NIST PUBLIC SAFETY COMMUNICATIONS RESEARCH

UNCREWED AIRCRAFT SYSTEMS

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

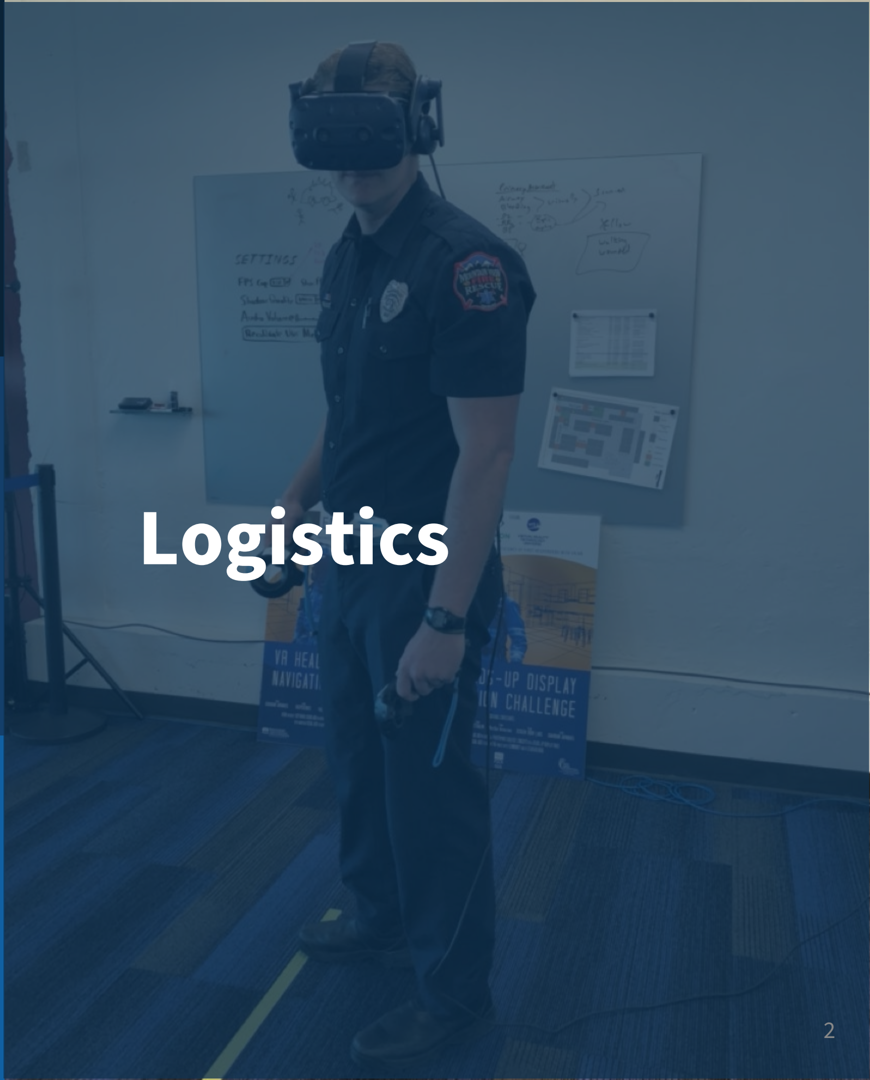
February 7-8 2024

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.

Introductions

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

PULLING THE ***FUTURE FORWARD***

The Public Safety Communications Research (PSCR) Division is the primary federal laboratory conducting research, development, testing, and evaluation for public safety communications technologies. It is housed within the Communications Technology Laboratory (CTL) at the National Institute of Standards and Technology (NIST). It addresses the R&D necessary for critical features identified by public safety entities beyond the current generation of broadband technology.

MISSION

PSCR is driven towards advancing public safety communications technologies by accelerating the adoption and implementation of the most critical communications capabilities to ensure the public safety community can more effectively carry out their mission to protect lives and property during day-to-day operations, large scale events, and emergencies.

PROMISE

PSCR accelerates innovation by investing in research to transform the future of public safety communications, technology, and operations.

PULLING THE *FUTURE FORWARD*

ABOUT PSCR | **5 KEY RESEARCH AREAS** | RESEARCH FACILITIES | RESEARCH PARTNERS | INTRAMURAL IMPACTS | EXTRAMURAL IMPACTS

USER INTERFACE USER EXPERIENCE

LOCATION-BASED SERVICES

MISSION CRITICAL VOICE

SECURITY

UNCREWED AIRCRAFT SYSTEMS

PULLING THE ***FUTURE FORWARD***

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.

Definitions

& Scope

For the purpose of this workshop:

- **Cybersecurity**
- **Artificial Intelligence**
- **Risk Management**
- **Uncrewed Aircraft System**
- **Public Safety**

Cybersecurity

The process of protecting information by preventing, detecting, and responding to attacks.

- NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1 (precursor to CSF 2.0)

Artificial Intelligence

… in general, are engineered systems that generate outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives.

– ISO/IEC 22989:2022

Artificial Intelligence
Scope for this working group:

*… in general, are engineered systems that generate outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives****, where the process used to generate the outputs cannot be practically (in the context of the application) derived and/or verified by humans using analytical methods.***

Risk Management

The process of identifying, assessing, and responding to risk.

- NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1 (precursor to CSF 2.0)

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

- NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1 (precursor to CSF 2.0)

(small) Uncrewed Aircraft System

… an uncrewed aircraft and the equipment necessary for the safe and efficient operation of that aircraft.

- Federal Aviation Administration (FAA)

(small) Uncrewed Aircraft **System**

- Dispatch systems, e.g. Drone as First Responder (DFR).
- Collaboration systems, e.g. TAK, DroneSense, DroneDeploy.
- Asset management and maintenance systems.
- Data storage and analysis systems, AI and otherwise.
- Communications systems.
- Downstream consumers, e.g. GIS.

Public Safety

- Fire
- Police
- Search and Rescue
- Hazmat

Public Safety

For this working group:

- Fire
- Police
- Search and Rescue
- Hazmat
- Contractors
- Industry and Resources
- Utilities
- Forest/Land Management

Day 1 Agenda

1. Intro
2. Public Safety Responder Risk Management
3. Resources, Regulation, and Accreditation
4. Cybersecurity and Artificial Intelligence
5. Connected Systems and Society
6. UAS Breakout Scenario - Identifying Gaps
7. Day 1 Recap

Responder Risk Management

- Katie Thielmeyer
  DRONERESPONDERS
- Bart Ramaekers
  Carma Police
- Jason Day
  Texas Department of Public Safety

