# From Ivory Tower to Real World:

## Building Bridges Between Research and Practice in Human-Centered Cybersecurity

Julie Haney
National Institute of Standards and Technology
May 21, 2024

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.

# Human-Centered Cybersecurity @ NIST

***Championing the Human in Cybersecurity***

- Go beyond usability
  - Human, social, organizational factors
  - People's perceptions of, interactions, and relationships with cybersecurity
- Conduct applied research and other human-centered projects
- Provide actionable guidance to practitioners → **IMPACT**

# Impact on Practice


## Digital Identity Guidelines

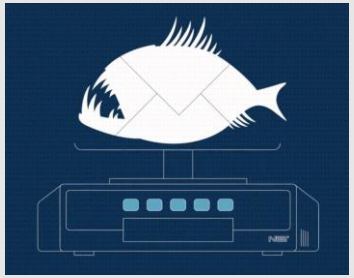
- Password choices, behaviors, policies
- Mobile device authentication
- MFA

## U.S. Cyber Trust Mark

- User perceptions, behaviors, challenges related to smart home security and privacy

## Kids Online Health & Safety Taskforce

- Password behaviors
- Online security and privacy perspectives of youth, parents, teachers



## NIST Phish Scale

- Why people click or don't click
- Method to determine difficulty of a phish and contextualize click rates



U.S. Cyber Trust Mark logo used with permission of the Federal Communications Commission

# Research-Practice Gap


- Disconnect between researchers and practitioners
- Due to differing incentives, values, work routines, language
- Can harm both communities

# Exploring the Research-Practice Gap in Human-Centered Cybersecurity

# Research Questions


- How do human-centered cybersecurity (HCC) research and cybersecurity practice inform and influence each other?
- What challenges do researchers and practitioners encounter during their interactions?
  - Does HCC pose unique challenges as compared to other fields?

# Surveys

## Practitioners

- Frequency, importance, and challenges of integrating HCC into practice
- Preferred ways of receiving HCC information
- Perceptions of HCC research
- HCC research topics of most importance

## Researchers

- Frequency, importance, and challenges of consulting practitioners/practitioner resources throughout the research life cycle
- Ways of distributing HCC information to practitioners

# Survey Participants

## 152 Practitioners

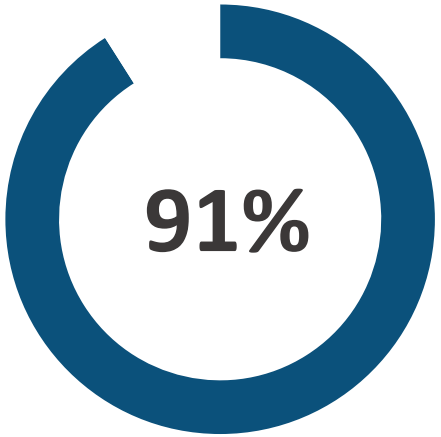
- **63%** security professionals, **32%** managers/execs, **18%** IT
- **81%** N. America, **11%** Europe
- **58%** industry, **21%** government
- **41%** had researcher experience

## 133 Researchers

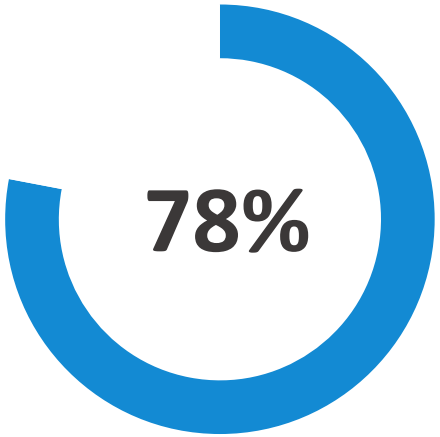
- **40%** tenure-track/tenured faculty, **31%** grad students
- **50%** N. America, **42%** Europe
- **80%** academia, **11%** industry
- **68%** had practitioner experience
- **93%** thought practitioners could make use of their research

