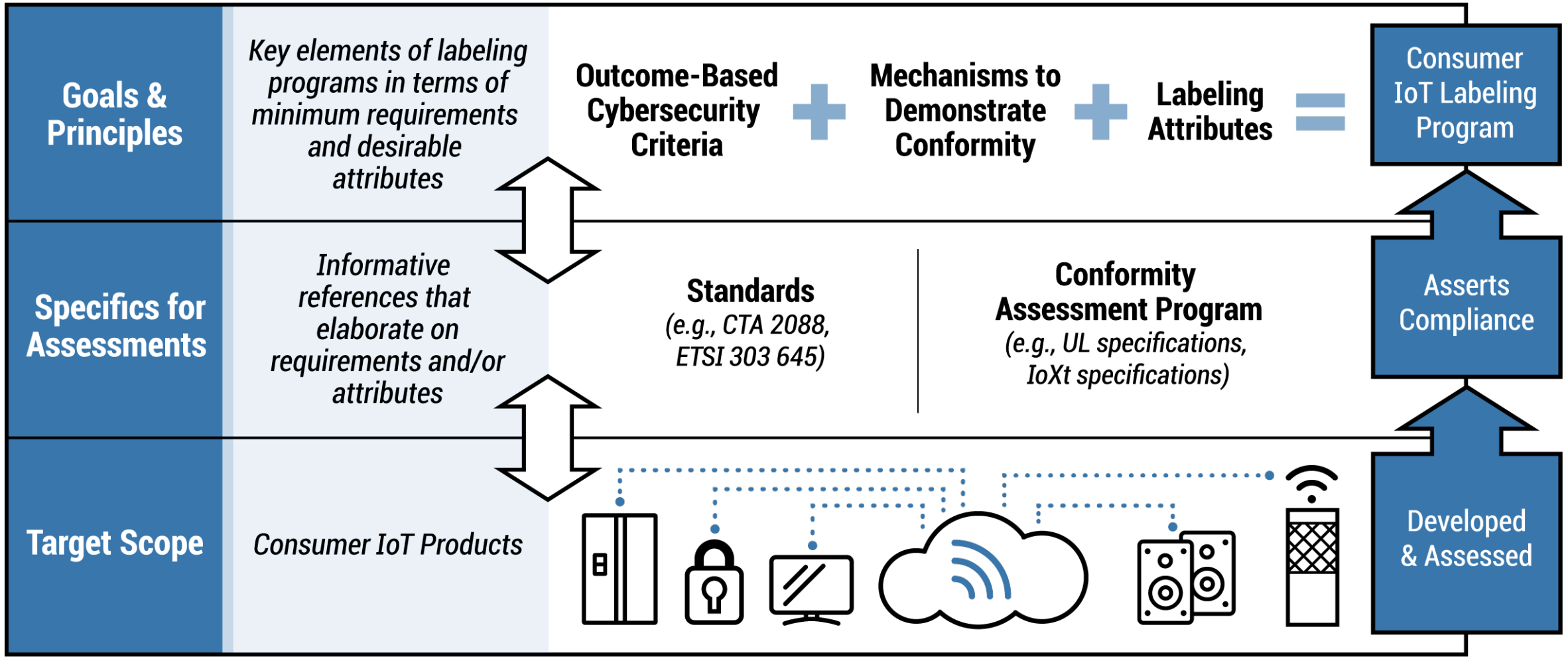
Labeling

- Binary Label (yes/no)
  - Visible before / at time of purchase
- Layered: More information available via scanned code or web link
- Accompanied by “robust” consumer education campaign

Conformity

- “Scheme Owner” determine structure and provides oversight
- Allow for multiple conformity approaches
- Range of conformity assessment activities could be applied

