NIST PUBLIC SAFETY COMMUNICATIONS RESEARCH

UNCREWED AIRCRAFT SYSTEMS

Cybersecurity and AI Risk Management for Uncrewed Aircraft Systems in Public Safety

February 7-8 2024

Gaithersburg, MD + Online

Safety

Conduct

Comfort

Logistics

In-Person Attendees

- Be **respectful and supportive**
- Be sure to state **your full name** and organization when speaking
- **Primary Q&A will take place online**. For any in-person participation, wait until you **receive a microphone to share questions or comments** so all participants can hear you
- Please be courteous of others and conduct **side conversations outside of the room**
- For questions, assistance or troubleshooting, reach out to Stephanie: stephanie.layman@nist.gov / (720) 202-7226

Virtual Attendees

- Be **respectful and supportive**
- Be sure your screen name includes **your first and last name**
- All virtual participants will be **muted with cameras off**
- For **closed captioning (CC)** head to Zoom's 'Settings' **>** 'Accessibility' **>** 'Closed Captioning'. Then click 'Always show captions'.
- For questions, assistance or troubleshooting, reach out to Elizabeth via email: ejh5@nist.gov / (717) 398-4891

Photo and Recording Policy

Record and Share

By default, screen will be recorded and broadcast. Photos are welcome.

Check otherwise

Attendees may have different levels of sensitivity.

Raymond Sheh

- Workshop Chair
- Contact: Raymond.Sheh@NIST.gov

Terese Manley

- UAS Portfolio Lead and Moderator
- Contact: Terese.Manley@NIST.gov

Ellen Ryan

- Host, Deputy Division Chief
- Contact: Ellen.Ryan@NIST.gov

Sid Bittman

- Technical and Logistical Support
- Contact: Sidney.Bittman@NIST.gov

Purpose & Outcomes

Purpose

- To improve management of Cybersecurity and AI Risk.
- Across the UAS for Public Safety Ecosystem.

Outcomes

- Network and hear each others' challenges and capabilities.
- Identify resources and inform a future roadmap.
- Develop an initial Top 10 list.

Day 2 Agenda

1. Day 1 Recap
2. Q&A
3. Experiences with Self-Driving Cars
4. UAS Breakout Scenario - Proposing Solutions
5. Prioritization Exercise
6. Event Recap and Next Steps

What did we discuss?

- UAS and risk management in public safety operations
- AI, cybersecurity, and UAS regulation
- AI and cybersecurity frameworks and ongoing research
- Law and ethics re: AI and UAS
- UAS in connected systems
- Collaborative structured UAS training

What are you most concerned with?

- AI action without human oversight (i.e. no human in the loop)
- Human reliance, trust, and complacency
- False positive identification
- Legal liability
- Lack of adequate or available training on AI systems
- No simple tools / checklists to assess AI or cybersecurity risk

What are you most concerned with?

- Possibility and ease of conducting cyber attacks (e.g. spoofing, overtaking command)
- Lack of cybersecurity defense against adversaries
- Technology limitations to reliably support autonomous flight
- AI bias, hallucinations, and model poisoning
- Unknown unknowns


