Telecom MRAs -

Recent US Developments on Cybersecurity

March 10, 2022

Ramona Saar

National Institute of Standards and Technology (NIST)

Department of Commerce

United States

- US TEL MRA Participation
- Scope of MRAs and Addition of Cybersecurity
- Recent US Developments on Cybersecurity
- Voluntary Consumer IoT Product Labeling Criteria

US TEL MRA Partners

APEC TEL MRA

Australia
Canada
Chinese Taipei
Hong Kong
Korea
Malaysia
New Zealand
Singapore
Vietnam

BILATERAL MRAs

Israel
Japan
Mexico
European Union
UK

United States **FCC** - Equipment Authorization Procedures
47 CFR

1. **Supplier's Declaration of Conformity** (SDoC)

2. **Certification**

Requires use of FCC Recognized Test Labs

Requires use of FCC Recognized Telecommunications Certification Bodies

Resource: https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization

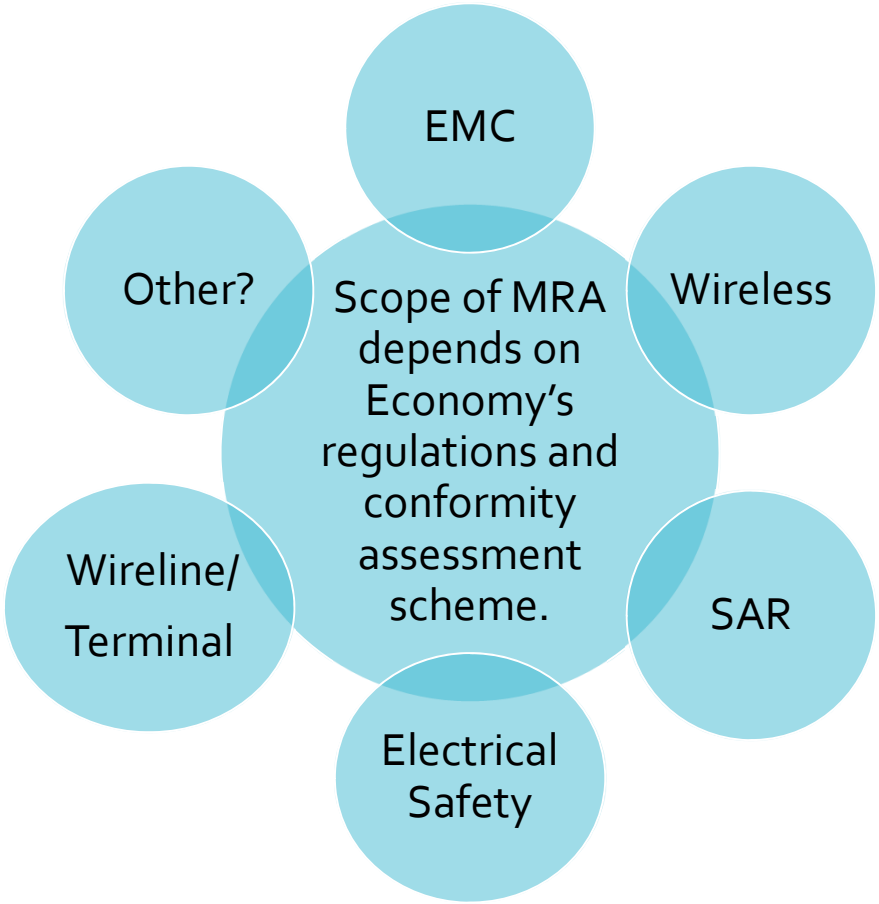
United States **NIST** Designating Authority - Role

