Consumer Technology Association™ CES®

Introduction to The U.S. National Cybersecurity Label Project

Mike Bergman

VP of Technology & Standards

Consumer Technology Association

mbergman@CTA.tech

standards@CTA.tech (information on joining)

CyberMockup™

NETFLIX
amazon
IBM
lyft
ALARM.COM
ANT GROUP
Meta
boingo
Microsoft
Disney+
BEST BUY
Ford
expedia group
airbnb
pandora
Google
in
verizon
SONY
gm
dailypay.

CTA at a Glance

Our mission: To help innovators of all sizes grow their business.

1500+
Member Companies

30+
Research Reports Free to Members Each Year

20+
Special Focus Divisions, Councils and Working Groups

130+
Standards including:

Airplane Mode, Closed Captioning, Accessibility Standards and more.

The U.S. effort to define a single national cybersecurity label for consumer connected devices was officially launched by the White House at a public-private "summit" on October 19 2022.

Deputy National Security Advisor Anne Neuberger convened a group of high-ranking government and private sector leaders. Summit attendees were agency chairs, famous brands' chief technology officers, test laboratory executives, trade association leadership, consumer advocates, academic researchers, a representative of the European Parliament and a U.S. Senator.

At the end of the day, Ms. Neuberger announced that the effort would go forward, under an architecture originally proposed by CTA and endorsed by the White House meeting participants. She further announced a Spring 2023 launch for the effort.

This introduction is based on slides originally presented by CTA at the White House summit meeting and is current as of Q1 2023.

CyberMockup™

The U.S. National Label Effort – the plan:

1. Create a single common U.S. label (mark).
2. Set criteria for use of the mark.
3. License existing industry label programs (3rd party and self-attestation) to issue the mark.
4. Promote & advertise domestically / Negotiate international for recognition

This is a voluntary program—not a regulatory requirement.

Stripped to its most basic elements, the program is a common mark endorsed by the U.S. government because it meets criteria set by NIST. In execution, we use the current ecosystem, because industry already knows how to certify product for food and product safety, manufacturing quality and more.

Once the program is established, it needs to be promoted domestically to consumers, to make them aware of the mark. And industry and the government need to work internationally to achieve mutual recognition of the U.S. mark so that manufacturers can use it in lieu of national requirements in allied nations.