Katie Thielmeyer

DRONERESPONDERS

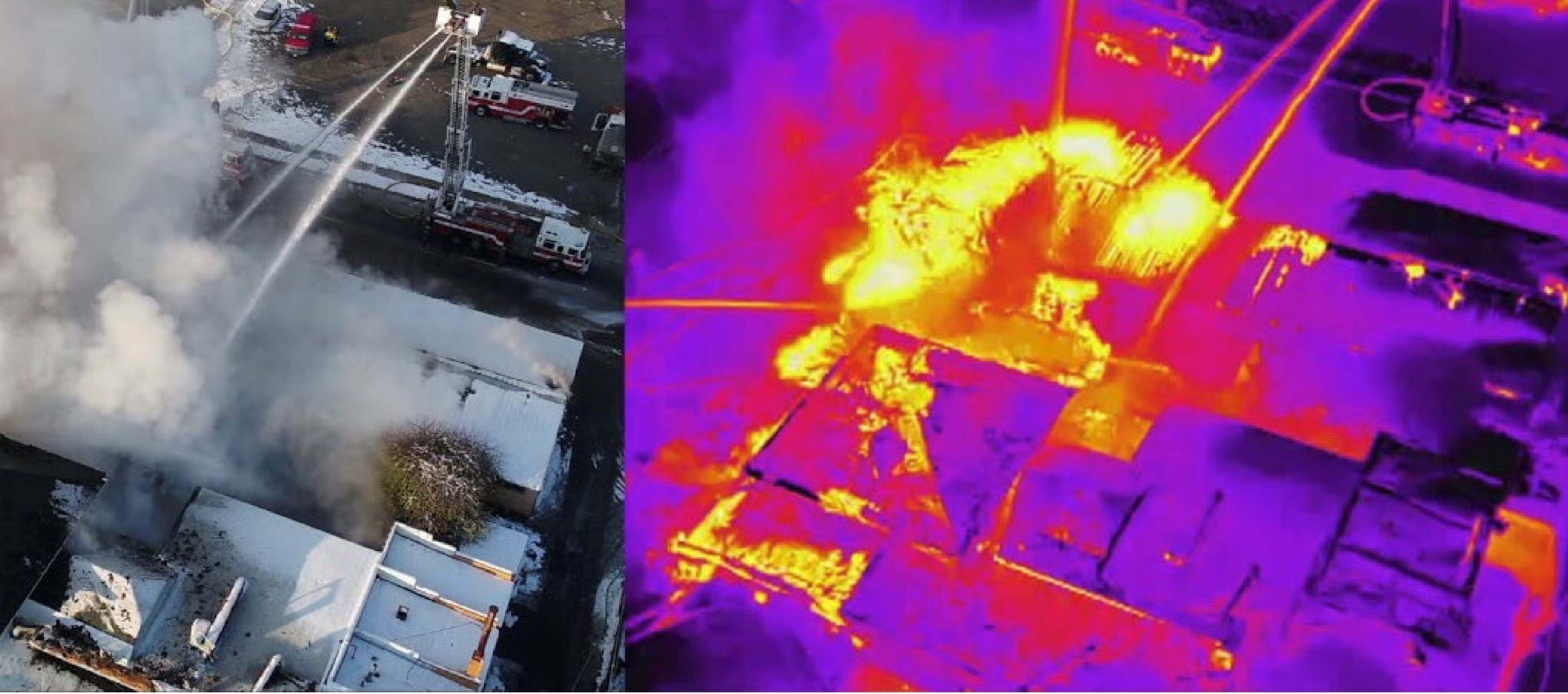
DRONERESPONDERS

Drones in Public Safety

Over 40 Public Safety Use Cases

Structural FireFighting – Visual Optics

Thermal Imaging Structure Fire



Optical View vs. Thermal Image View

See through Smoke and Effective Application of Water on the Fire

Major Traffic Accidents

Mass Casualty

Multiple Vehicle Fires

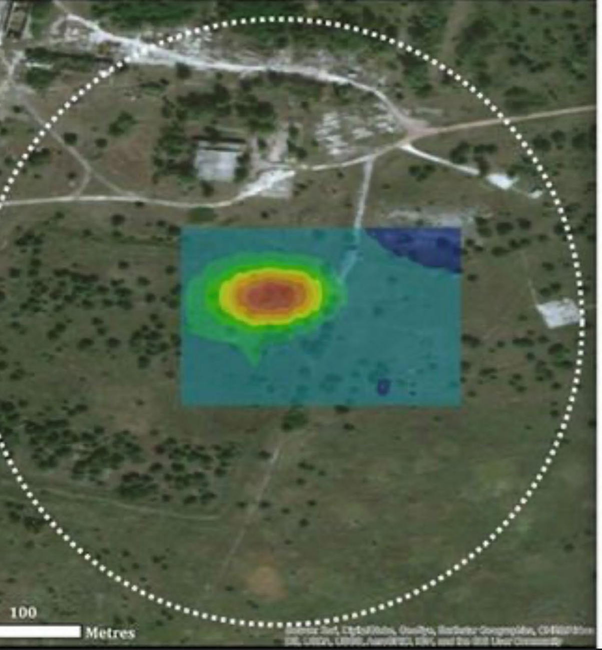
HAZMAT Operations
CBRNE

East Palestine, OH

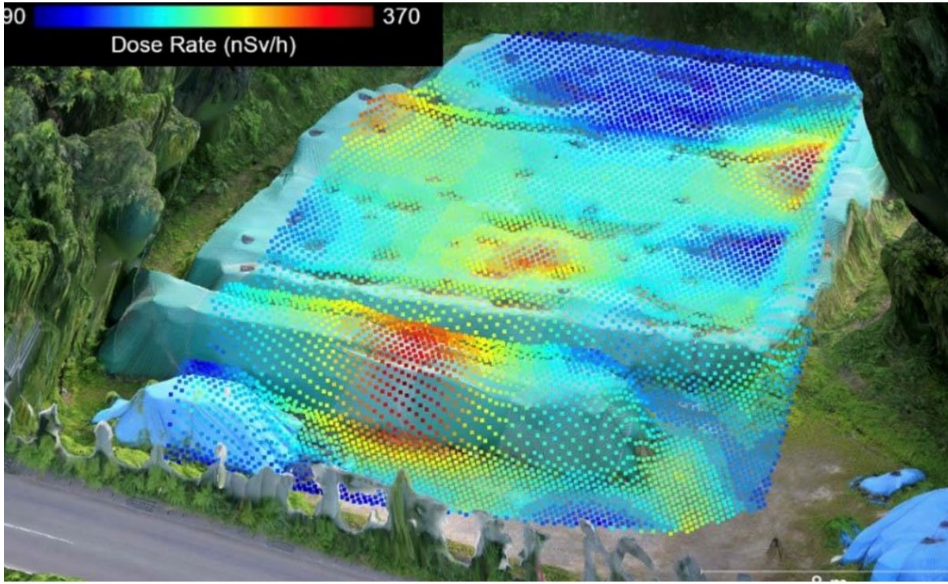
Philadelphia, PA

Lynchburg, VA

Train Derailment, Crash, Fire & Spill



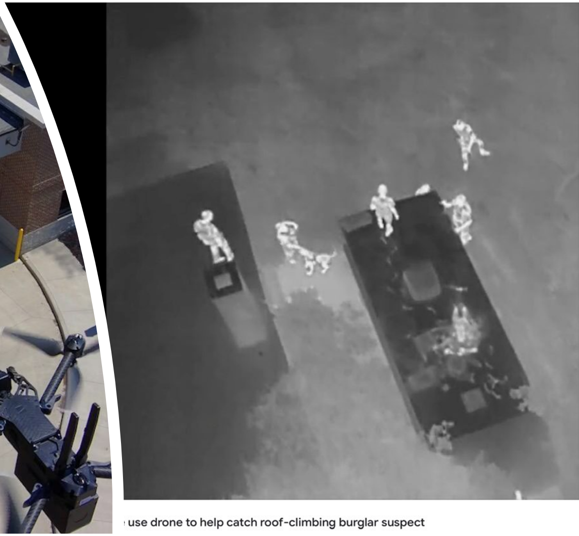
aster: New radiation hotspots found in Chernobyl's ...