Q&A
NIST
PUBLIC SAFETY
COMMUNICATIONS
RESEARCH

Experiences with Self Driving Cars

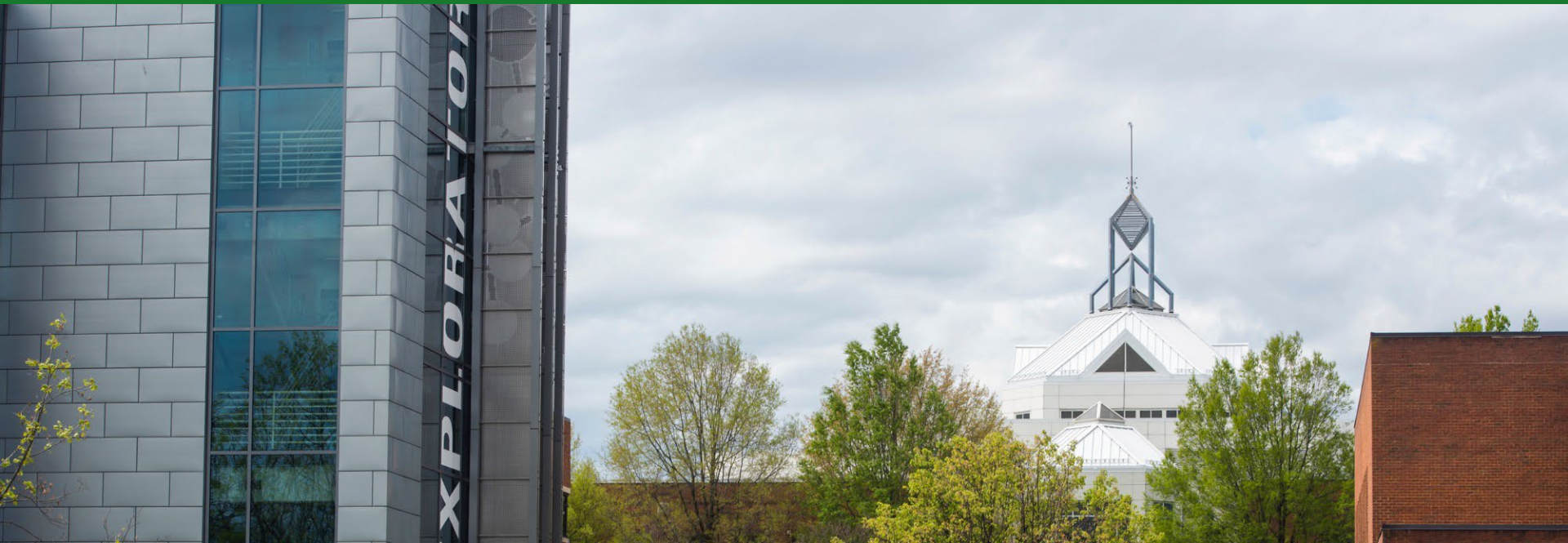
- Missy Cummings
  George Mason University