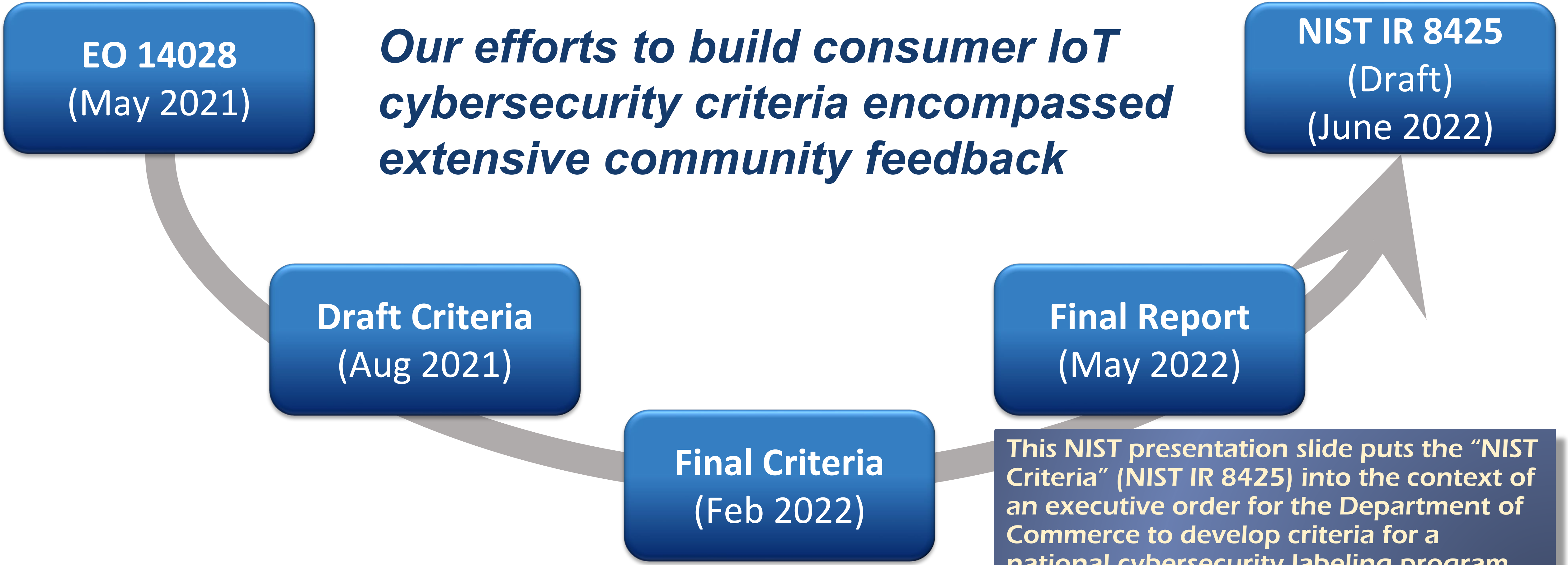
Some Background

(starting with two slides borrowed from NIST)

CyberMockup™

From the EO to NIST IR 8245 . . .

Our efforts to build consumer IoT cybersecurity criteria encompassed extensive community feedback



EO 14028
(May 2021)

Draft Criteria
(Aug 2021)

Final Criteria
(Feb 2022)

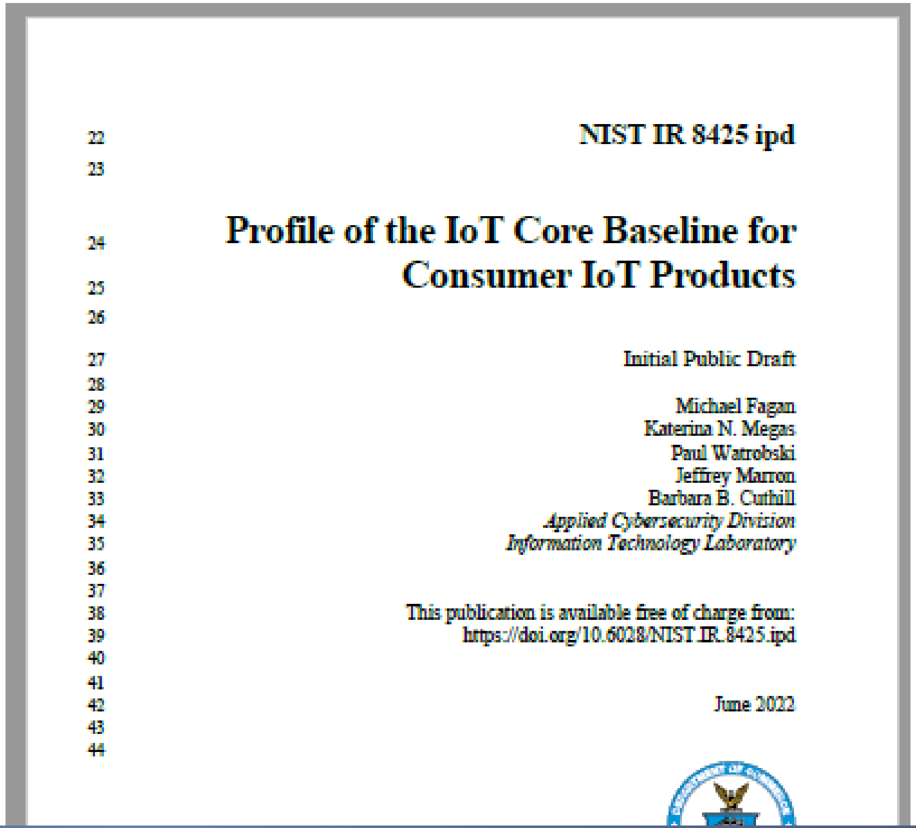
Final Report
(May 2022)

NIST IR 8425
(Draft)
(June 2022)

This NIST presentation slide puts the "NIST Criteria" (NIST IR 8425) into the context of an executive order for the Department of Commerce to develop criteria for a national cybersecurity labeling program for consumer connected devices.

The Consumer IoT Criteria Have Now Been Formalized in NIST IR 8425 (draft)

- Criteria are consistent with February 2022 cybersecurity white paper
  - Product-oriented
  - Outcome-focused
- Supporting information added
  - Criteria mapped to common vulnerabilities and known cybersecurity incidents
  - Supporting rationale from landscape review and stakeholder interactions
- Comments requested by July 31st
- Anticipate proceeding to final versi
  due to level of community support



NIST IR 8425 ipd

Profile of the IoT Core Baseline for Consumer IoT Products

Initial Public Draft

Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8425.ipd

June 2022

NIST IR 8425 ("NIST Criteria") is fundamental to the program. The program doesn't define a single scheme of labeling and requirements. Instead, it assesses labeling programs against these Criteria and authorizes the label scheme owner to issue the U.S. national mark. A label scheme can use an existing technical spec or define a new one, as long as the requirements meet the bar set by the NIST Criteria.