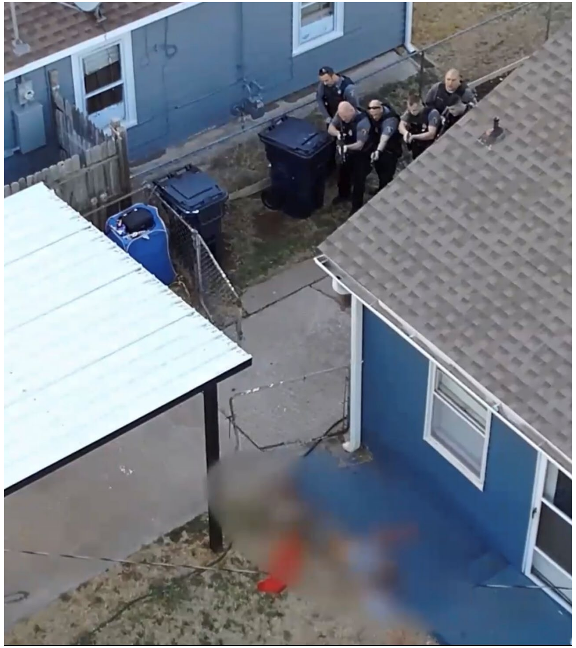


ll 3D aerial photogrammetry superimposed with a radiological map obtained using a single
o consecutive flights. (Image: IAEA and Fukushima Prefecture)