Missy Cummings
George Mason University

DEPLOYING AI: LESSONS LEARNED FROM SELF-DRIVING CARS

Missy Cummings, PhD

George Mason University

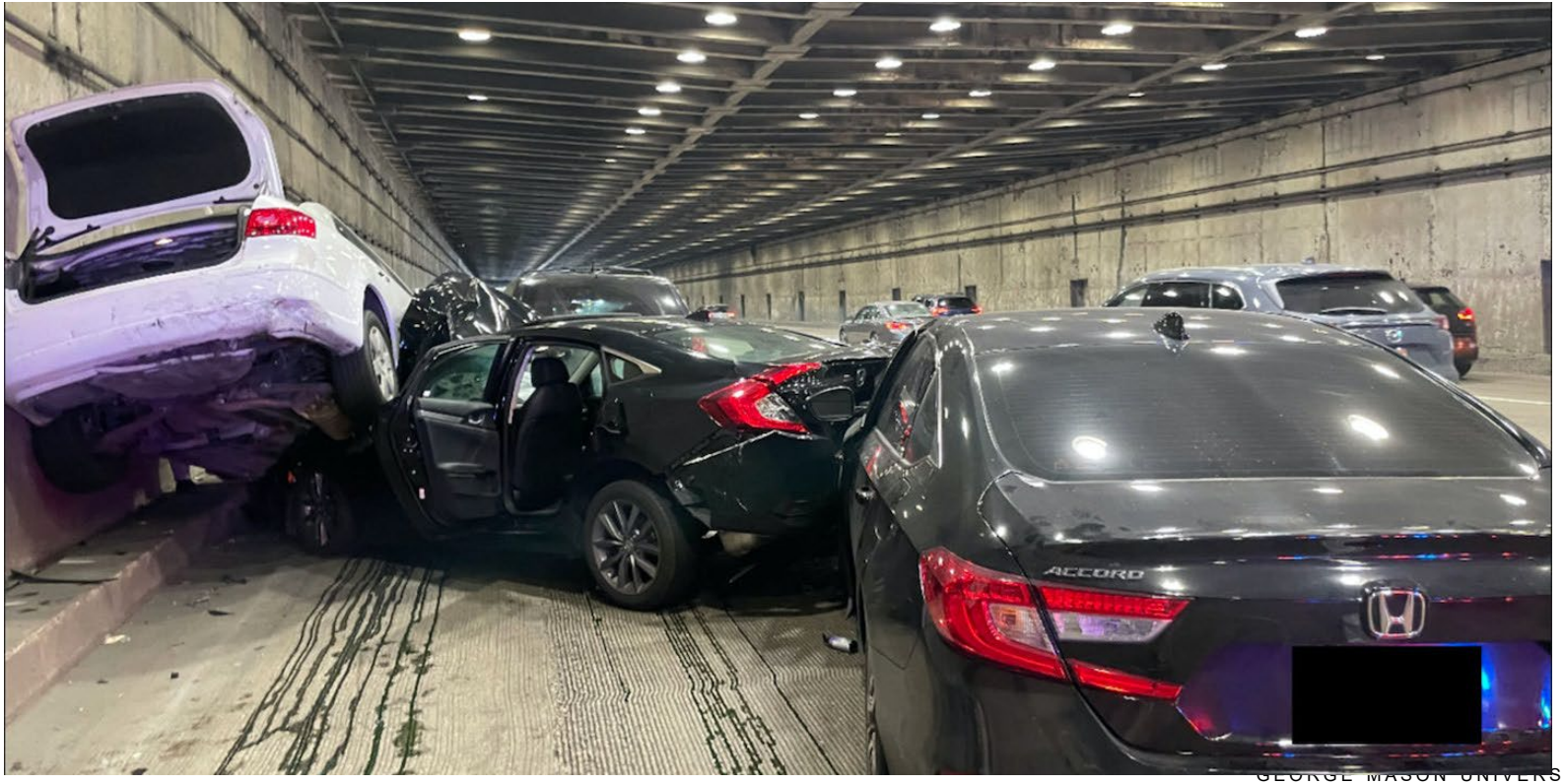


5 lessons learned for deployments of any kind of algorithmic decision maker

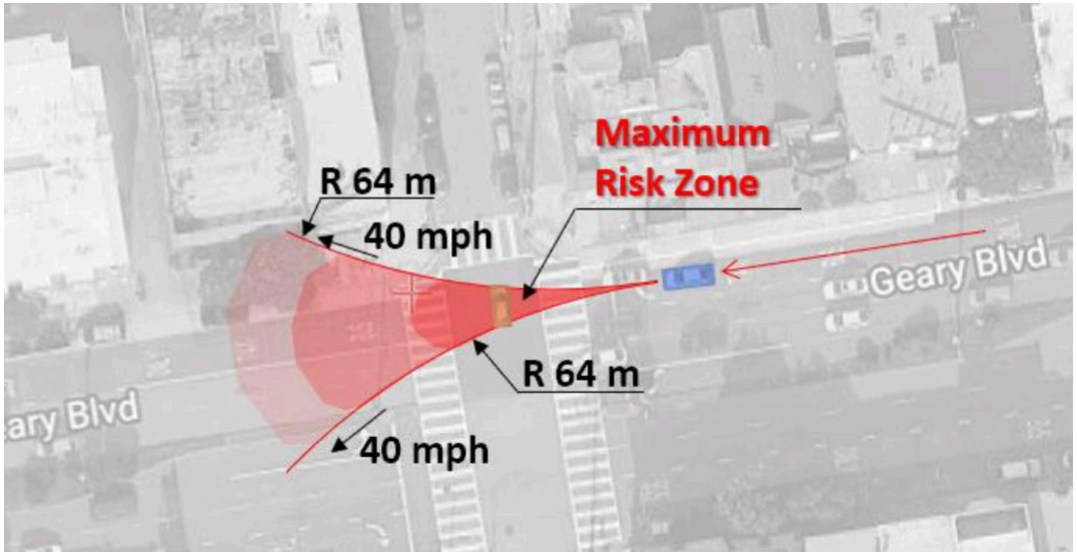
- Human errors in operation get replaced with human errors in coding
- Failure modes can be surprising
- Probabilistic estimates do not approximate judgment under uncertainty
- Maintaining AI is just as important as creating AI
- AI should be implemented with an understanding of system-level implications