White House IoT Cybersecurity Strategic Workshop Oct. 19 2022

- Industry
  - Amazon
  - AT&T
  - Cisco
  - Google
  - LG Electronics
  - Intel
  - Samsung
  - Sony
  - UL

- Associations
  - ANSI
  - Consumer Technology Association (CTA)
  - CSA/Matter/ZigBee
  - CTIA
  - IoXT
  - National Retail Federation

- Other Private Sector
  - Carnegie-Mellon Univ.
  - Consumer Reports
  - R Street

- Government
  - CPSC
  - DHS CISA
  - FCC
  - FTC
  - NIST
  - NSC
  - ONCD
  - OSTP
  - Sen. Angus King
  - European Commission

This summit meeting established the "plan of record". The White House provided a Strawman summary. This Strawman is an excellent two-page overview and is available on the CTA National Label website.

Key elements in the Strawman are:
(1) A mark/label; (2) Conformity requirements; (3) Determination & attestation criteria; (4) A registry of certified products; (5) Encouragement & enforcement of adoption

The U.S. National Label Program

Examples of Existing Schemes:
IoT Cybersecurity Label Programs

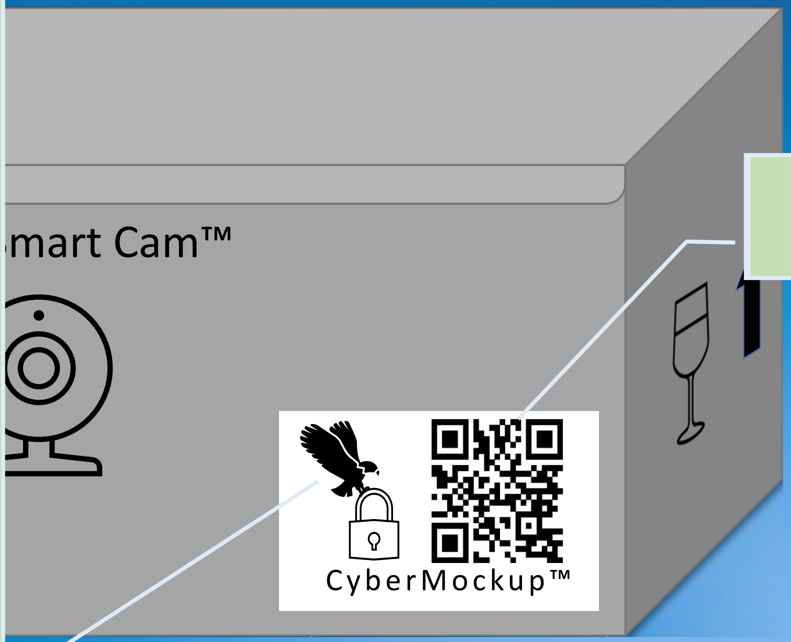
- *Consumer-facing*: IoXT, UL, & others
- *B2B:* CTIA, Google, & others
- *As program requirement:* Apple, Comcast, Samsung, & others
- *Emerging/various:* CSA, GSMA, & others

The global ecosystem has been testing, certifying and accrediting products and organizations for decades. Food, health, safety, manufacturing, systems engineering, and more have such experience. In consumer technology safety and emissions certifications are common on products.

The entities that support the global certification and accreditation of consumer technology and companies are already providing the same kind of programs for cybersecurity.