# Practitioner Survey Results

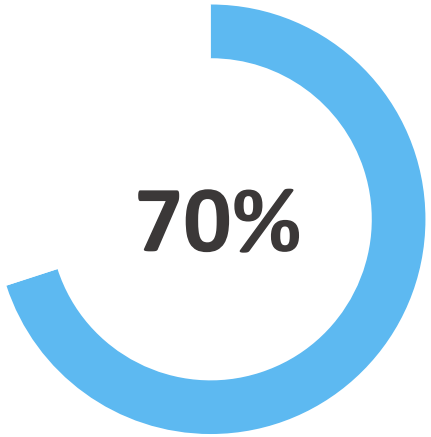
# What Practitioners Think About HCC



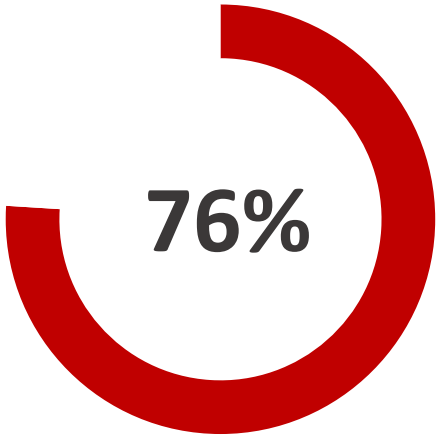

**Considering HCC is moderately or extremely important**




**Often or always consider HCC**




**Agree or strongly agree HCC has made a positive impact**




**Considering HCC is moderately or extremely challenging**

# Barriers to Integrating HCC into Work

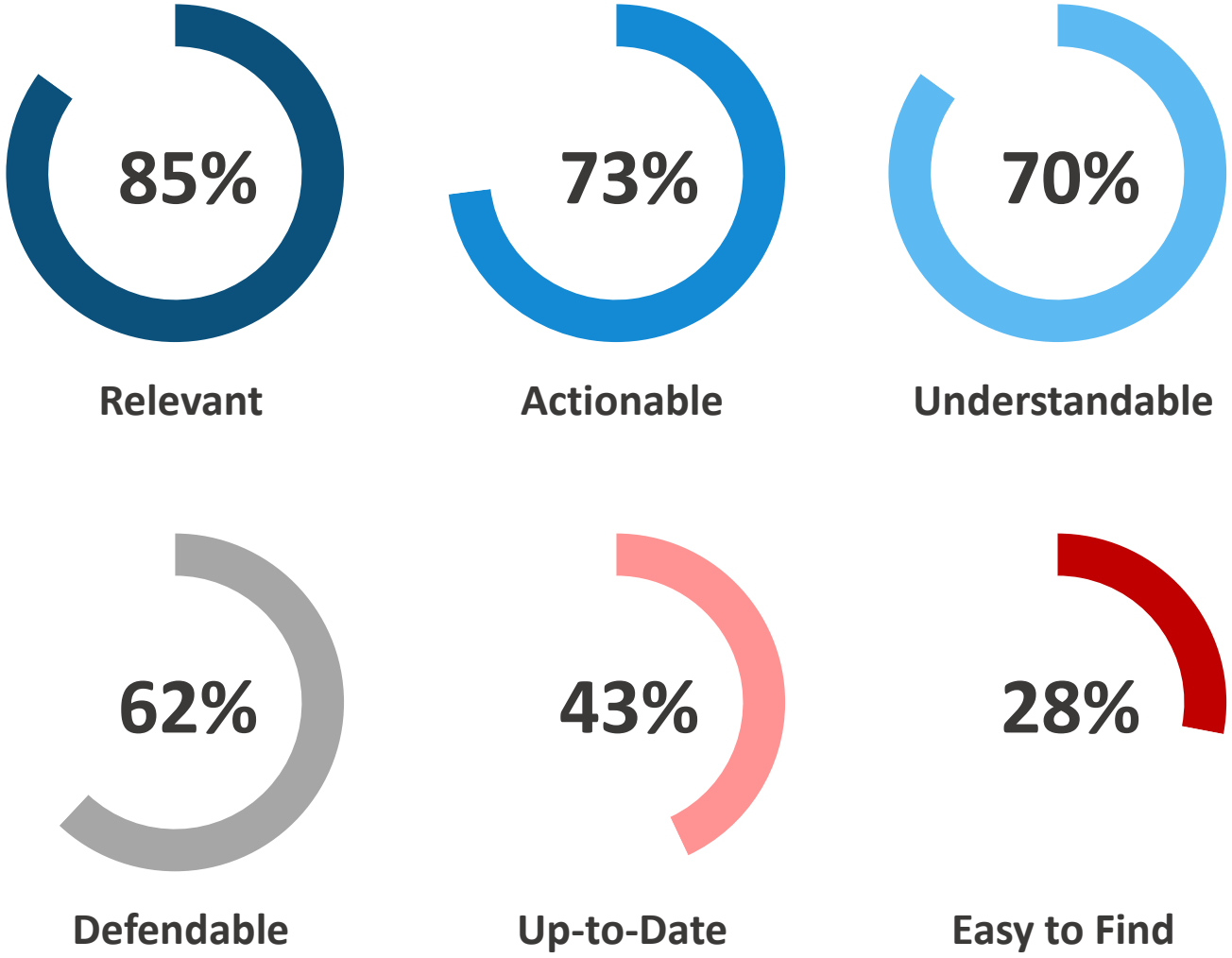
- Awareness and knowledge (**33%**)
- Organizational support and change (**18%**)
- Resources (**34%**)
- Tools and Technology (**17%**)
- Guidance (**13%**)
- Users (**8%**)