Human errors in operation get replaced with human errors in coding

Failure modes can be surprising



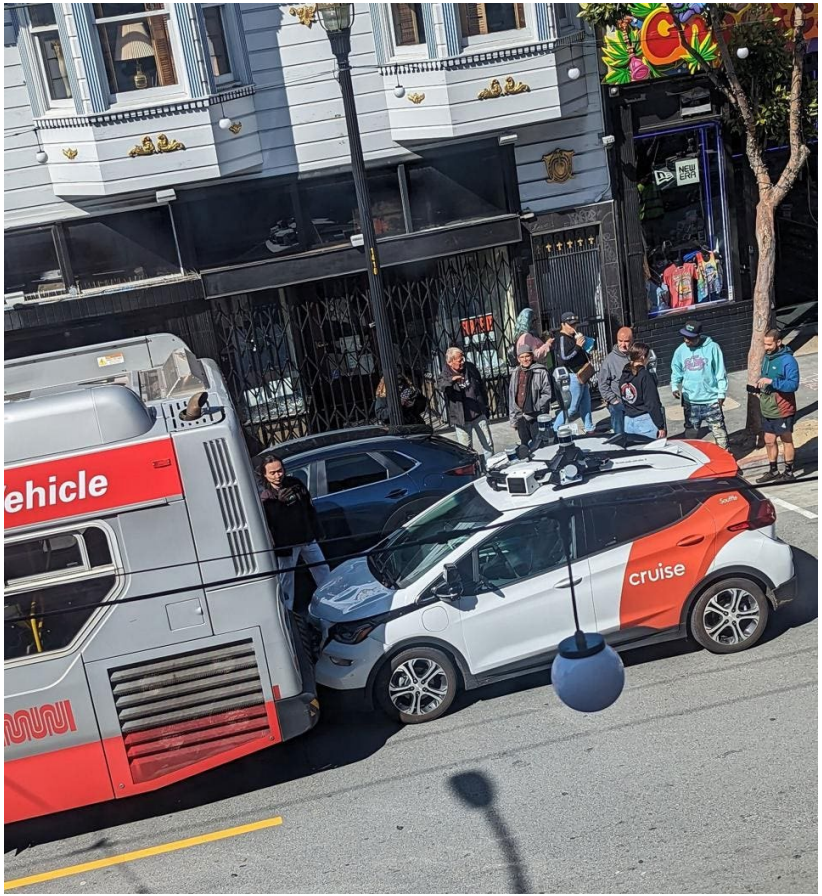
Probabilistic estimates do not approximate judgment under uncertainty



