IoT Cybersecurity Labels:

Lessons Learned When Applying Human-Centered Research to Practice

Julie Haney

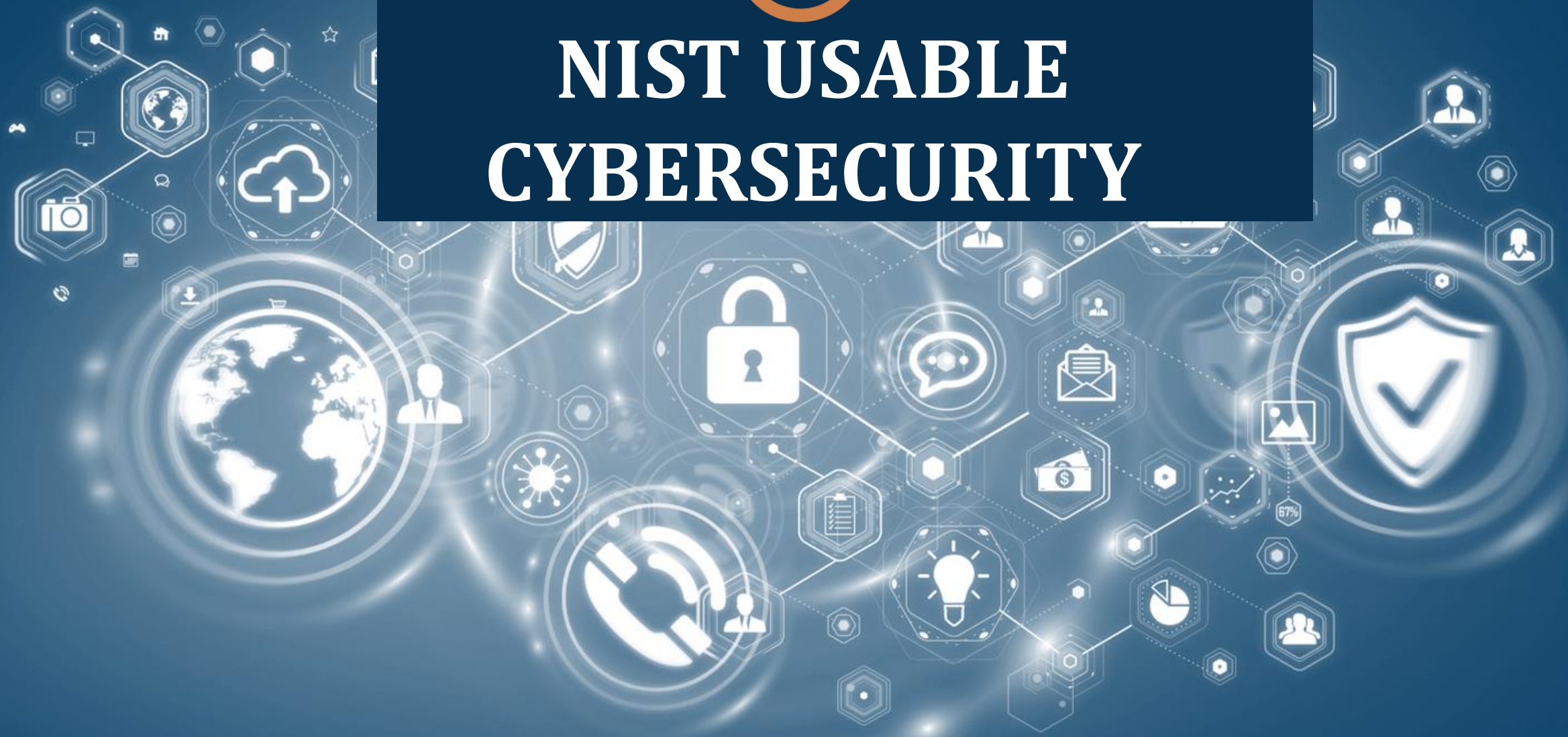
May 23, 2023

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

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products mentioned are necessarily the best available for the purpose.

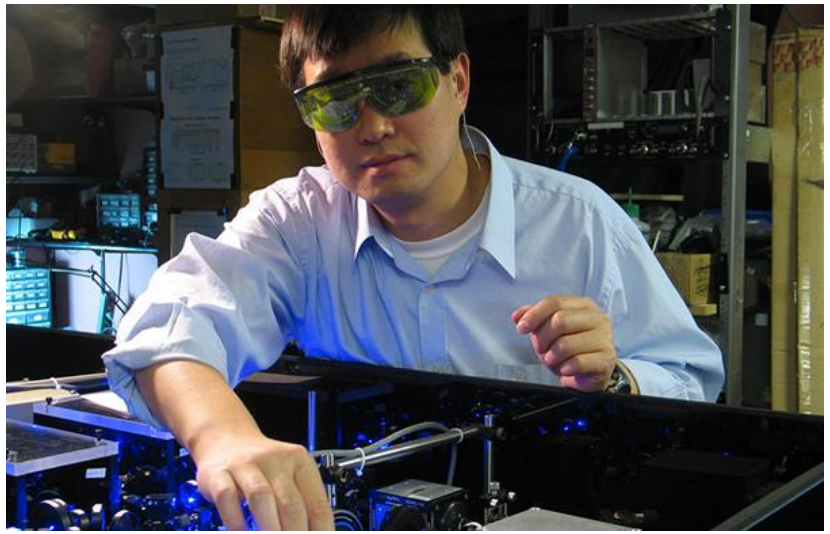
NIST USABLE CYBERSECURITY



NIST Mission

- **NIST:** 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

- **Information Technology Lab:** To cultivate trust in IT and metrology.