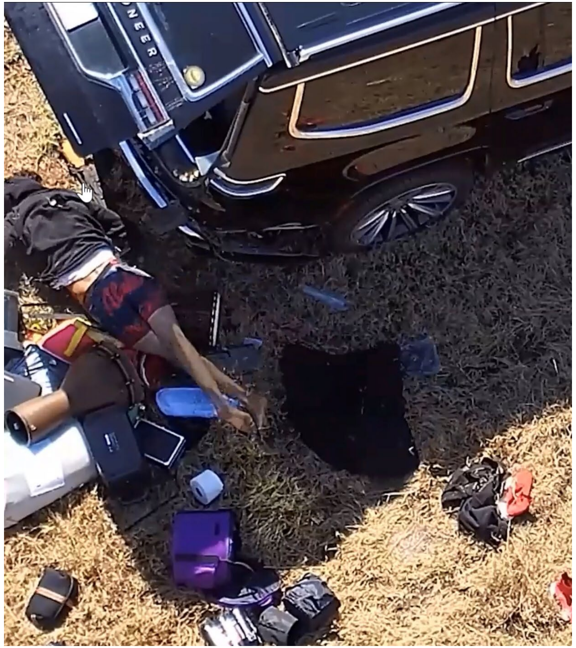
Drone Radiation Detection & Mapping

Law Enforcement Tactical Ops Overwatch

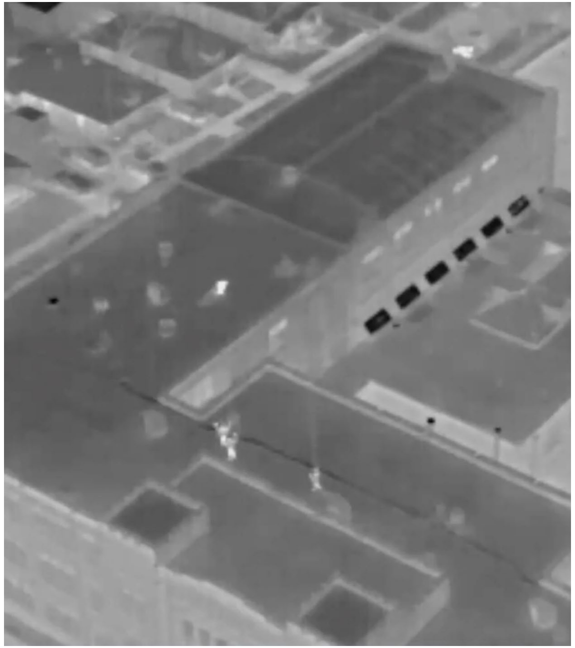




Avoids Ambush

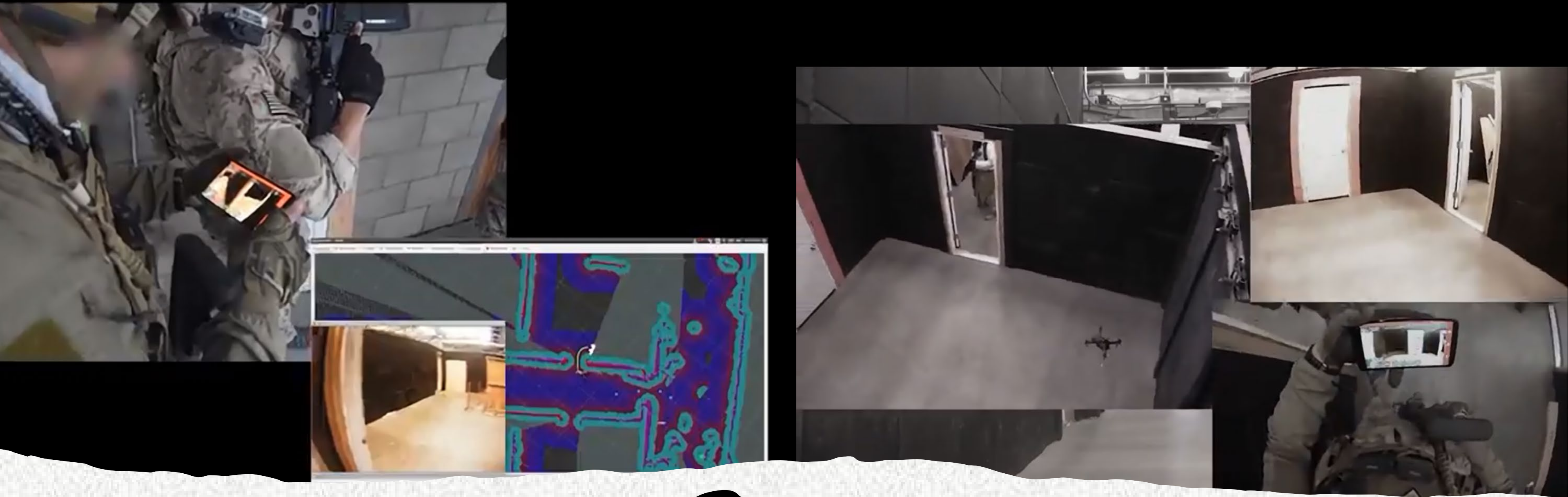


Suspect Reaching for AR15



Detect Thieves Hiding on Roof

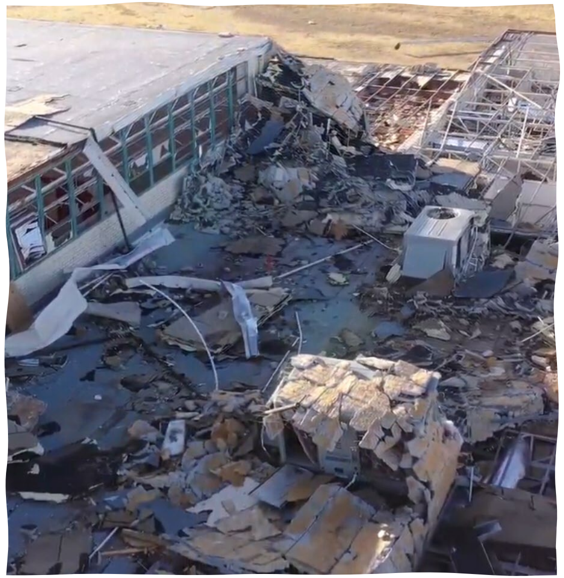
Oklahoma City PD Drone Incidents

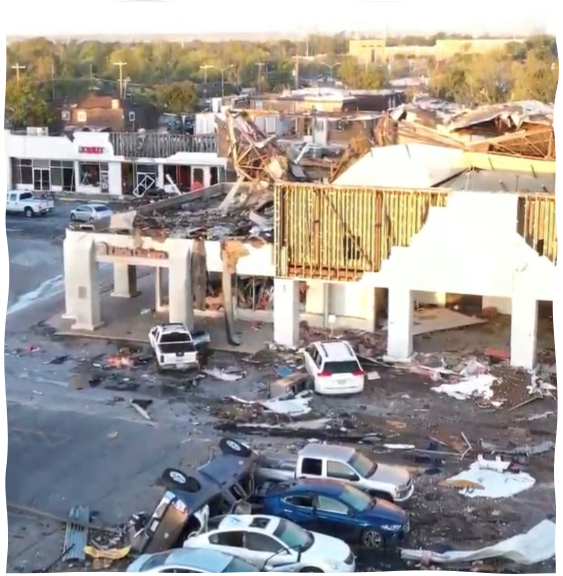


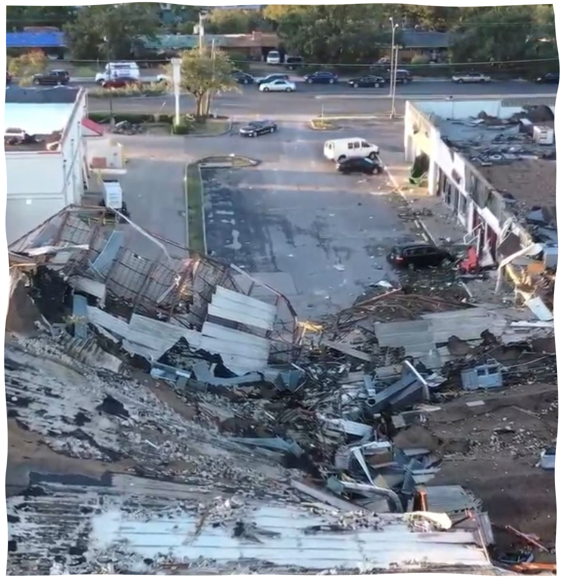
Law Enforcement Indoor Flights Room Clearing

Quickly Assess

How Bad is Bad?