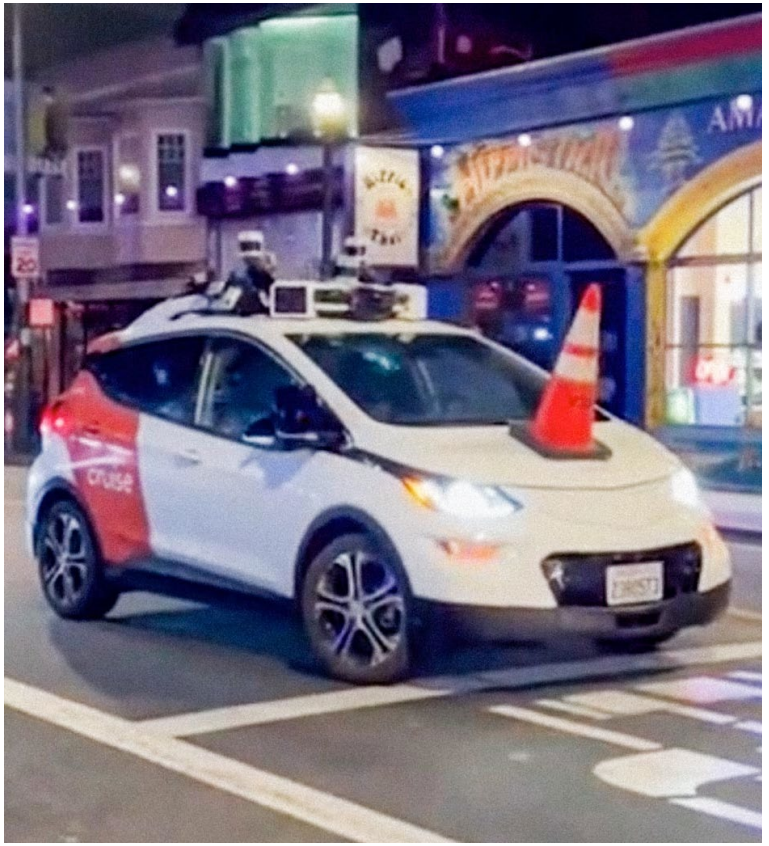
"The Cruise AV had to decide between two different risk scenarios and chose the one with the least potential for a serious collision."

https://www.autoblog.com/2022/09/01/gm-cruise-autonomous-crash-recall/ and https://www.retrospectav.com/blog/unacceptably-risky-part-1-safety-report-on-cruises-crash

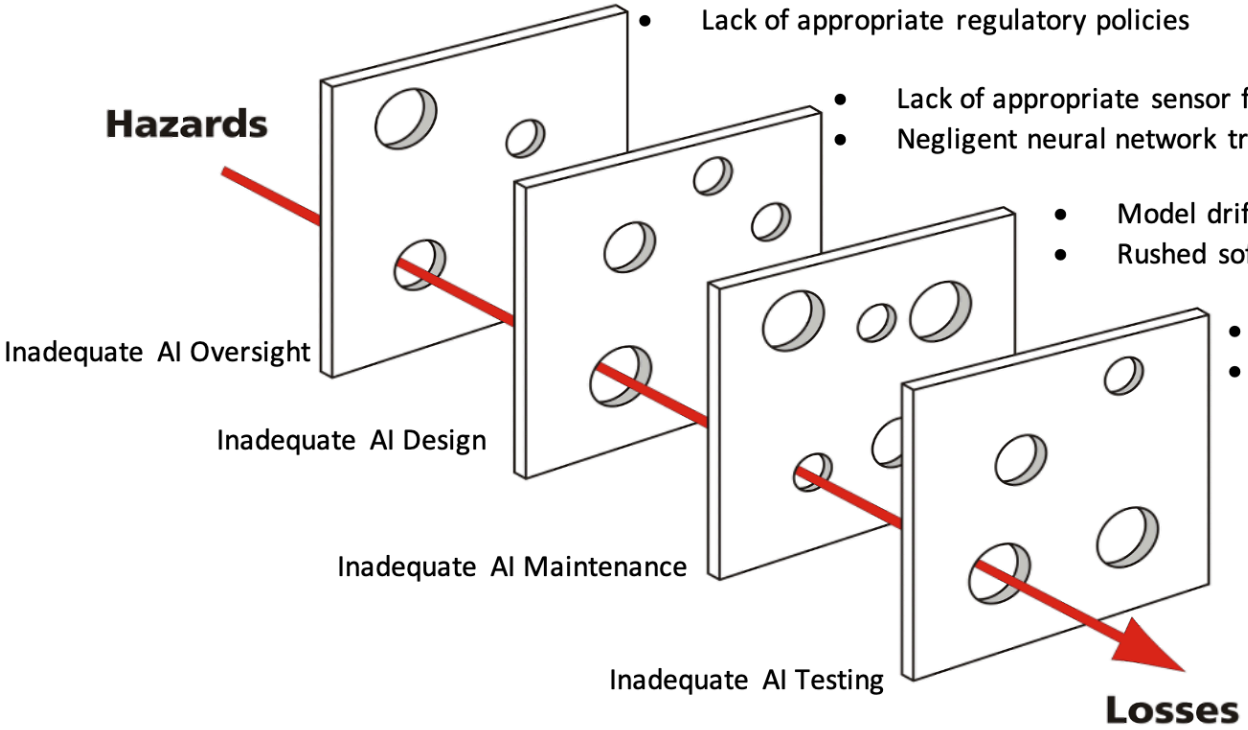
Maintaining AI is just as important as creating AI