> Personnel in organizations may not be aware of the value of human-centered security, and therefore don't understand, have confidence in, or allocate time or resources to it. (P44)

> Technology workflows do not support or involve the human aspect or context. (P117)

> Lack of generally accepted and widely known principles and recommendations for practitioners (P15)

# What Practitioners Think About HCC Research



# HCC Research Topics of Most Importance to Practitioners

- Security awareness & training (**42%**)
- Incident response & security ops (**32%**)
- Governance, policy, & compliance (**31%**)
- Social engineering & media (**27%**)
- Authentication (**23%**)
- Workforce development (**22%**)
- Secure development (**22%**)
- User behaviors and attitudes (**22%**)

# Researcher Survey Results

# Research Life Cycle

## Research Conceptualization

- Identify new research topic
- Develop research questions or hypotheses
- Conduct literature review

## Study Design

- Decide on research methodology
- Develop and pilot study instruments or experiments
- Develop sampling and recruitment plan

## Data Collection

- Recruit practitioners

## Data Analysis

- Analyze data
- Develop implications & recommendations

## Dissemination

- Target outputs to practitioners

# Practitioner Engagement Throughout Research Life Cycle

- Saw importance of engaging practitioners/practitioner resources at different points
  - Highest at the beginning and end of the life cycle
  - Lowest for literature review, methodology, data analysis
- However, did not engage practitioners as frequently, possibly due to high level of challenge
  - Recruiting practitioners and targeting outputs for practitioners particularly challenging

# Pre-dissemination Barriers to Engaging Practitioners

- Practitioners don't have time (**67%**)
- Organizational gatekeeping (**45%**)
- Practitioners don't see value (**43%**)
- Not sure how to reach practitioners (**42%**)
- Practitioner resources not based on rigorous evidence (**38%**)
- Little funding/resources (**36%**)

> I often reach out to practitioners to discuss study designs…Most of the time, I never hear back. (R47)

> The most difficult challenge I face in working with practitioners is getting approval (from their organizations) to share security related data. (R27)

> Uncertainty how to cite (whether they are appropriate to cite) practitioner resources (R41)

> The issues the academic community values, e.g. privacy, are not necessarily valued by practitioners. (R100)

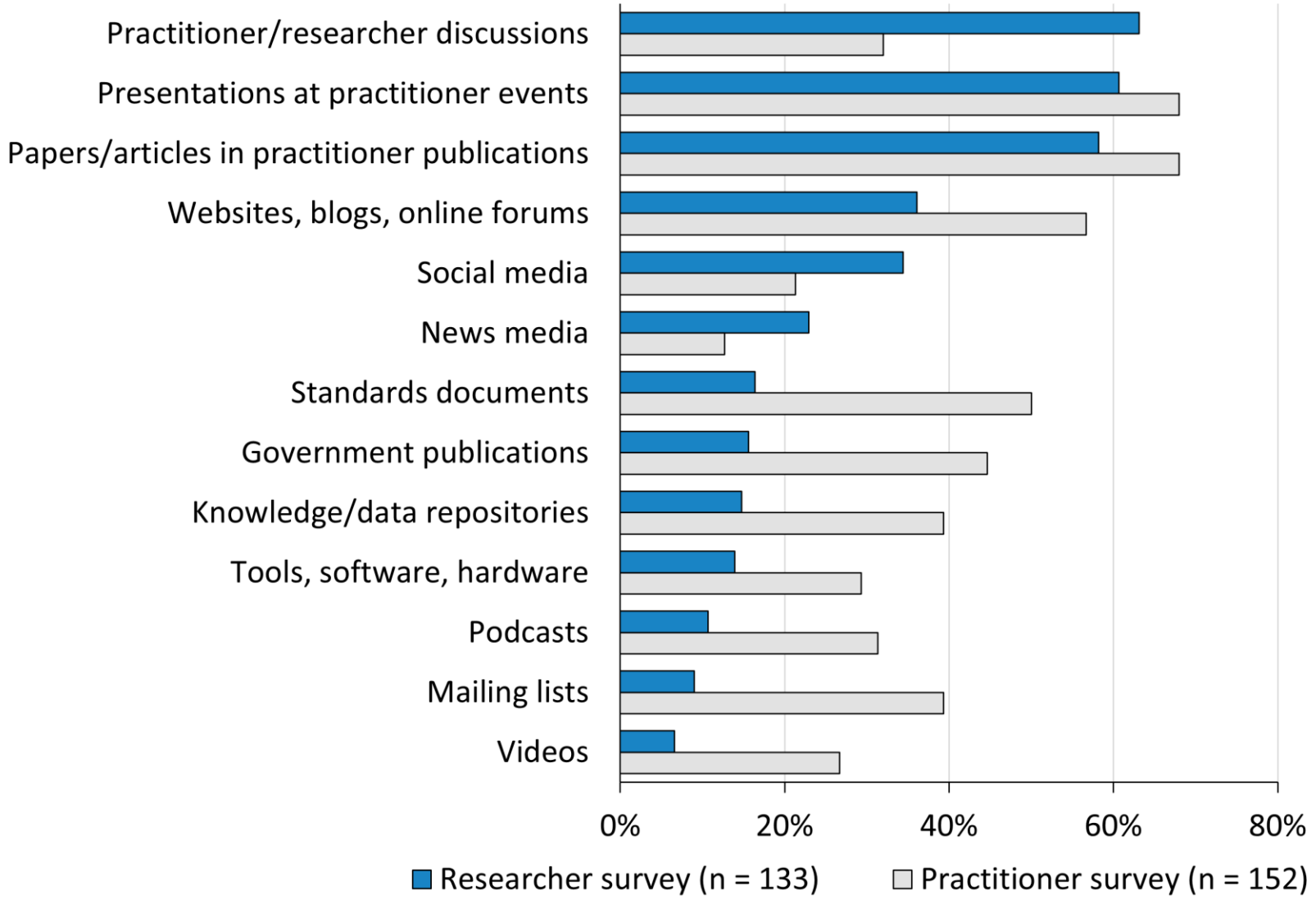
> These [practitioner] publications do not contribute towards my academic promotion, so there is little incentive. (R116)