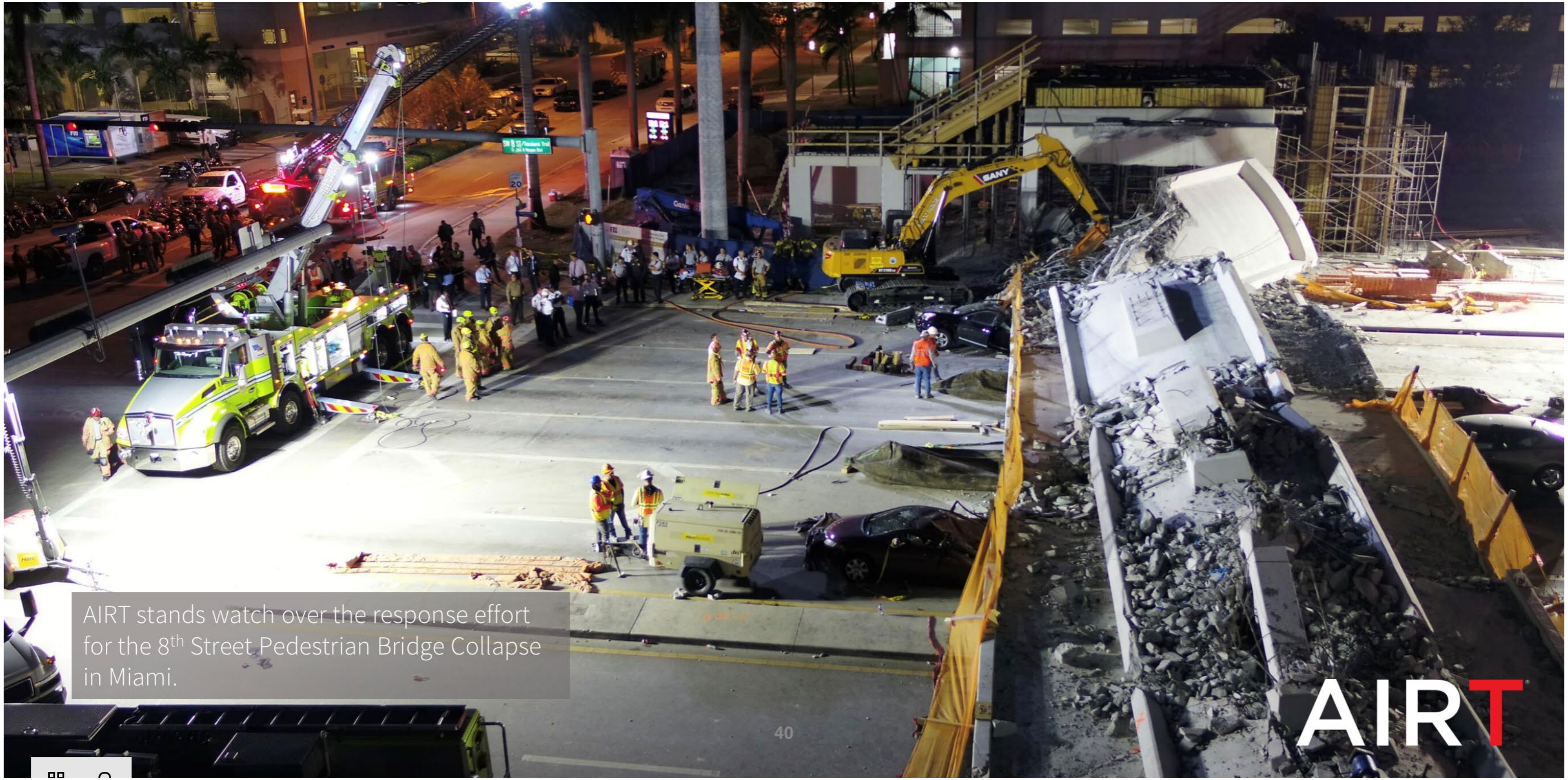
Tornado – Dallas TX

Search & Rescue, Damage Assessment

Drone Imagery & Damage Assessment Combined with GIS

Damage assessment using deep learning in ArcGIS

Damage assessment using deep learning in ArcGIS



AIRT stands watch over the response effort for the 8th Street Pedestrian Bridge Collapse in Miami.

- Surfside Condominium Collapse

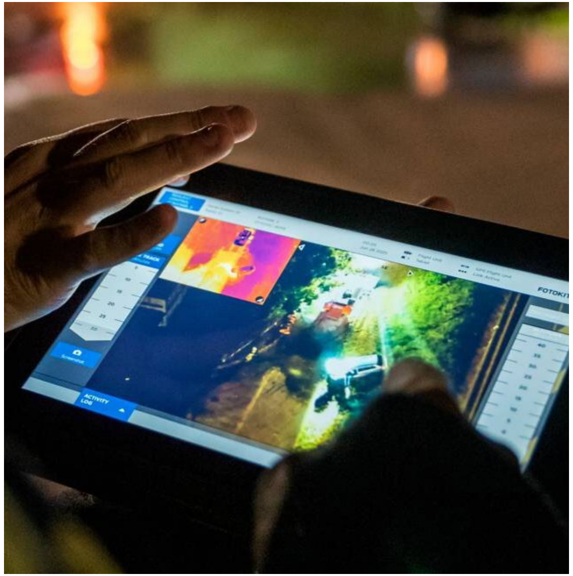
Charlottesville Unite the Right Rally & Protest

Traffic Crash Reconstruction – 1/3 Time, Reduces Secondary Accidents, Restores Commerce and Normal Traffic Flow

ACTIVELY TETHERED DRONE

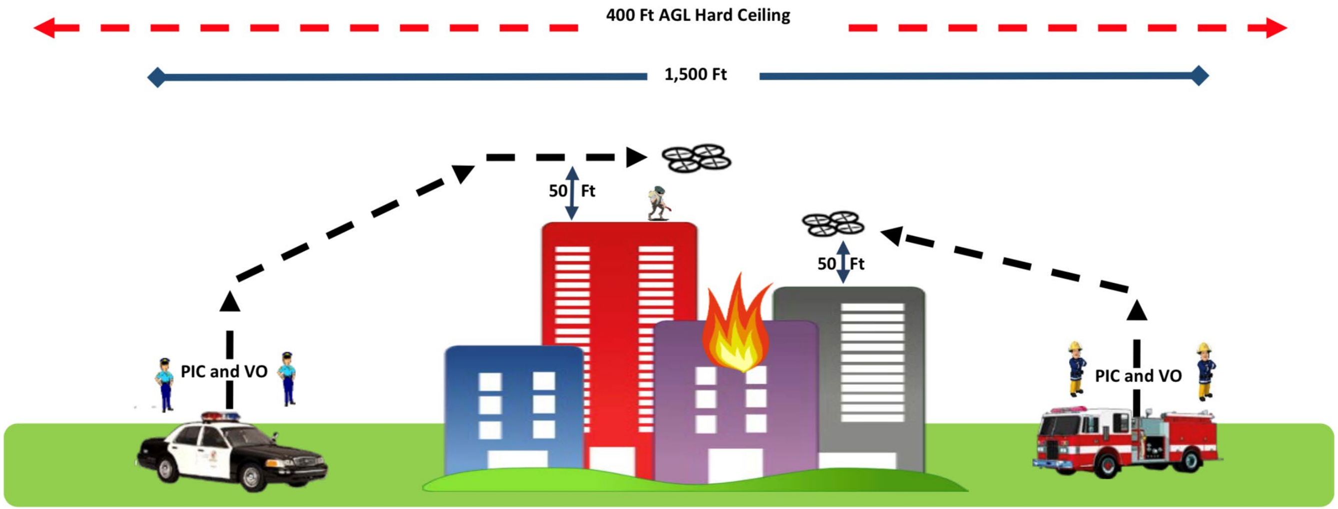
Public Safety Vehicle or Portable Tethered Drones – Continuous Power

- Can maintain constant overwatch – no batteries as tether provides power
- Quick setup – one button launch, one button land
- Switchable visual optic and thermal view



Tactical Beyond Visual Line of Sight Waiver *Requires a COA

Background: In a time of extreme emergencies to safeguard human life, first responders require the capability to operate their unmanned aircraft (UAS) beyond visual line of sight (BVLOS) to assess the operational environment such as a fire scene at a large structural fire, to conduct an aerial search on a large roof area for a burglary in progress, or to fly over a heavily forested area to look for a missing person (see diagram below for a visual perception). To support public UAS operators acting in an active first responder capacity, the FAA may approve "First Responder Tactical Beyond Visual Line of Sight" (TBVLOS) waivers to 14 CFR 91.113(b).



DRONE AS A FIRST RESPONDER (DFR)

*Requires a COA

Drone launches from rooftop at same time as 911 dispatch

CHULA VISTA POLICE DEPARTMENT - DRONE AS FIRST RESPONDER (DFR)

CHULA VISTA POLICE DEPARTMENT

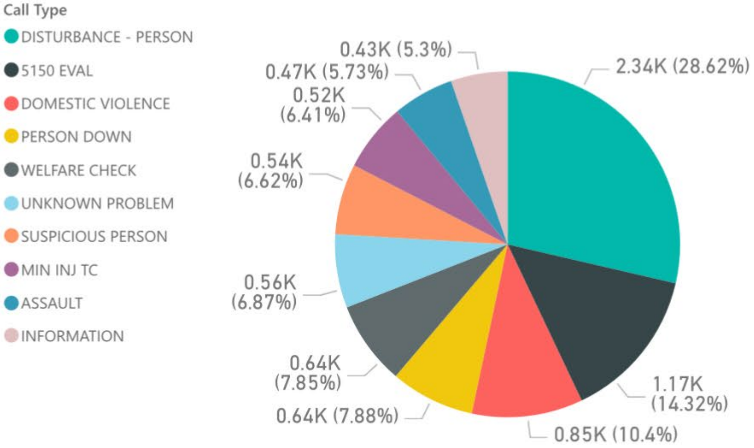
* Selected as part of the IPP on October 2018