1. Designate **US CABs to MRA Partner Telecom Regulators** for recognition

2. Designate **US TCBs to the FCC** for recognition

Resource: https://www.nist.gov/mutual-recognition-agreements-mras

Scope of TEL MRAs Has Changed Based on Technology and Regulations



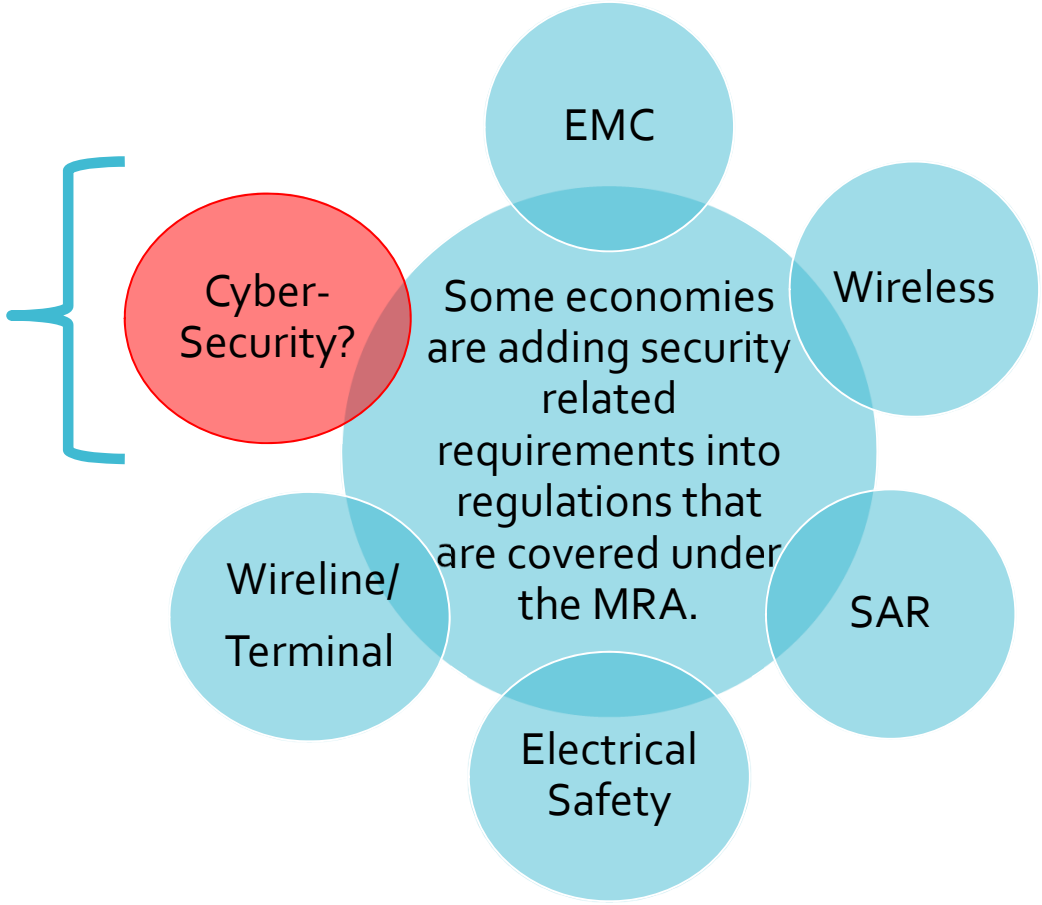
Each regulator determines the elements included in their regulations and covered in the MRA.

Recent Development: Introduction of Cybersecurity Requirements

Japan

EU

Others?



CABs must demonstrate competency in the cybersecurity conformity assessment activities to participate in the relevant MRA Partner regulatory schemes.

Each regulator determines the elements included in their regulations and covered in the MRA.

Recent Radio/IoT Device **Cybersecurity** Developments
United States – FCC

Publication of FCC 21-73 **Notice of Proposed Rule Making** (NPRM) and **Notice of Inquiry (NOI)** on 08/19/2021

NPRM: Proposes specific changes to equipment authorization procedures

NOI: Request for public comments on how the FCC's equipment authorization program could be used to improve the cybersecurity of devices through appropriate standards and guidelines.

The comment period and the FCC reply comment period on FCC 21-73 have closed.

The FCC is reviewing the comments and determining how to proceed.

Recent Radio/IoT Device **Cybersecurity** Developments
United States – **White House Executive Order (EO)**

Publication of White House Executive Order 14028 on *Improving the Nation's Cybersecurity* on 05/12/2021

Section 4 of the EO assigned specific tasks for NIST regarding development of cybersecurity labeling criteria for :

Consumer IoT Devices

Consumer Software

Time Given: One year

US Executive Order 14028 - Consumer IoT Product Labeling Criteria

Current Status

Internet of Things (IoT) devices **often lack device cybersecurity capabilities their customers**—organizations and individuals—can use to help mitigate their cybersecurity risks.

Source: NISTIR 8259

Label Goals:

Incentivize manufacturers to **voluntarily** improve the cybersecurity of their IoT products.

Educate consumers and **raise their awareness** about cybersecurity issues.

Recommended Criteria Has Been **Published**

In 2021, NIST held public workshops, received stakeholder input to develop recommended criteria.

On February 4, 2022, NIST published ***Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products*** (NIST White Paper)

- See Consumer IoT Product Criteria

Note: NIST has also published Recommended Criteria for Cybersecurity Labeling of Consumer Software. While this is not being covered here, this is another important document.