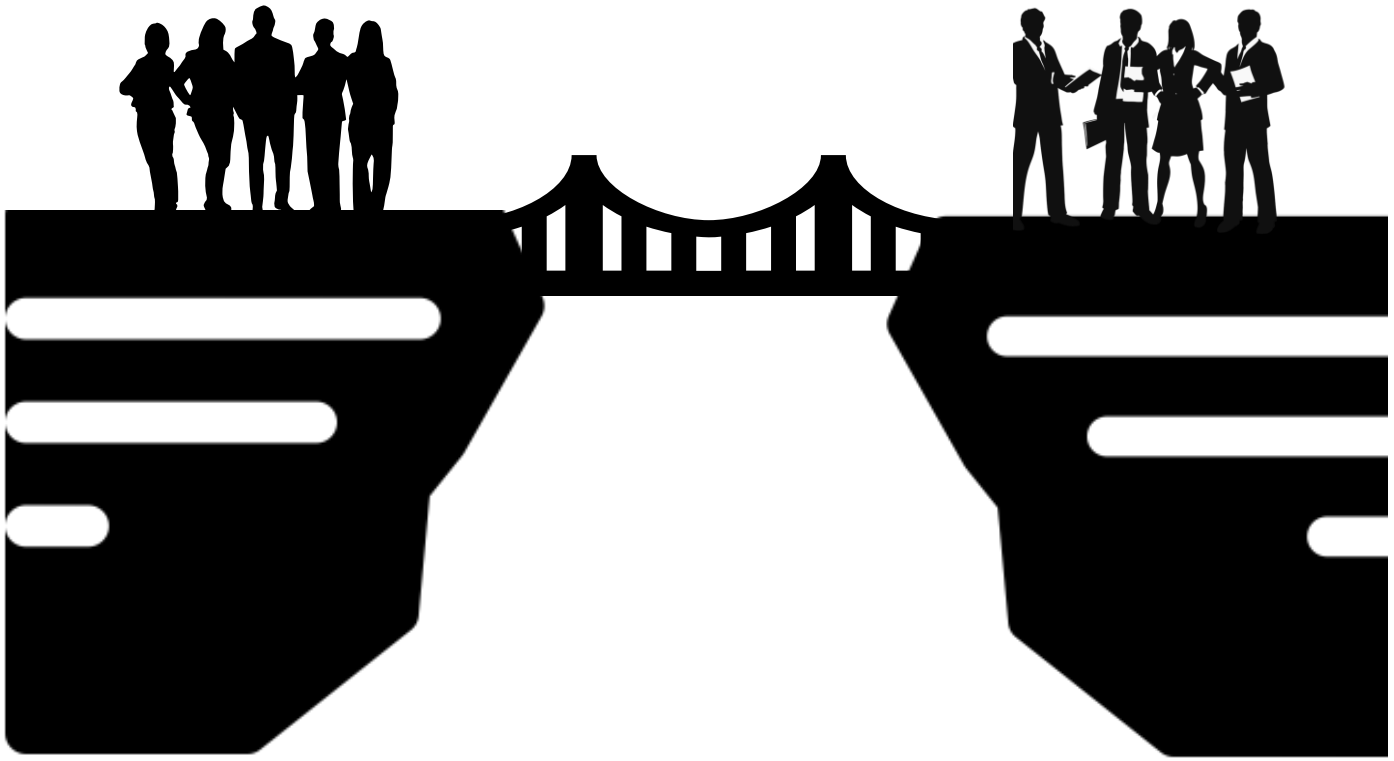
> As study results aren't always 'clean,' communicating the nuance of research findings to practitioners while providing useful, actionable insights can be challenging. (R80)