* First program in the nation using Drones as a First Responder (DFR). See FAA site

* Current status: DFR Pilot Program currently based from CVPD HQ with limited flight range of about 1 mile radius

* Common use of drones in Chula Vista: Drones as first responders, documenting crime and accident scenes, searching for missing or wanted persons, fires, and evaluating damage after a major incident or natural disasters

TOP 10 CALLS RESPONDED WITH DFR ASSISTANCE



PLEASE SELECT A TIME FRAME

Y Q M
Year

2018 - 2024

2018 2019 2020 2021 2022 2023 2024

DFR ACTIVITY BY THE NUMBERS

TOTAL CALLS RESPONDED TO	18371
DFR ASSISTED ARRESTS	2508
DFR DEPLOYMENT AVOIDED DISPATCHING A PATROL UNIT	4171
DFR FIRST ON SCENE COUNT	13.72K
AVG RESPONSE TIMES - FIRST ON SCENE (IN SECONDS) *	94.16
AVG RESPONSE TIMES - ALL CALLS (IN SECONDS) *	111.89

* Response times from dispatch to arrival.

EARLIEST RESPONSE 10/23/2018 8:29:57 ...

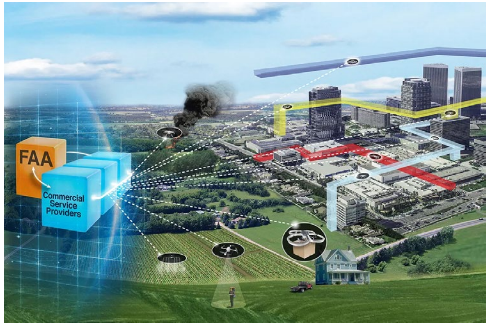
LATEST RESPONSE DATE/TIME 1/30/2024 1:27:58 PM

Public Safety UAS Programs 2023

- **There over 5000 public safety UAS Programs**
- **70% are law enforcement, 25% fire, 5% EM & SAR**
- Safer for Responders & Community
- Better Operational Effectiveness (Better Decisions)
- Real Time Situational Awareness
- A Major De-escalation Tool
- Flying with Part 107 & Certificate of Authorization (COA)*

What’s Next?

- BVLOS Rules – 1st Qtr 2024
- Autonomous Flight
- 1 Remote Pilot To Many Aircraft
- Drone Swarms
- Fully BVLOS Autonomous DFR
  - NARCAN to Scene
  - Defibrillator to Scene
- Artificial Intelligence
  - Analytics (search, damage assessment, predictive fire behavior, etc.)
  - Smart Cities & Integrated Systems
- Larger Aircraft w/Longer Flights
- Development of UTM



DRONERESPONDERS
Public Safety Alliance

DRONERESPONDERS.ORG

Register on the website
(it's FREE)

JOIN and access the largest online collection of Public Safety UAS documents (SOPs, Best Practices, Lessons Learned, Training Info and more)

DRONERESPONDERS.ORG

Contact Information

Fire Chief Charles L. Werner (Emeritus - Ret.)

Director, DRONERESPONDERS

Aviation Technology Advisor, Virginia Department of Aviation

Charles@droneresponders.org

Mobile: 434.825.5402

DRONERESPONDERS

Bart Ramaekers

Carma Police

PSCR 2024 - UAS Portfolio Workshop

February 7-8, 2024
Gaithersburg, MD, USA

Peter Monnens, Inspector
Bart Ramaekers, Superintendent

BART RAMAEKERS

SUPERINTENDENT

28 YEARS OF SERVICE

10 YEARS OF UAS PILOT

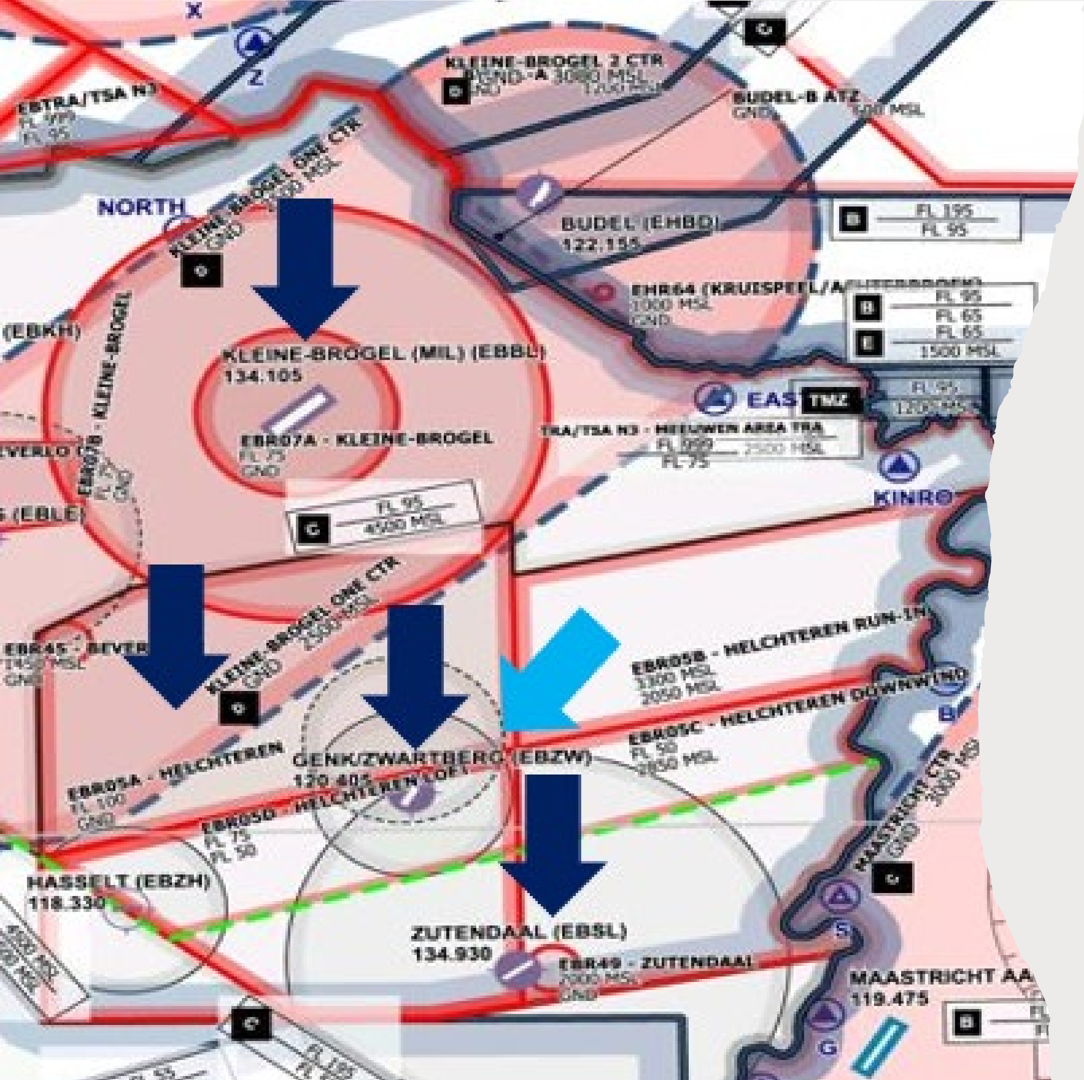
7 YEARS TRAINING EXPERIENCE

SENIOR LECTOR PLOT LIMBURG

Positioning of Belgium in Europe

Positioning of Province Limburg in Belgium

Positioning of Police Carma in Limburg



Live feed : CP-Ops + civil teams

BVLOS : 5 km (3,1 mi)

2 devices (DJI M30T – DJI M3T)

Mobile pilot

Deployment within 15 min.