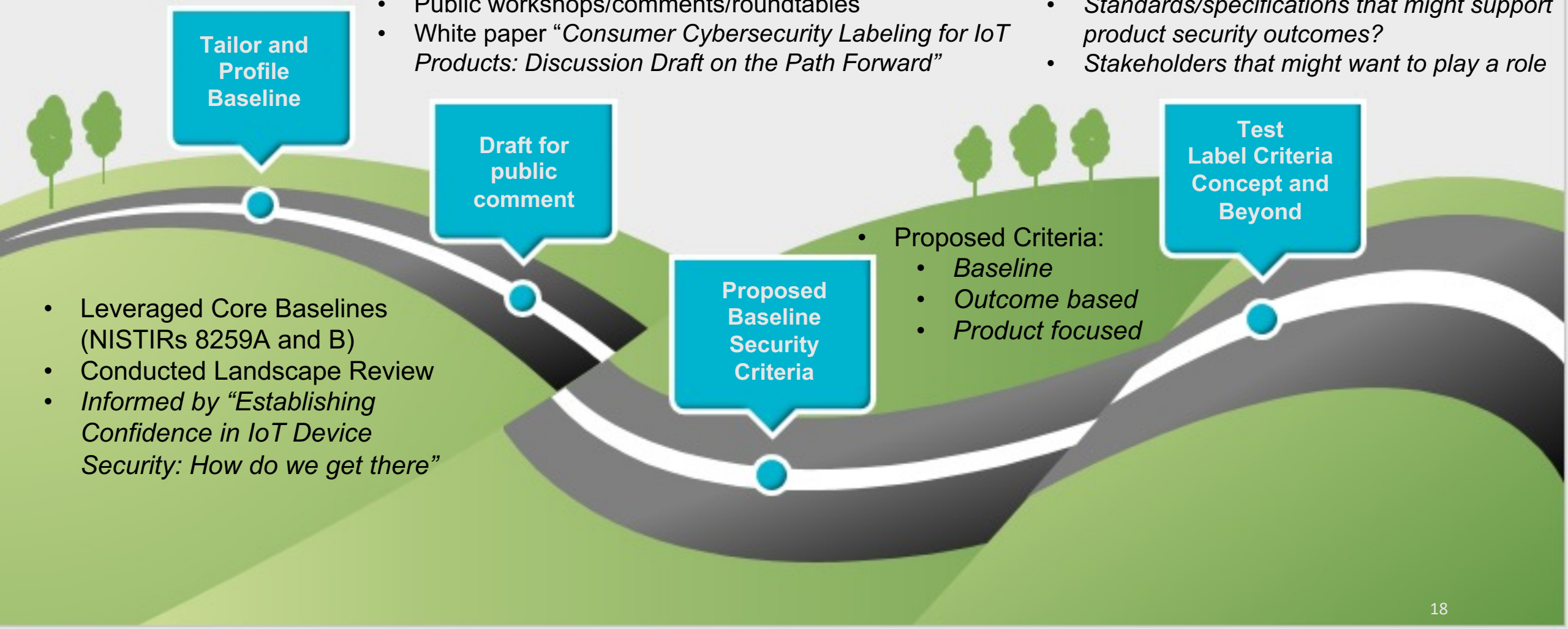
Desired outcome approach can allow for flexibility in how outcomes are achieved but requires governance



Results from piloted concept as well as observations will be summarized in summary report to WH

- About 20 responses under review
- Overall we have observed from the effort:
  - Support for product focus, however: recognition that will present some challenges in actual execution
  - Support for outcome-based, but recognition that it will require governance to ensure consistency
  - Varied responses with respect to the role of government, ranging from need to undertake public awareness, enforcement, incentives through potential liability protections and potential governance
  - Unclear whether the drivers are there to change market behavior through labeling

Roadmap to criteria for IoT product cybersecurity label



- Leveraged Core Baselines (NISTIRs 8259A and B)
- Conducted Landscape Review
- *Informed by "Establishing Confidence in IoT Device Security: How do we get there"*

- "*Draft Baseline Security Criteria for Consumer IoT Devices*"
- Public workshops/comments/roundtables
- White paper "*Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward*"

- Proposed Criteria:
  - *Baseline*
  - *Outcome based*
  - *Product focused*

- Test drive the criteria:
- *What are the existing programs that relate?*
- *Standards/specifications that might support product security outcomes?*
- *Stakeholders that might want to play a role*

Summary

- NIST is not a legislative or regulatory body
- Our work is informed and driven by market need and U.S. legislation
- What you know, is what we know
- NIST is proposing a baseline set of cybersecurity criteria for consumer IoT products
- NIST has made recommendations regarding the cybersecurity label and evaluation of conformance
- NIST will not be the scheme owner
- We recognize that some tailoring may be needed for specific use cases and risks, as the market determines
- The scheme owner(s) will be responsible for determining additional criteria and evaluating conformance
- NIST hosts the National Online Informative References Program (OLIR) which may be useful for comparing standards and criteria

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

@NISTcyber

labeling-eo@nist.gov

https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity
https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program