# Barriers to Dissemination

- Lack of practitioner interest (**41%**)
- Little funding/resources (**38%**)
- Not sure where to disseminate (**38%**)
- Little/no incentive (**34%**)
- Not sure how to translate for practitioners (**30%**)
- Difficult to get outputs accepted to practitioner forums (**26%**)

# Researcher Output Channels vs. Practitioner Preferences





# Implications: Bridging the Research-Practice Gap

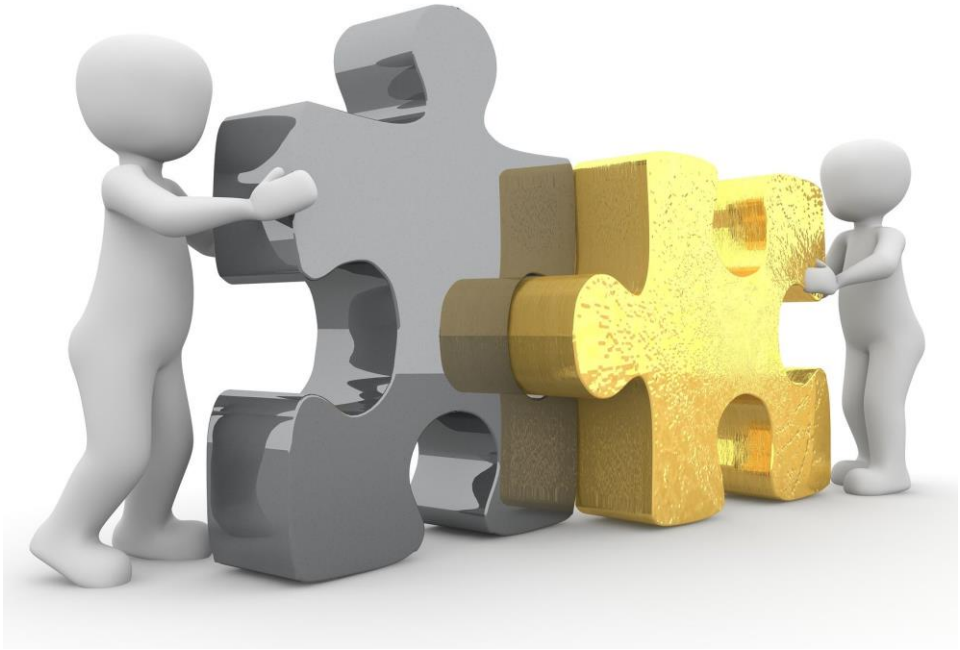
# Is Human-Centered Cybersecurity Different?

- Sociotechnical considerations
  - technology-focused workforce
- Rapid pace of change
  - practitioners don't have time
  - perception that research is quickly outdated
- Hard to show value proposition
  - reticence to implement operationally unproven recommendations
- Adversarial setting
  - hesitance to share security information
  - perception that users are a problem

# Suggestions for Researchers

- Consider where additional practitioner engagement may be beneficial
- Share via channels most preferred by practitioners
- Prioritize synthesis and reporting of research topics of most importance to practitioners
- Focus on a body of work rather than just one study

# Suggestions for Intermediaries



- Create space for research within practitioner forums and publications
- Establish evidence bridges
- Include basic HCC principles and benefits in standards and guidance documents
- Provide venues for researchers and practitioners to have meaningful interactions

# Future Plans

- Follow-up interviews to discover communities' preferences for potential solutions
- Establish HCC community of interest
- Determine how to make a broader impact

# Questions? Comments? Ideas?

julie.haney@nist.gov

human-cybersec@nist.gov

https://csrc.nist.gov/projects/human-centered-cybersecurity