NIST Usable Cybersecurity

Championing the Human in Cybersecurity

- Conduct research and other human-centered projects at the intersection of cybersecurity and human factors
- Provide actionable guidance so that the human element can be considered in cybersecurity decisions, processes, and products

Projects

Past Efforts

- Authentication
- Security & privacy perceptions
- Cryptographic development
- Cybersecurity advocacy

Recent Efforts

- Youth security & privacy
- Phishing
- Security awareness & training
- Smart home security & privacy

Smart Home Research

- Interview study
  - *"It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security* – USENIX Security Symposium 2021
  - *Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges* – International Conference on Human-Computer Interaction 2020

- Smart home updates survey
  - *User Perceptions and Experiences with Smart Home Updates* - IEEE Symposium on Security & Privacy 2023
  - *Smart Home Device Loss of Support: Consumer Perspectives and Preferences* - International Conference on Human-Computer Interaction 2023 (to appear)

LABELING EXECUTIVE ORDER

Executive Order 14028:

Improving the Nation's Cybersecurity (May 12, 2021)

NIST was directed to:

"initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of internet-of-Things (IoT) devices and software development practices, and shall consider ways to incentivize manufacturers and developers to participate in these programs."

Executive Order 14028

- "identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products."

- "examine all relevant information, labeling, and incentive programs and employ best practices. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation."

Consumer Goals

Aid consumers in IoT purchases

Enable comparisons among products and educate consumers about IoT cybersecurity considerations

Engender consumer trust/confidence

Encourage IoT product developers to consider ways to achieve consumer confidence & facilitate management of cybersecurity risks

Label Criteria

BASELINE PRODUCT CRITERIA

Technical and non-technical security requirements for the IoT product

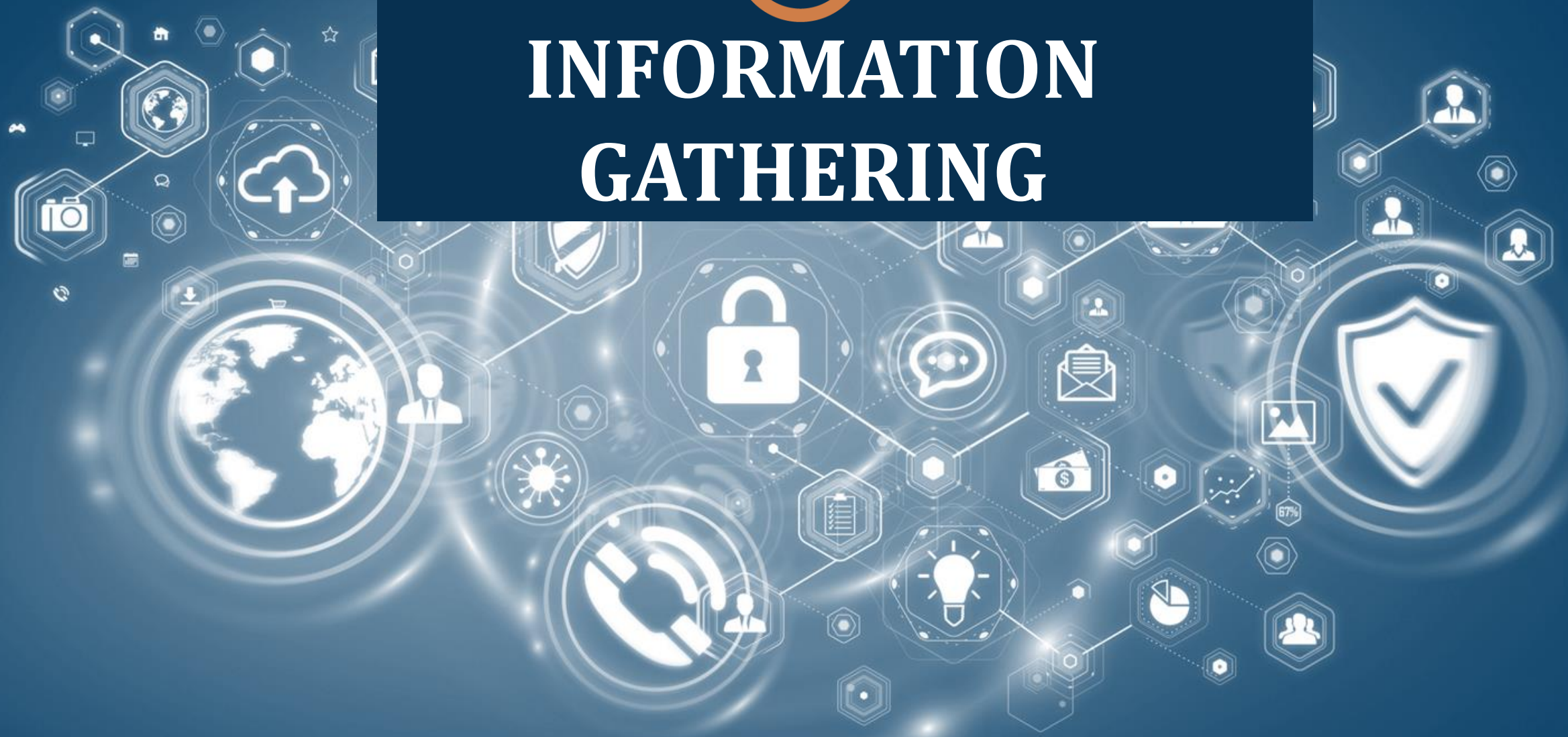
CONFORMITY ASSESSMENT

Means of demonstrating that specified requirements are fulfilled

LABEL CONSIDERATIONS

Label approach, label presentation, consumer education, consumer testing

INFORMATION GATHERING



Sources

In formulating consumer label considerations, NIST synthesized feedback and information from government, academia, industry, and non-profit sources.