100 % attendance

Low cost

- € 25,000/year cfr. helicopter

120 events/year

- more than 1200 since 2011

2024 : expecting + 300 deployments

Less damages and injuries

Quick intervention according standards

UAS in Europa

- 01/01/2021 : Introduction of European drone legislation

- Geozones : Specific rules for certain zones in each Member State

UAS use in Belgium – UAS State Operator

Ministerial circular from the Minister of the internal affaires

Police departments, fire brigades and civil protection

UAS use in policezone Carma

General

- GDPR (General Data Protection Regulation)
- DPIA (Data Protection Impact Assessment – Data Protection Officer)
    - Processing of the images
    - Purposes
    - Legal basis
    - Proportionality
    - Guarantees to avoid violations of fundamental rights
    - remedial measures

UAS use in
policezone Carma

Constitution

art. 15 Immunity of the property

-> Recording of the images

-> Making pictures

-> No in-flight recording

-> Unless necessary for the assignment !

Cfr. tracking of person/vehicle

UAS use in policezone Carma

Police Act

Visible use of a camera (CCTV, Drone, Picto)

Non-visible use of a camera

Processing of data

UAS use in Policezone Carma

Camera Act

Only filming of the intervention
(cfr streaming/recording)

inform staff in advance (briefing)

no police staff:
->only real-time images under supervision (events, joint dispatch)

only aimed at gathering information

->**NO**: racial or ethnic origin, religious or political background, trade union membership, sexual orientation, health status

UAS use in police zone Carma - risk mitigation

Before each flight

- Flight plan
- Risk analysis of the flight
- Permission (gouvernement/prosectors office)

During the flight

- Only UAS State Operator pilots
- Education and training
- Observing the sky
- Using the camera correctly/recording
- Live feed at CP-Ops/smartphone

After the flight

- Removing Micro-SD from the drone
- Saving images on a separate server
- Formatting Micro-SD
- Completing registers and flight logbooks

UAS use in police zone Carma - risk mitigation

Fleet

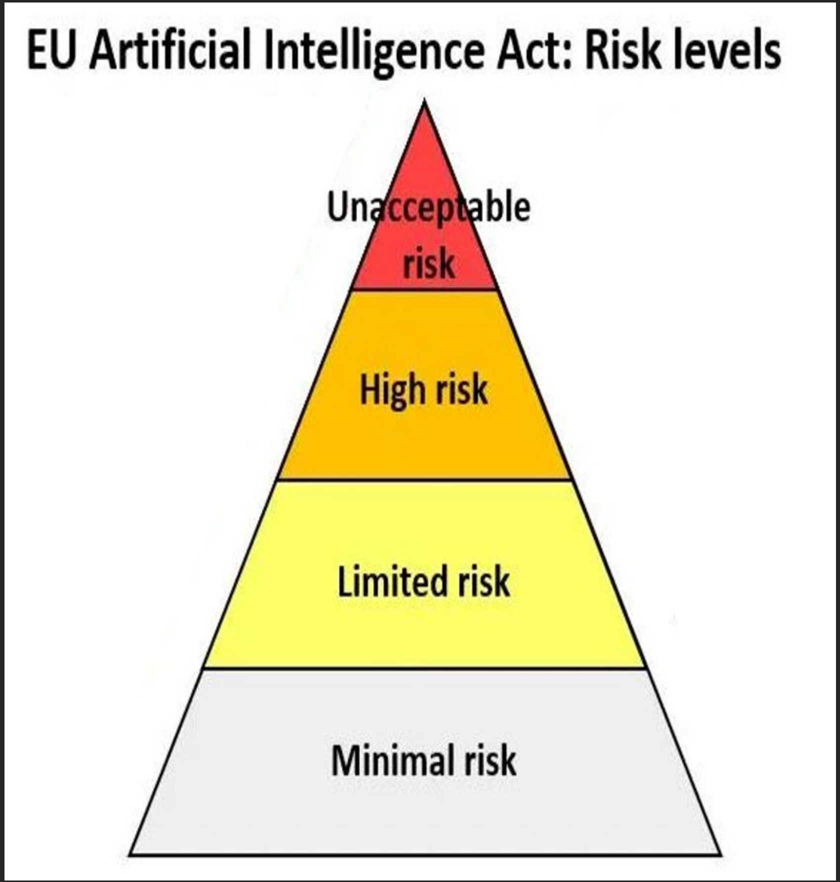
- DJI Mini 3 pro
- Dji Mavic 2 enterprice (2)
- DJI M210
- DJI Mavic 3T
- DJI M30T

Geopolitical sensitivities

! Updates!

- delete data from device
- return to factory settings
- perform update

AI ACT Regulation


EU Artificial Intelligence Act: Risk levels
Unacceptable risk
High risk
Limited risk
Minimal risk


EU A I ACT

EU AI ACT Cheat Sheet

Understand the world's first comprehensive AI law

THE BASICS

- **Definition of AI:** aligned to the recently updated OECD definition
- **Extraterritorial:** applies to organisations outside the EU
- **Exemptions:** national security, military and defence; R&D; open source (partial)
- **Compliance grace periods** of between 6-24 months
- **Risk-based:** Prohibited AI >> High-Risk AI >> Limited Risk AI >> Minimal Risk AI
- **Extensive requirements** for 'Providers' and 'Users' of High-Risk AI
- **Generative AI:** Specific transparency and disclosure requirements

PROHIBITED AI

- **Social credit scoring** systems
- **Emotion recognition** systems at work and in education
- AI used to **exploit people's vulnerabilities** (e.g., age, disability)
- **Behavioural manipulation** and circumvention of free will
- **Untargeted scraping of facial images** for facial recognition
- **Biometric categorisation systems** using sensitive characteristics
- Specific **predictive policing** applications
- **Law enforcement use of real-time biometric identification in public** (apart from in limited, pre-authorised situations)