About the Criteria

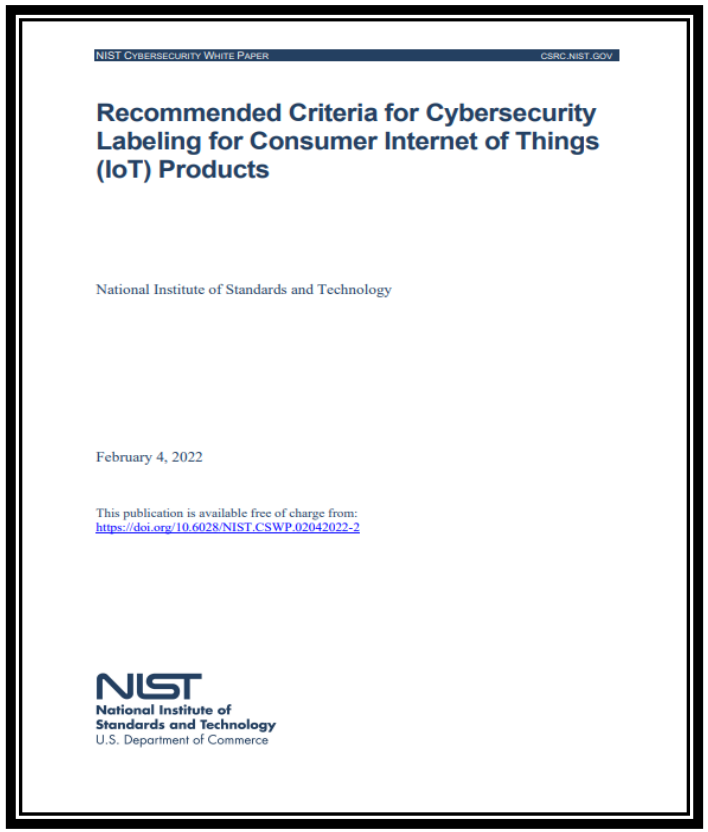
These are baseline (minimum) technical and non-technical criteria for **voluntary Consumer IoT Product** cybersecurity labeling.

The criteria is for **scheme owners to use** as part of their own labeling programs.

NIST is not establishing its own labeling program and NIST is not designing a label.

The criteria is expressed in terms of **desired outcomes** and not in terms of specific technical standards/conformity assessment approaches.

Technical approaches are to be determined by the **scheme owner** based on **product type** and functionality, and available technical standards.