AI should be implemented with an understanding of system-level implications



AI & Hazard Analysis



- Pressure to use AI from external stakeholders
- Lack of appropriate regulatory policies

- Lack of appropriate sensor fusion
- Negligent neural network training

- Model drift not corrected
- Rushed software updates

- Lack of comprehensive testing
- Overreliance on simulation for testing

Questions?

Resume at 11:00 am
(in 15 minutes)

A breakout session will follow the break.

Break

Breakout Session 2:
*How *should* the risks be managed?*
What questions should a chief/manager be asking?

Same groups
as yesterday

Same scenarios
as yesterday

This time discuss
solutions

Breakout Session 2: Instructions

- Listen as we read through a brief UAS scenario and provide prompting questions **(2-3 minutes)**
- Work with your group and facilitator to discuss and provide answers to the prompting questions **(12-13 minutes)**
- Time-permitting, we'll repeat for 3-5 scenarios.
- For each scenario, consider **solutions** to the issues raised on Day 1 and questions that a police chief/public safety manager should be asking.

Scenario 1: Changing Maps

1. *911 Call, suspicious person in an industrial park.*
2. *DFR dispatched to a wooded park across the road for the best view.*
3. *On descent, the dispatcher suddenly realizes that the park is now a construction site that isn't on the map yet.*
4. *Due to delays in the system, the dispatcher cannot intervene in time. The AI on the UAS must figure out what to do.*

- What technical and procedural measures could manage this risk?
- What residual risks are unavoidable?
- How do these inform the cost/benefit analysis?

Scenario 2: HAZMAT Accident

1. *DFR dispatched to interstate tanker crash ahead of HAZMAT team.*
2. *Due to smoke, dispatcher switches to IR camera.*
3. *AI on IR camera behaves inconsistently, identifying people and fire in seemingly random locations.*
4. *A gust of wind clears the smoke, visible light camera observes neither people nor fire.*

- What technical and procedural measures could manage this risk?
- What residual risks are unavoidable?
- How do these inform the cost/benefit analysis?

Scenario 3: Wildfire

1. *Back-burn West side of canyon using autonomous UAS.*
2. *Pre-planned flight path using ATAK to deploy “Dragonball” system.*
3. *Remote Pilot stationed on large antenna array on East side of the canyon.*
4. *UAS observed to be almost a half-mile off course.*
5. *Manual controls and mission abort failed to respond.*

- What technical and procedural measures could manage this risk?
- What residual risks are unavoidable?
- How do these inform the cost/benefit analysis?

Scenario 4: Public Event

1. *DFR system for monitoring and response for a state fair.*
2. *DFR system uses Remote-ID to track rogue drones and pilots.*
3. *A second drone appears with the same remote-ID.*
4. *DFR system assumes a malfunction and initiates a landing nearby.*
5. *On landing, connection is lost. Drone was never seen again …*

- What technical and procedural measures could manage this risk?
- What residual risks are unavoidable?
- How do these inform the cost/benefit analysis?