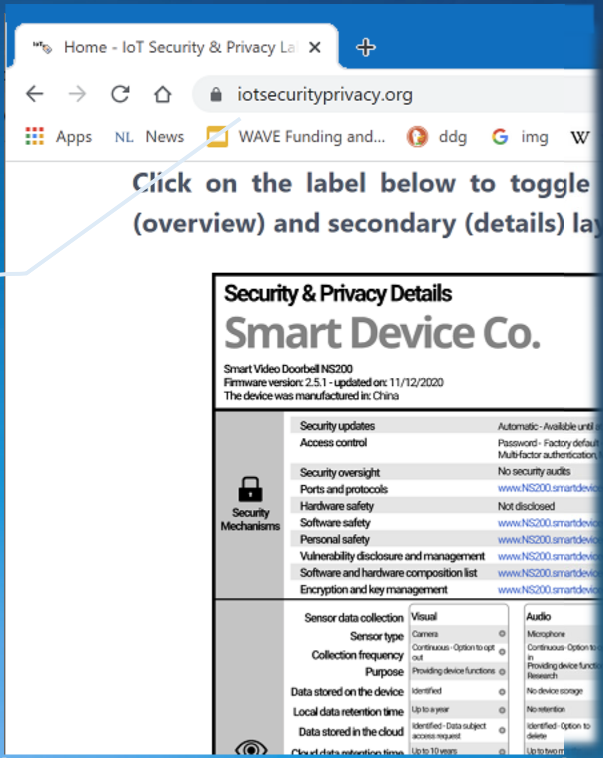
Label, Binary & Layered

- Limited on-package "footprint" to allow for small products
- Comprehensive online info available from link
- Trademarked element enables legal protections
- Follows industry practice for safety or compliance "certification" marks



Trademarked element

On-package label



Click on the label below to toggle (overview) and secondary (details) lay

Security & Privacy Details

Smart Device Co.

Smart Video Doorbell NS200
Firmware version: 2.5.1 - updated on: 11/12/2020
The device was manufactured in: China

Security Mechanisms	Security updates	Automatic - Available until a
	Access control	Password - Factory default Multi-factor authentication,
	Security oversight	No security audits
	Ports and protocols	www.NS200.smartdevic
	Hardware safety	Not disclosed
	Software safety	www.NS200.smartdevic
	Personal safety	www.NS200.smartdevic
	Vulnerability disclosure and management	www.NS200.smartdevic
	Software and hardware composition list	www.NS200.smartdevic
	Encryption and key management	www.NS200.smartdevic

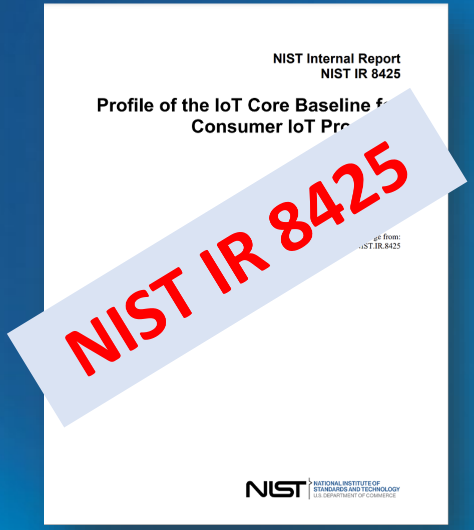
Sensor data collection	Visual	Audio
Sensor type	Camera	Microphone
Collection frequency	Continuous - Option to opt out	Continuous - Option to o in
Purpose	Providing device functions	Providing device functio Research
Data stored on the device	Identified	No device storage
Local data retention time	Up to a year	No retention
Data stored in the cloud	Identified - Data subject access request	Identified - Option to delete
Cloud data retention time	Up to 10 years	Up to two m

Online details:
1) Landing page is consumer-friendly
2) Secondary page is more technical

On a product box, the label will have a trademark portion and a digital link portion. The trademark shown here is a mock-up.

Components

Criteria



NIST Internal Report
NIST IR 8425

Profile of the IoT Core Baseline f
Consumer IoT Pro

e from:
IST.IR.8425

NIST IR 8425

A label "scheme" is the requirements, technical and non-technical, how the organization performs test and conformity assessment, and other aspects of the program. Existing scheme owners are shown here, along with some of the specs they use.

Evaluates

Schemes

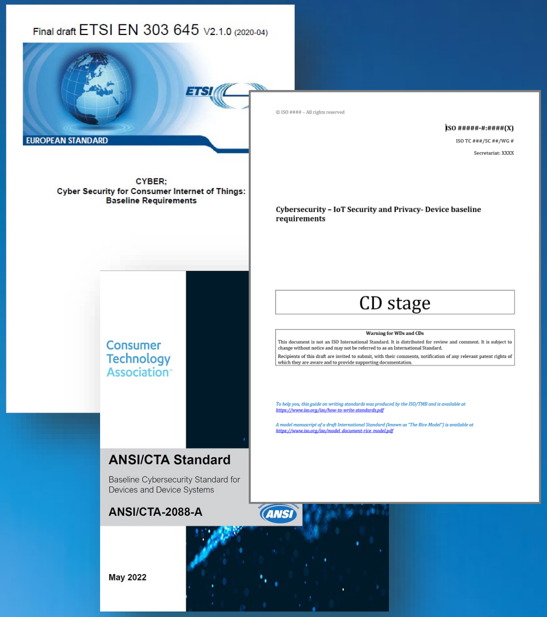
- Apple
- Comcast
- CSA*
- Eurofins
- Google
- GSMA*
- IoXT
- Samsung
- UL
- Wi-Fi Alliance
- ..others