WORKSHOPS

Position papers and input obtained during two NIST workshops on Cybersecurity Labeling Program for Consumers (Sep. & Dec. 2021)

PUBLIC COMMENTS

Comments on two draft documents on cybersecurity labeling for IoT products (Aug. & Dec. 2021)

MEETINGS

Information, questions, concerns from meetings with other government labeling programs, researchers, and private and non-profit groups

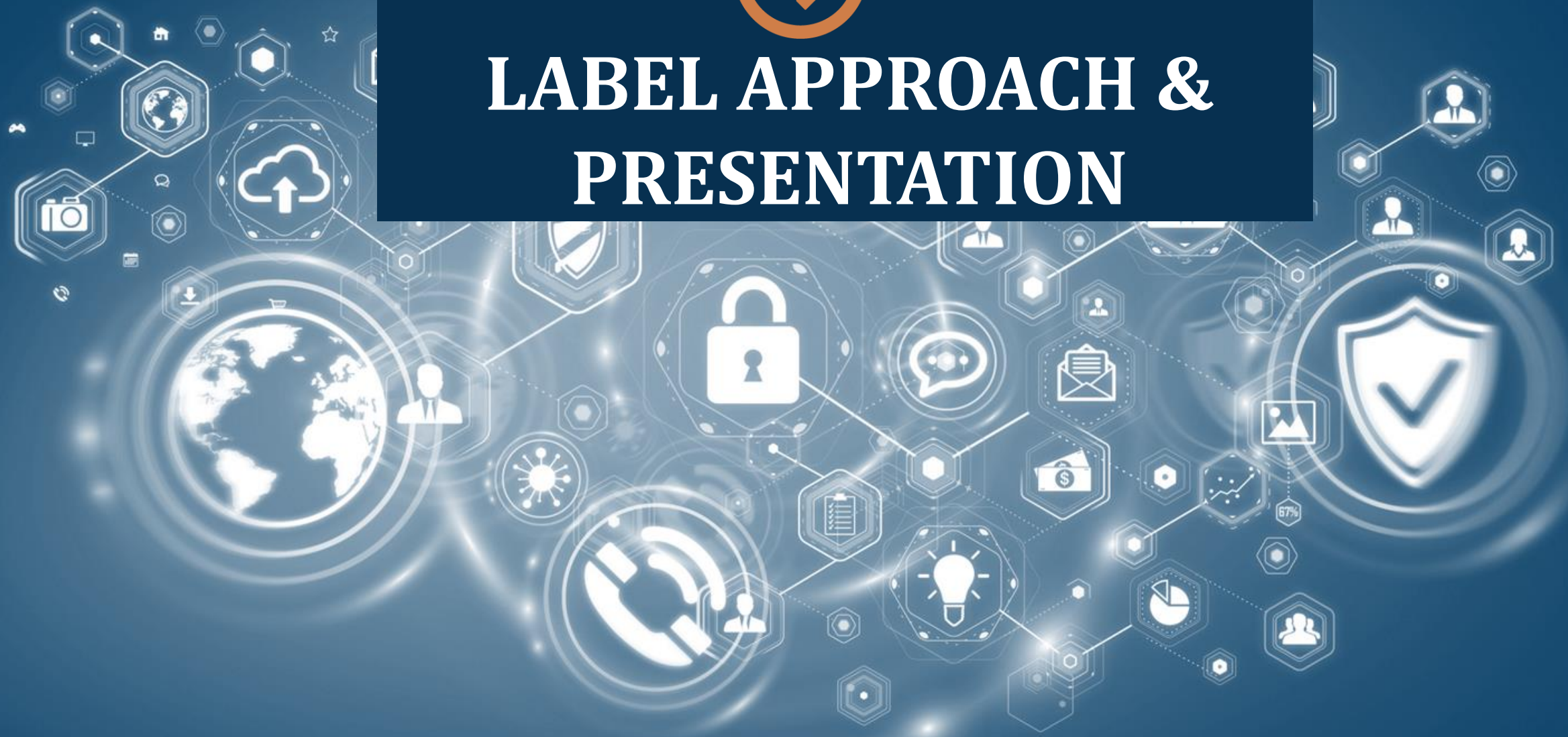
RESEARCH

Prior research about labels in both security and non-security domains

Labeling Feedback

1. Conveying cybersecurity information to diverse consumers will be challenging.
2. Consumers may have difficulty determining appropriate risk levels.
3. A robust consumer education program should accompany the label.
4. Consumer testing to assess usability and impact of the label is critical.
5. The label format should be flexible to reflect changing security & label status.
6. Retailers and third-party service providers will play an important role.

LABEL APPROACH & PRESENTATION



Guiding Principles for Label Considerations

Appropriate to technical criteria

Usable by diverse range of consumers

Label Types

https://www.fda.gov

Descriptive

Provides facts about product properties or features without any grading or evaluation

https://www.energystar.gov

Binary

Single label indicating a product has met a baseline standard

https://www.nhtsa.gov/ratings

Graded/Tiered

Indicates the degree to which a product has satisfied a standard, sometimes based on attaining increasing levels of criteria