Key Recommendations

Scope

Technical Label Criteria

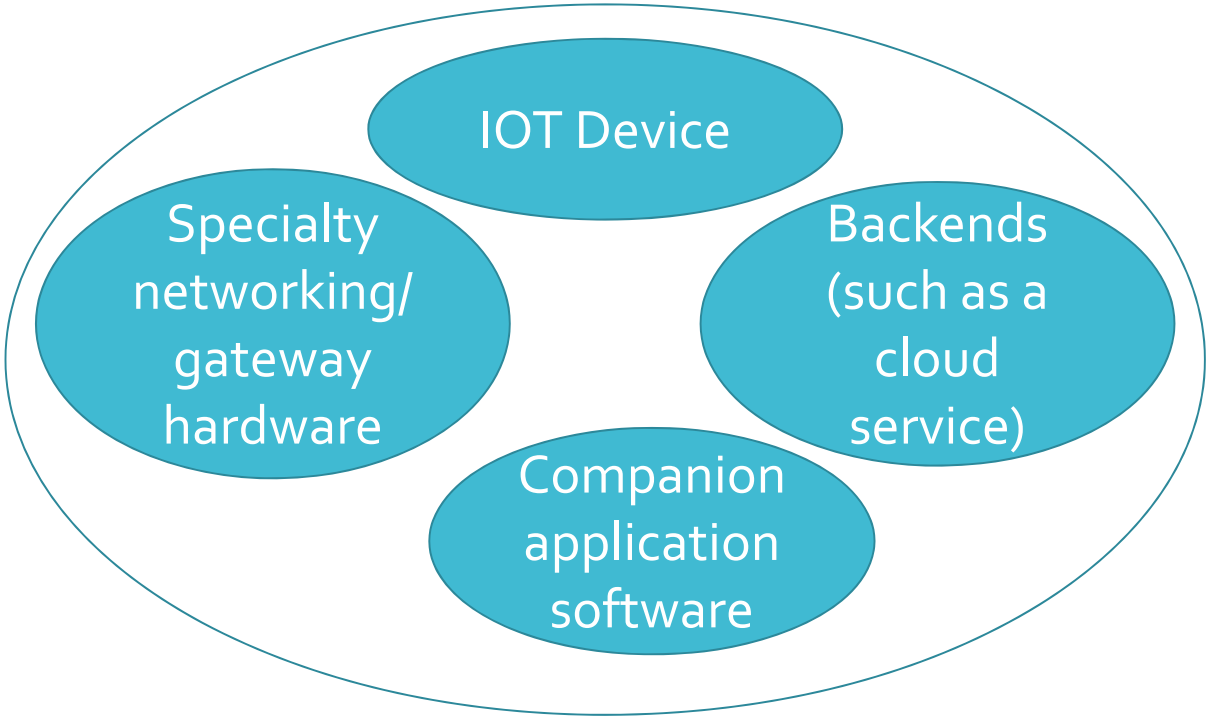
Non-Technical Label Criteria

Label Type

Consumer Education

Many more details and considerations are included in the document.

Scope of Recommended Labeling Criteria: **Entire Consumer IoT Product**



NIST White Paper: The IoT Device's components have access to the IoT device and the data it creates and uses – making these components potential attack vectors that could impact the IoT device, customer, and others…. Since these ***additional components can introduce new or unique risks to the IoT product, the entire IoT product, including auxiliary components, must be securable****.*

Recommended Baseline (Minimum) **Technical Criteria** for a Label

Technical (6)

- Asset Identification
- Product Configuration
- Data Protection
- Interface Access Control
- Software Update
- Cybersecurity State Awareness

See also NISTIR 8529A - https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf

Recommended Baseline (Minimum) **Non-Technical Criteria** for a Label

Non-Technical (4)

- Documentation
- Information and Query Reception
- Information Dissemination
- Product Education and Awareness

- See also NISTIR 8259B: https://csrc.nist.gov/publications/detail/nistir/8259b/final

Recommended **Label Type**

NIST Recommends a Binary Label

- This means a single label indicating a product has met a baseline standard.
    - *The product either has the label or it does not.*
- Provide additional information through a URL or QR code
- Support physical and digital formats

Usable to General Consumers

- The label should be usable for the general consumer population that does not have expertise in cybersecurity and may not be able to judge the technical merit of the label criteria.

Recommended **Consumer Education Efforts**

NIST recommends that label scheme owners include a strong **consumer education campaign.**

- Establish and increase label recognition
- Provide transparency to consumers about important aspects of the program
- Ensure a common way for IoT product stakeholders to talk about the labels

Scheme owners should also ensure that consumers have **online access to key details about the labeling scheme**, including details such as what the label signifies and what it does not signify, for example.

.

Next (Current) Step: **Pilot Phase**

NIST is now seeking stakeholder input on questions such as:

- Are there any existing labeling schemes that address some or all the criteria?
- Are there organizations interested in setting up a new programs based on the criteria?
- What are potential incentives for a consumer IoT Product labeling scheme based on the criteria?

Interested parties should send comments to labeling-eo@nist.gov by **March 15, 2022.**

Resource: *https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots-approach*

Final Step: Publication of a NIST **Summary Report**

To conclude the tasks assigned in the EO, NIST must prepare and issue a **summary report** by May 12, 2022, taking into consideration information obtained during the pilot phase.

Publication of the summary report will then complete the actions requested in the EO.

Any further actions related to this effort have not yet been defined or determined.

[*For example, there is no indication or request for the initiation of **mandatory** consumer IoT product or consumer software labeling programs.]*

Review of Topics Covered Today

Some MRA Partner regulators are including **cybersecurity** in regulations covered under MRAs. CABs must demonstrate **competence** for relevant cybersecurity conformity assessment activities.

The current scope of the FCC's equipment authorization program does not include cybersecurity. The FCC has issued an **NOI** to determine if/how the program might be used to help improve cybersecurity of devices. The FCC is reviewing stakeholder comments in order to determine how to proceed.

The USG (NIST) has developed recommended cybersecurity labeling criteria for **Consumer IoT Products** and **Consumer Software**. It is hoped that scheme owners will adopt this criteria and begin to offer **voluntary** labeling programs to (1) incentivize **improvements in cybersecurity** and (2) raise consumers**' awareness** of cybersecurity issues.

Thank you for your attention.

Questions:
mra@nist.gov

Contact:
Ramona.saar@nist.gov