Scenario 5: Eavesdropping

1. *Sensitive drone footage posted on social media.*
2. *Included AI-generated overlays that identified the wrong person.*
3. *Suspect used a wireless ethernet sniffer near the DFR launch point.*
4. *DFR maintenance access point still had factory default settings.*
5. *Maintenance access point was also not firewalled from other DFR systems.*

- What technical and procedural measures could manage this risk?
- What residual risks are unavoidable?
- How do these inform the cost/benefit analysis?

Breakout Session 2:

Think about the top questions that every fire and police chief should ask as part of their cybersecurity and AI risk management approach.

- *What are some obvious questions to ask?*
- *What are some less obvious questions to ask?*

Your handout has some examples.

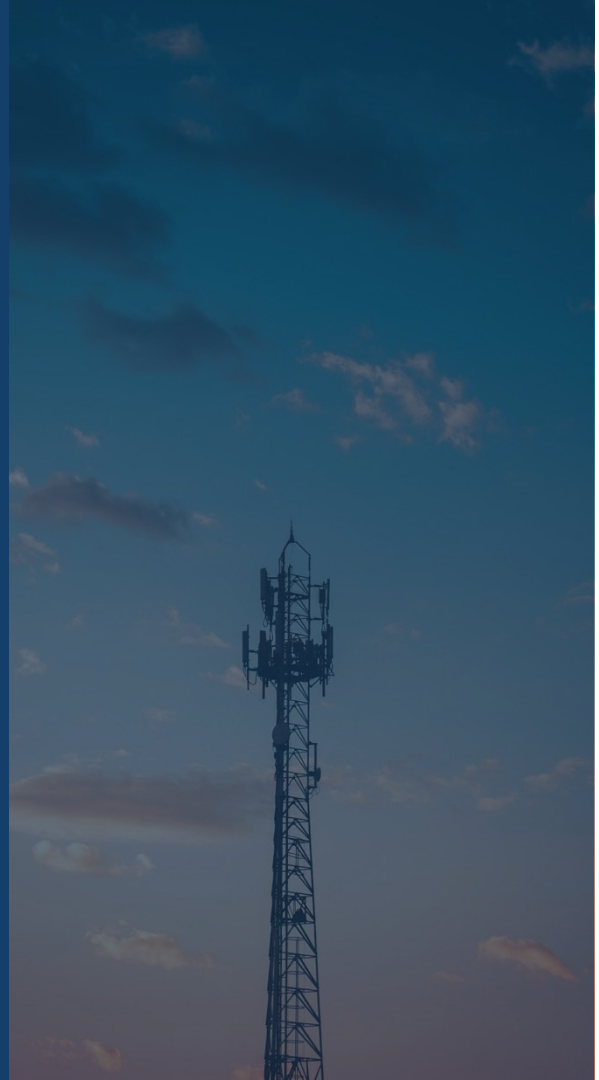
Slido

Grab your phone and head to
slido.com

Enter the code:
#1910 124

Type your responses in
to **answer the questions!**

Resume at 2:00 pm
(in 90 minutes)



Lunch

Top-10 and Next Steps

- Prioritizing via Dotstorming
- Top 10 Discussion
- Informing the Roadmap
- Next Steps

Dotstorming

- Navigate to: https://bit.ly/UASVote (or scan the QR code in your handout labeled “Prioritization Exercise”)
- Sign in by **typing your name** and then select **Join.**
- **You may now begin voting:** Vote by clicking on the small dots at the lower left of the card.
- With **10 votes in total** you can choose to cast all 10 votes on the same card **or** a variety before the cards are locked.

- **All slides and recordings will be available**!
  - See handout for site.

- **Submit follow-up questions and interest in participation in the ongoing working group here:**
- https://bit.ly/UASWorkshopQandA

Find out more!


Thank You!
NIST
PUBLIC SAFETY
COMMUNICATIONS
RESEARCH