** In process*

The **definition** of a label program

Are part of

Standards



Final draft ETSI EN 303 645 V2.1.0 (2020-04)

EUROPEAN STANDARD

CYBER;
Cyber Security for Consumer Internet of Things:
Baseline Requirements

Consumer Technology Association

ANSI/CTA Standard

Baseline Cybersecurity Standard for Devices and Device Systems

ANSI/CTA-2088-A

May 2022

© ISO #### – All rights reserved

ISO #####-#:####(X)
ISO TC ###/SC ##/WG #
Secretariat: XXXX

Cybersecurity – IoT Security and Privacy- Device baseline requirements

CD stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

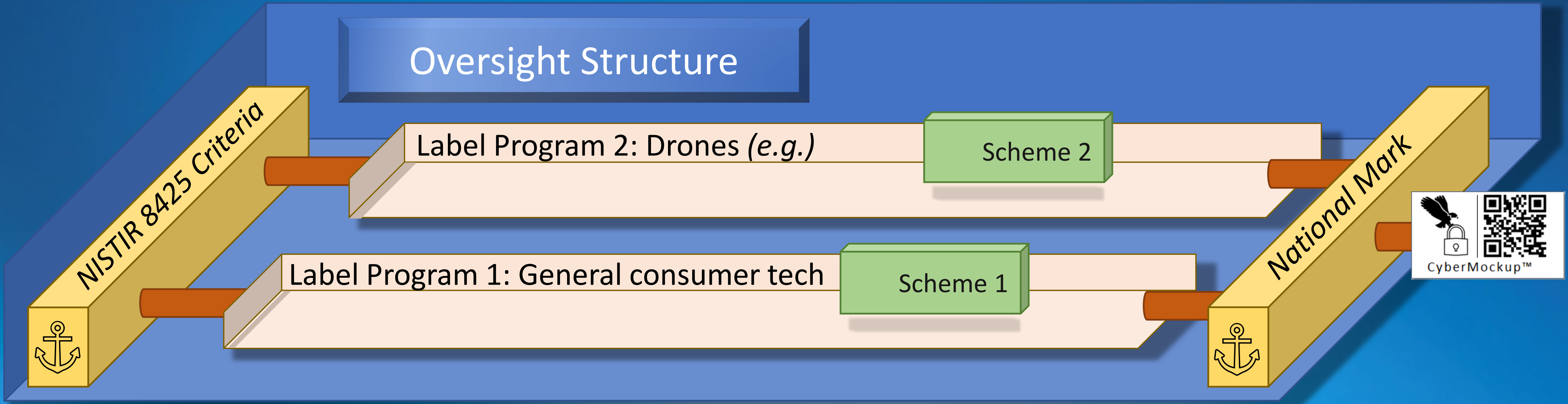
Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

To help you, this guide on writing standards was produced by the ISO/TMB and is available at https://www.iso.org/iso/how-to-write-standards.pdf

A model manuscript of a draft International Standard (known as "The Rice Model") is available at https://www.iso.org/iso/model_document-rice_model.pdf