Layered

Primary label leads consumers to additional details online

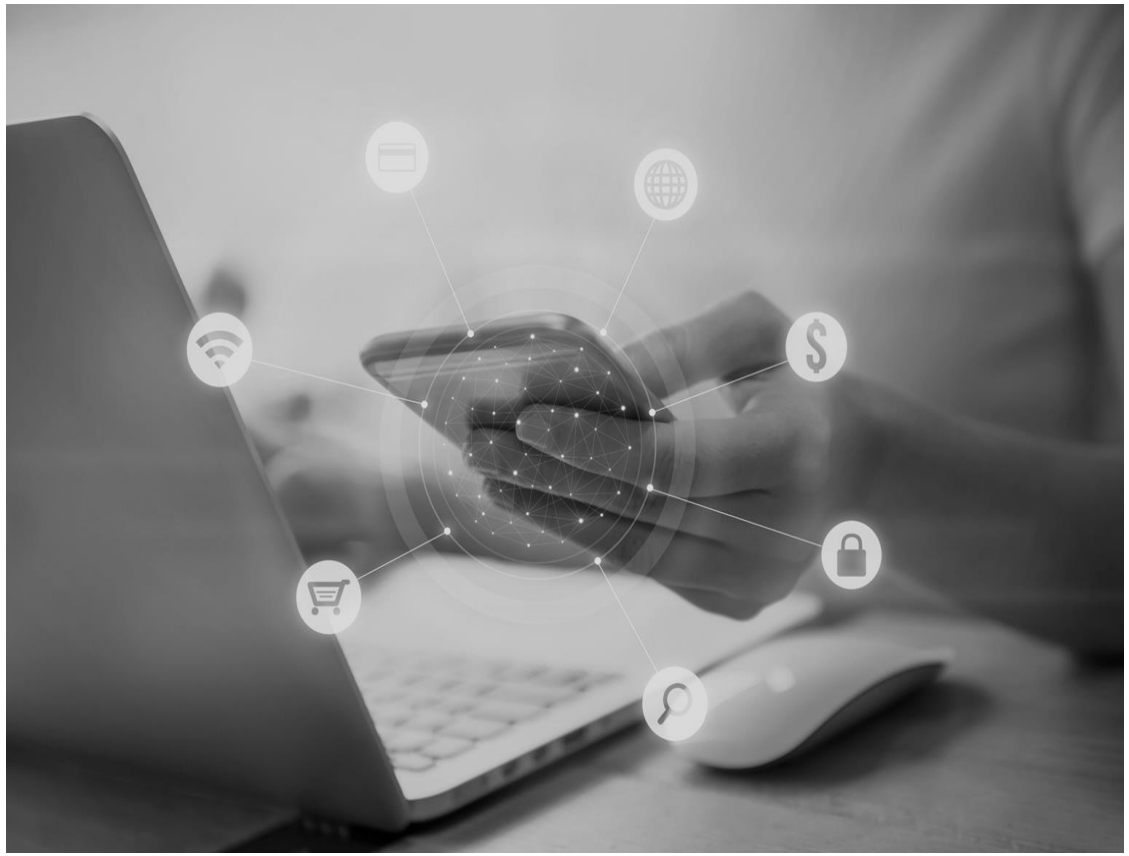
LABEL APPROACH

BINARY LABEL

Reflects conformity with a baseline, usable, simple. Effective in situations in which consumers may lack time, expertise, desire to be presented with more information

LAYERED APPROACH

Aids in consumer education and helps satisfy information needs of wide range of consumers. Provides means to access product's declaration of conformity, enables comparison to other labeling schemes



Label Presentation

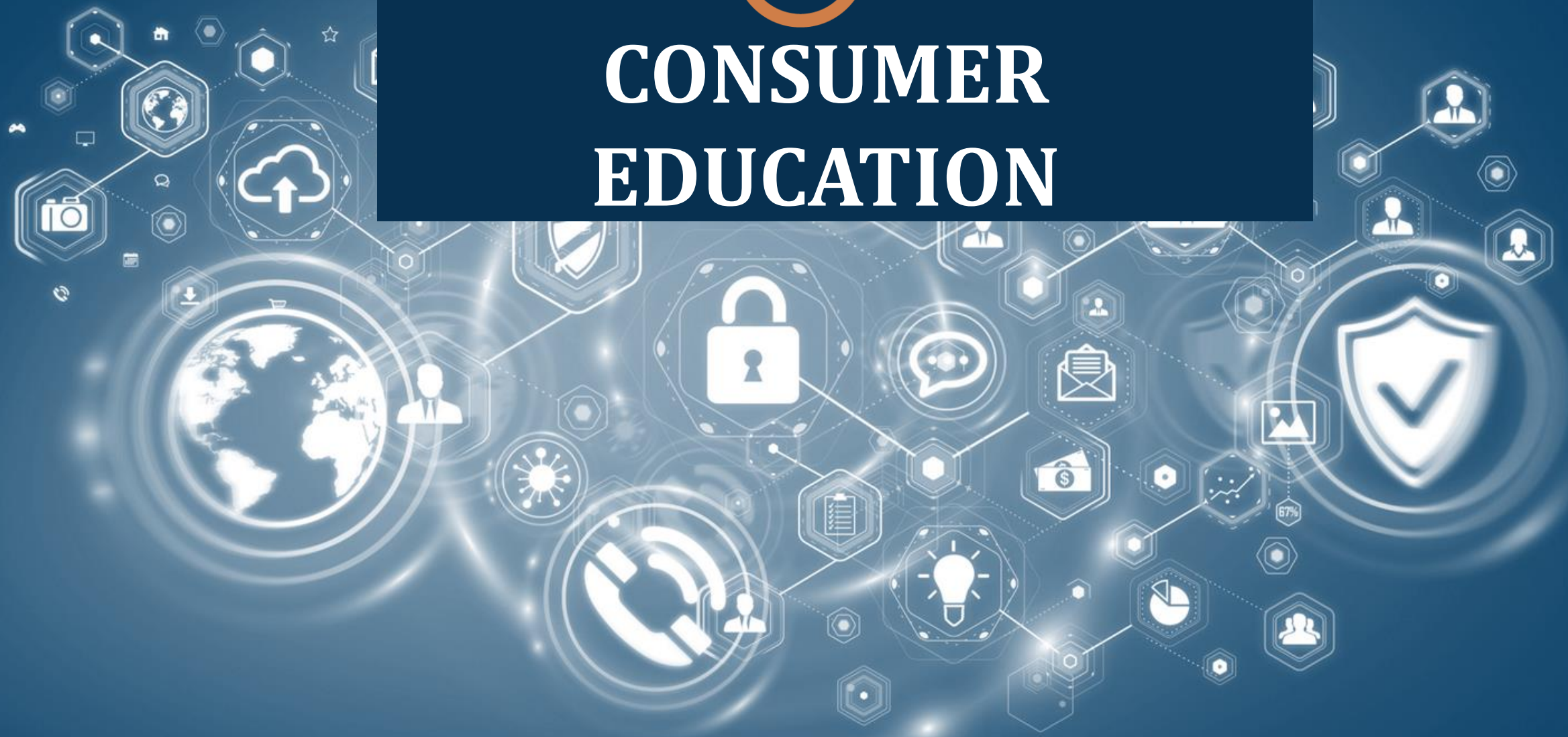
AVAILABLE DURING & AFTER PURCHASE

Allow for flexible formats - physical & digital (e-labels).