The **requirements** referenced by a scheme

Cybersecurity Labels At Scale



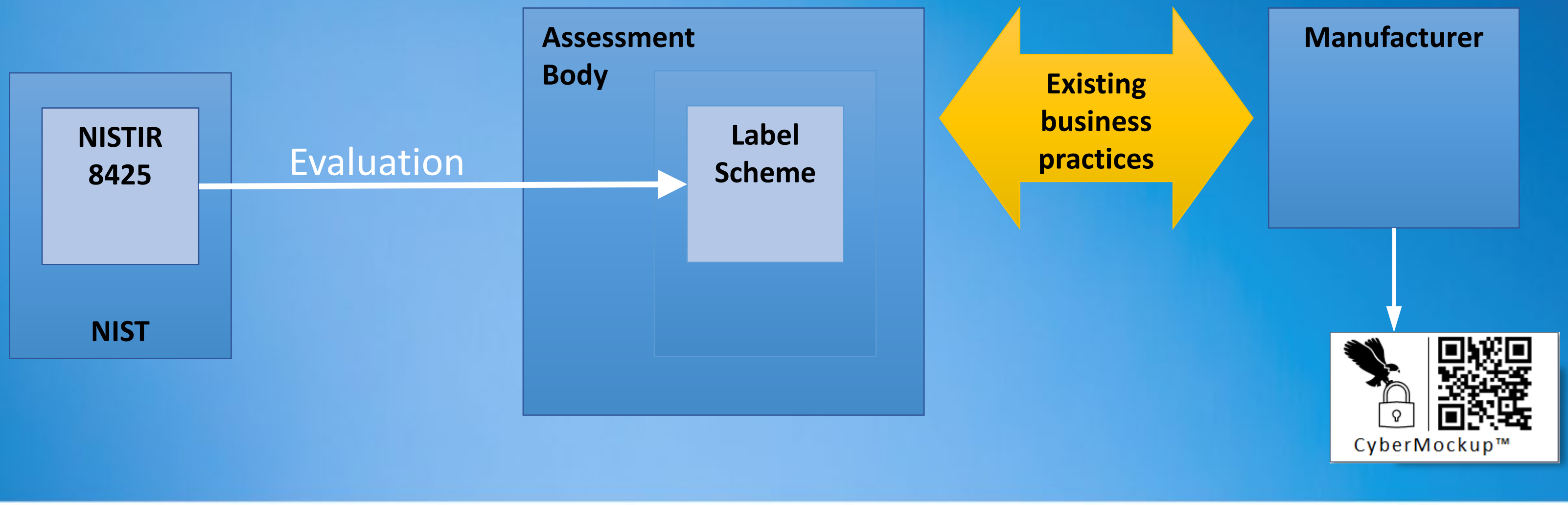
"Scale" is critical because the IoT is huge. We anchor the program with the NIST Criteria and with a common national mark. Multiple schemes for different purposes can be authorized. This slide shows one scheme for general consumer tech and one for drones.

The NIST Criteria are for consumer product. A different Criteria—for e.g. enterprise—can be added to extend the program.

Ensuring Trust At Scale: Common Structure

- Use NIST Criteria to evaluate Schemes before licensing them to offer the mark
- License assessment bodies & authorize Schemes
- License manufacturers for Self-Attestation
- Enforce appropriate label usage via trademark law

Trust mechanisms are critical to a successful program, because the public sector sponsors—the government—must be able to trust the program. Use of existing accreditation and assessment programs provides effective solutions.



Status: U.S. Phase 1

Key:

🟥	In progress
🟨	In progress
🟩	Completed

	Criteria	Evaluation	Schemes (3rd-Party)	Schemes (SA)
Technical Requirements	🟩 **NIST:** NISTIR 8425 🟨 *Maintain*	🟨 **CTA:** (Draft) CTA-2119 "Framework" via CTA R14 WG6*	🟩 *(open, would be e.g. UL / CSA / IoXT / Intertek / Eurofins)* 🟨 *Address gaps*	🟥 *(open, potentially move to Phase 2)*
Non-Technical Requirements				
Conformity Assessment Requirements	🟥 *(open, current under study in CTA ad-hoc)*	🟥 *(open, current under study in CTA ad-hoc)*		
Label Requirements	🟨 **NIST:** White paper 2/22; stakeholder consensus	🟨 **CTA:** (Draft) CTA-2120 "Label Specification" vis CTA R14-WG7*	🟨 *(requires Scheme owner to adopt label)*	🟨 *(requires Scheme owner to adopt label)*
National Product Registry	🟨 Developing requirements specification	🟨 *(open, early discussion)*	🟨 *(open, early discussion)*	🟨 *(open, early discussion)*

** How to participate: Email standards@CTA.tech*

NIST “Gestalt” product concept

The NIST Criteria asserts that the entire IoT product must be compliant, including anything required for full capability, including hardware but also smartphone apps, cloud services, hubs, etc.

- Possible paths

  A. Each product component ***independently*** meets 8425
     Example: Smart Phone app must meet 8425

  This is not recommended.

  B. The product components ***in combination*** meet 8425 as a whole
     Example: Smart phone app gets Device ID from hardware

  C. We substitute another category certification for 8425 (e.g. for cloud services)
     Example: Cloud Security Alliance trust mark

Consumer Technology Association™

CES®

For further information:

Michael Bergman
mbergman@CTA.tech

Participation:
standards@CTA.tech