MARKETPLACE PRESENTATION

Retailers should be engaged as active partners in label delivery. Framing is important.

CONSUMER EDUCATION



Education Purpose

Increase label recognition and provide transparency to consumers about important aspects of the labeling program

SUPPORT DIVERSE CONSUMERS

Understandable language, accessible, support experts and non-experts

ADDRESS POTENTIAL MISCONCEPTIONS

Information to counter dichotomous thinking (labeled="good", unlabeled="bad"), halo effect (false sense of security)

1. Intent and scope – what label means/does not mean, eligible products

2. Product criteria – baseline properties, why/how these were selected

3. Conformity assessment – general information & declaration of conformity

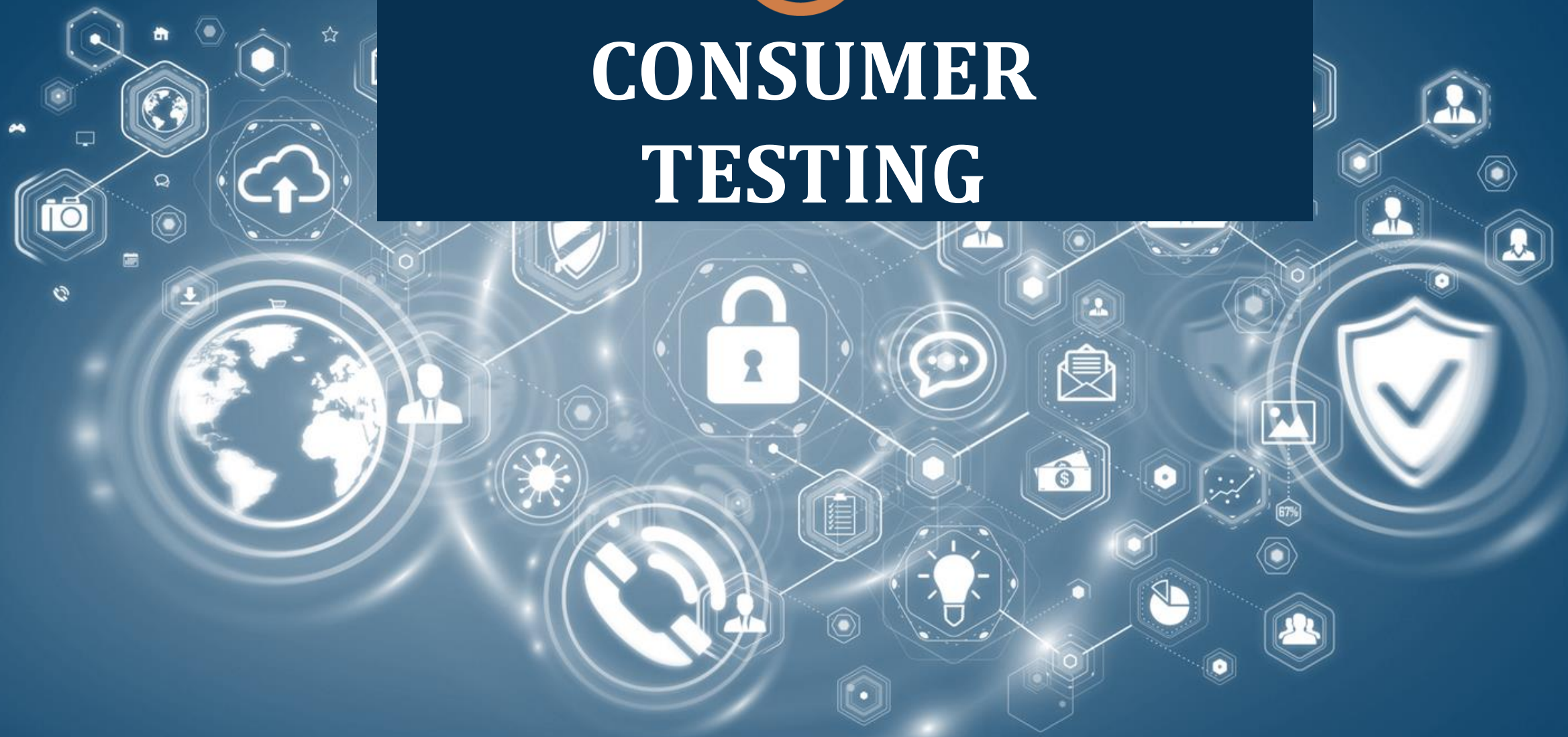
4. Changing applicability – current state of label as new security threats emerge

5. End-of-life considerations – security & non-connected functionality

6. Consumer expectations – how actions or inactions may impact product security

Consumer Education Elements

CONSUMER TESTING



Label Usability

Usability: “the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” (ISO 9241-11:2018)

EFFECTIVENESS

Consumers should be able to interpret the label’s meaning and successfully compare two or more products. Elements of the label should be commonly understood.

EFFICIENCY

Consumers should be able to quickly gain a broad sense of the product’s cybersecurity level. The label should have a minimalistic design and be understandable by those without expertise in cybersecurity. Documentation should be in plain language.

SATISFACTION

Consumers should perceive the labels as value-added, understandable, useful in their product purchase decisions, and aesthetically/visually appropriate.

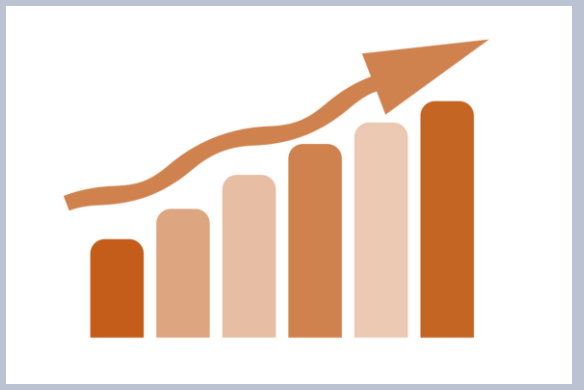
Testing Considerations

Pre-market Consumer Testing

Evaluate usability of potential label designs & consumer education materials with demographically diverse sample of consumers

Post-market Consumer Testing

Re-evaluate label usability. Assess growth of brand recognition and actual impact of label on consumers' purchase decisions



LESSONS LEARNED

Take Initiative

- Look for opportunities to leverage human-centered security research in practice
- Be ready to explain the value of your involvement

Human Element is a Hot Topic

- Discover most pressing issues for stakeholders
- Address misconceptions
- Identify allies and stakeholders with particularly valuable perspectives

Research Recommendations May Not Be Practical in the Real World

- Research findings may conflict
- Recommendations may not align with real-world goals
- Learn from prior real-world implementations
- “The devil is in the details.”

You Can't Make Everyone Happy

- Acknowledge competing goals and interests
- Aim for consensus rather than "perfect" solutions

NIST Labeling References

Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software

Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (Feb. 4, 2022)

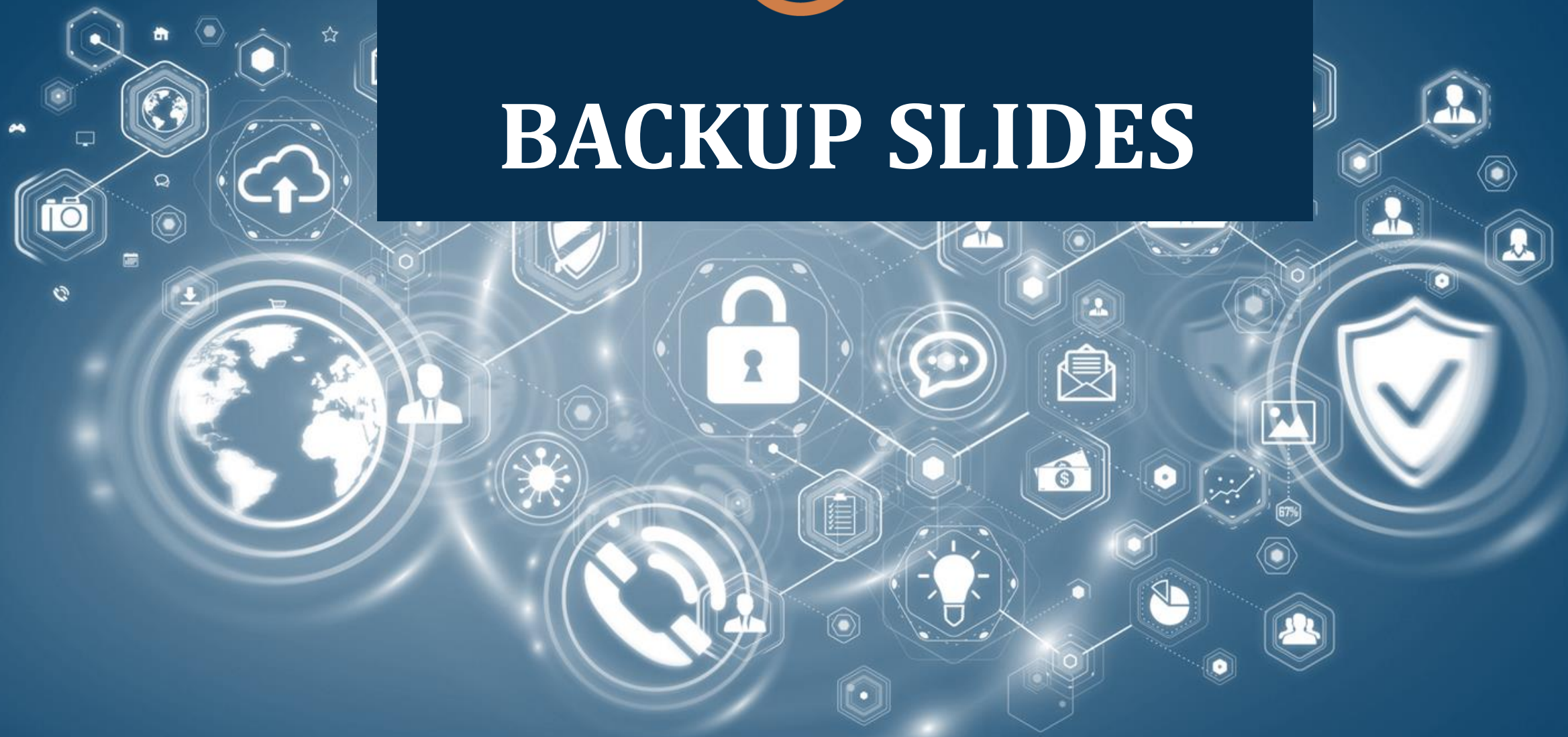
Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software A summary review of labeling actions called for by Executive Order (EO) 14028: Improving the Nation's Cybersecurity (May 10, 2022)

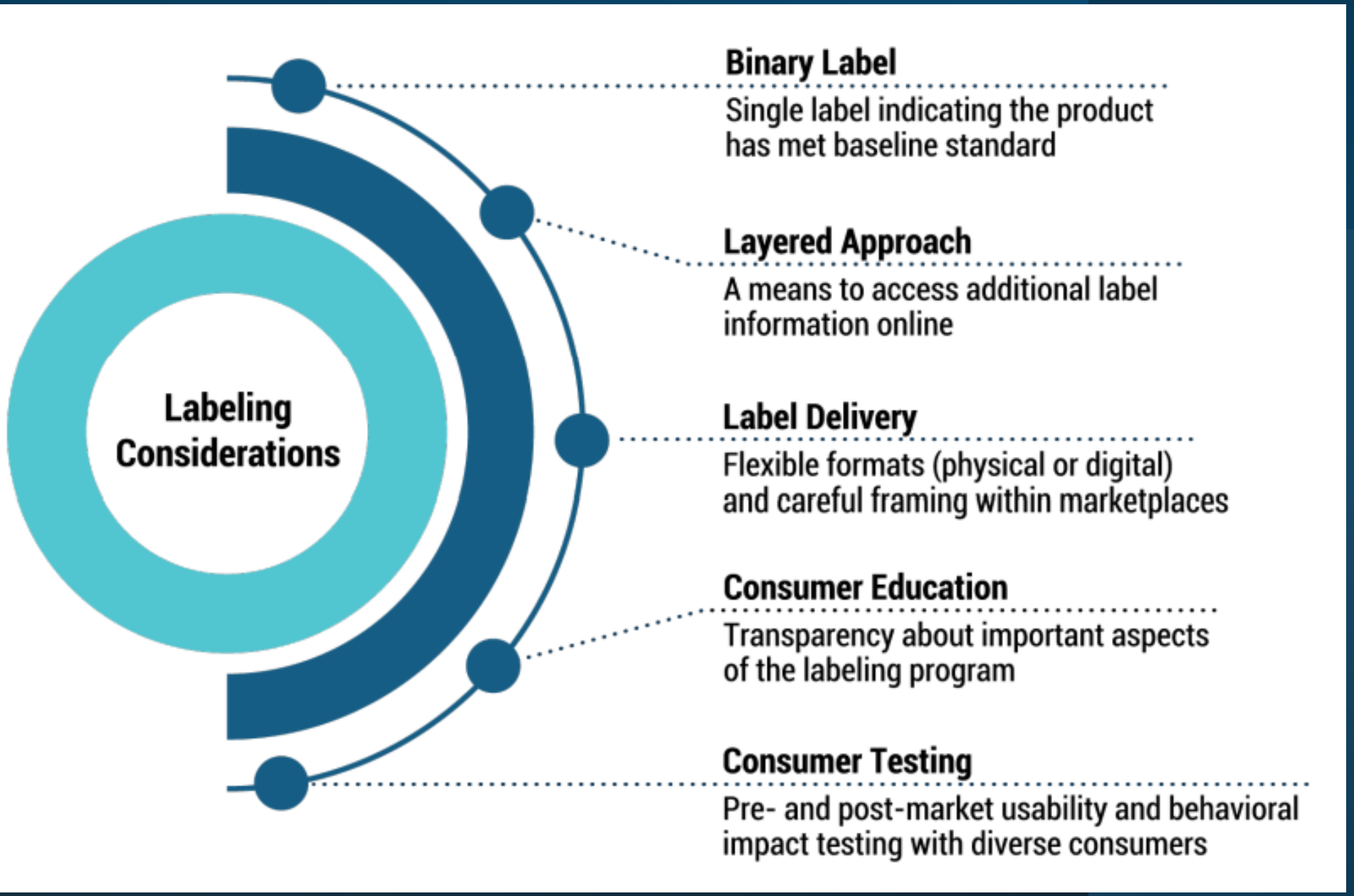
THANK YOU

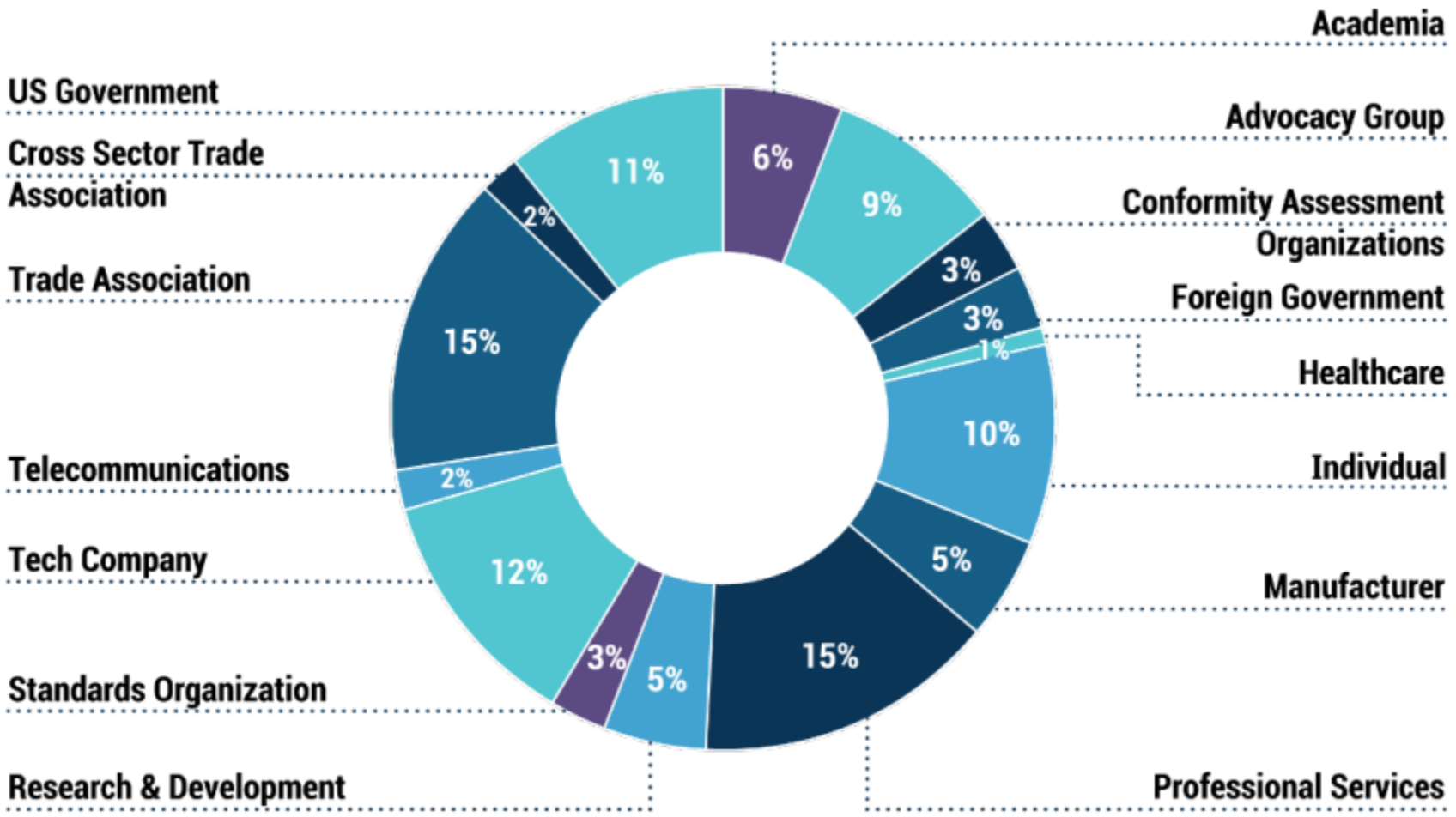
julie.haney@nist.gov

https://csrc.nist.gov/usable-cybersecurity

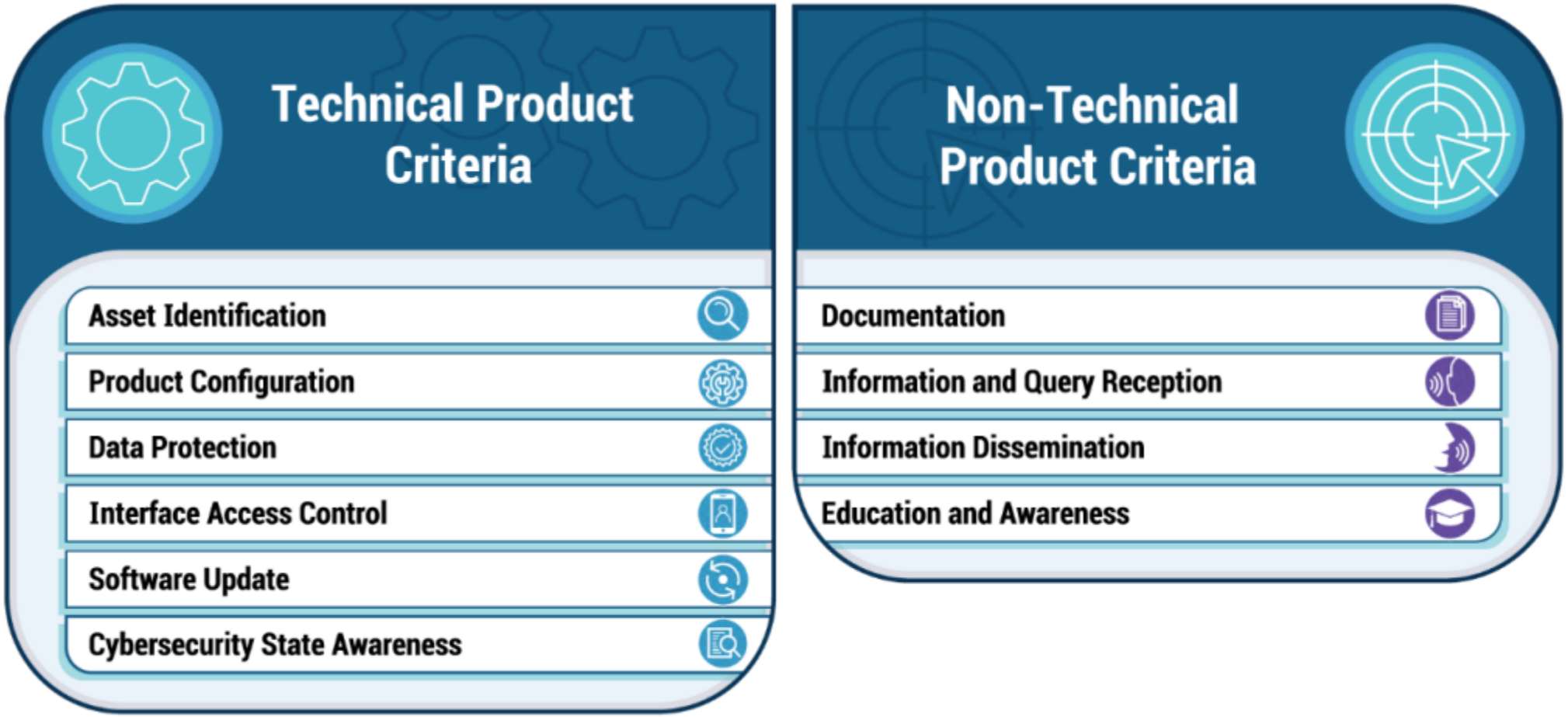
BACKUP SLIDES




Labeling Considerations
Binary Label
Single label indicating the product has met baseline standard
Layered Approach
A means to access additional label information online
Label Delivery
Flexible formats (physical or digital) and careful framing within marketplaces
Consumer Education
Transparency about important aspects of the labeling program
Consumer Testing
Pre- and post-market usability and behavioral impact testing with diverse consumers



Response Representation for EO Consumer IoT Labeling Criteria



Baseline IoT Product Criteria