HIGH-RISK AI

- **Medical devices**
- **Vehicles**
- **Recruitment, HR and worker management**
- **Education** and vocational training
- Influencing **elections and voters**
- **Access to services** (e.g., insurance, banking, credit, benefits etc.)
- **Critical infrastructure** management (e.g., water, gas, electricity etc.)
- **Emotion recognition** systems
- **Biometric identification**
- **Law enforcement, border control, migration and asylum**
- Administration of **justice**
- **Specific products** and/or **safety components** of specific products

KEY REQUIREMENTS: HIGH-RISK AI

- **Fundamental rights impact assessment** and **conformity assessment**
- Registration in **public EU database** for high-risk AI systems
- **Implement risk management** and **quality management** system
- **Data governance** (e.g., bias mitigation, representative training data etc.)
- **Transparency** (e.g., Instructions for Use, technical documentation etc.)
- **Human oversight** (e.g., explainability, auditable logs, human-in-the-loop etc.)
- **Accuracy, robustness and cyber security** (e.g., testing and monitoring)

GENERAL PURPOSE AI

- Distinct requirements for **General Purpose AI** (GPAI) and **Foundation Models**
- **Transparency** for all GPAI (e.g., technical documentation, training data summaries, copyright and IP safeguards etc.)
- Additional requirements for **high-impact models with systemic risk**: model evaluations, risk assessments, adversarial testing, incident reporting etc.
- **Generative AI:** individuals must be informed when interacting with AI (e.g., chatbots); AI content must be labelled and detectable (e.g., deepfakes)

PENALTIES & ENFORCEMENT

- Up to **7% of global annual turnover** or €35m for prohibited AI violations
- Up to **3% of global annual turnover** or €15m for most other violations
- Up to **1.5% of global annual turnover** or €7.5m for supplying incorrect info
- **Caps on fines for SMEs and startups**
- **European 'AI Office'** and **'AI Board' established** centrally at the EU level
- **Market surveillance authorities** in EU countries to enforce the AI Act
- **Any individual can make complaints** about non-compliance

Based on publicly-available information following the political agreement reached by the EU institutions on 8 December 2023

Implementing AI Police Carma

Counting participants

Recognizing patterns in the crowd

Recognizing suspicious circumstances

Recognizing criminal acts

‘The scary thing about the future...

there will be tiny cameras everywhere, and they'll be flying around like mosquitoes and drones.

That will be bad.

Drones are scary.

You can't reason with a drone.’

Matt Groening

PETER MONNENS

INSPECTOR OF POLICE

36 YEARS OF SERVICE

12 YEARS OF UAS PILOT

7 YEARS TRAINING EXPERIENCE

SENIOR LECTOR PLOT LIMBURG

The Future is ours

'CARMA strives to maintain and strengthen its leading position in the dynamic (police) landscape by continuing to take on the role of innovator in a search for the use of new technologies and tactics in our police environment.'

PROOF OF CONCEPT – PZ CARMA – GENK - BELGIUM

Legal obligations

- Formating DPIA and SORA cfr. European laws
- Cooperation DGLV (Belgian FAA)
- Corps directives
- Contracts with suppliers

POC policezone Carma – Genk 2024

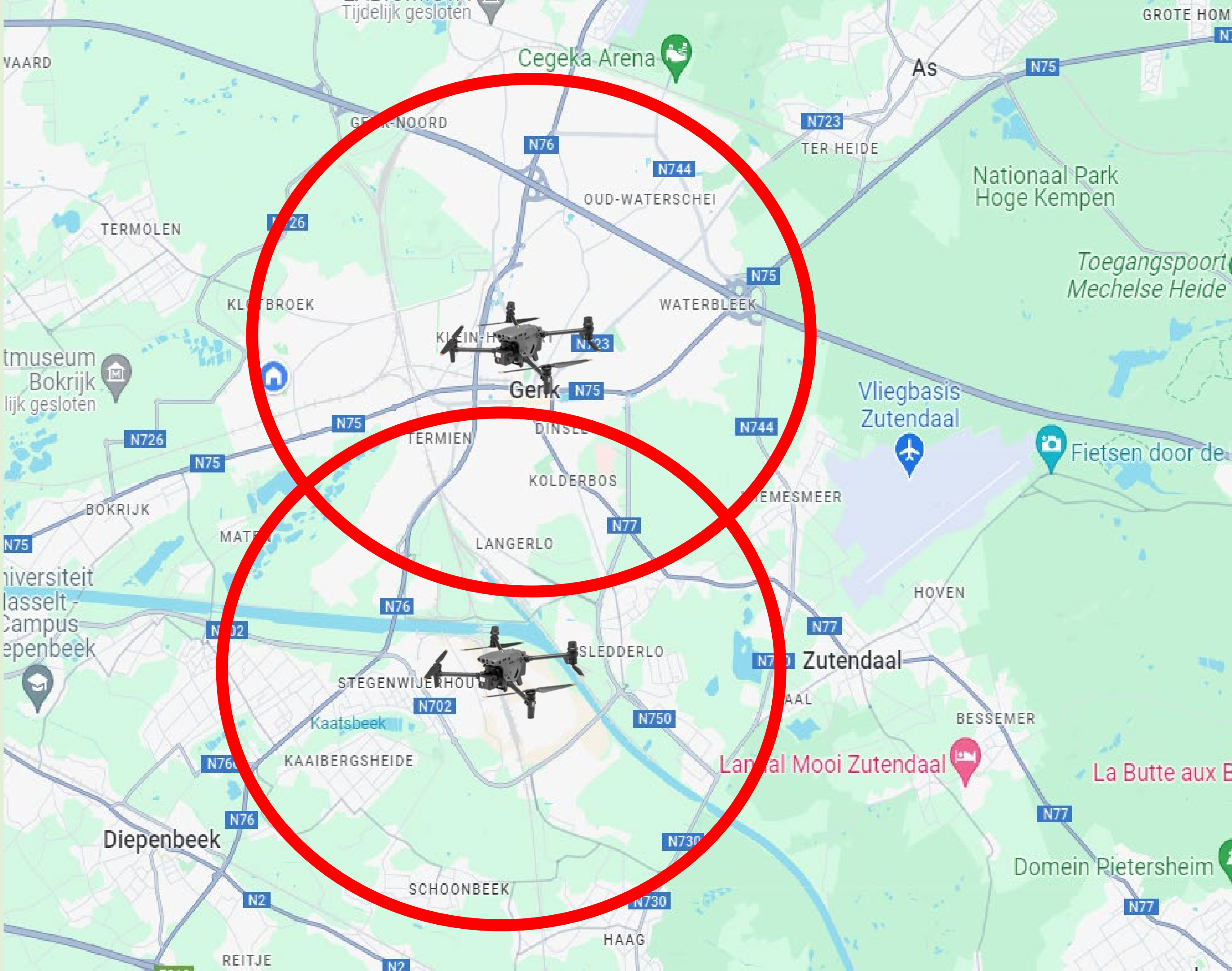
2 test setups

2 DJI Drone in a box, type M30T

Control from 1 central point

AI input

Evaluation August ‘24



POC policezone Carma – Genk 2024 - …

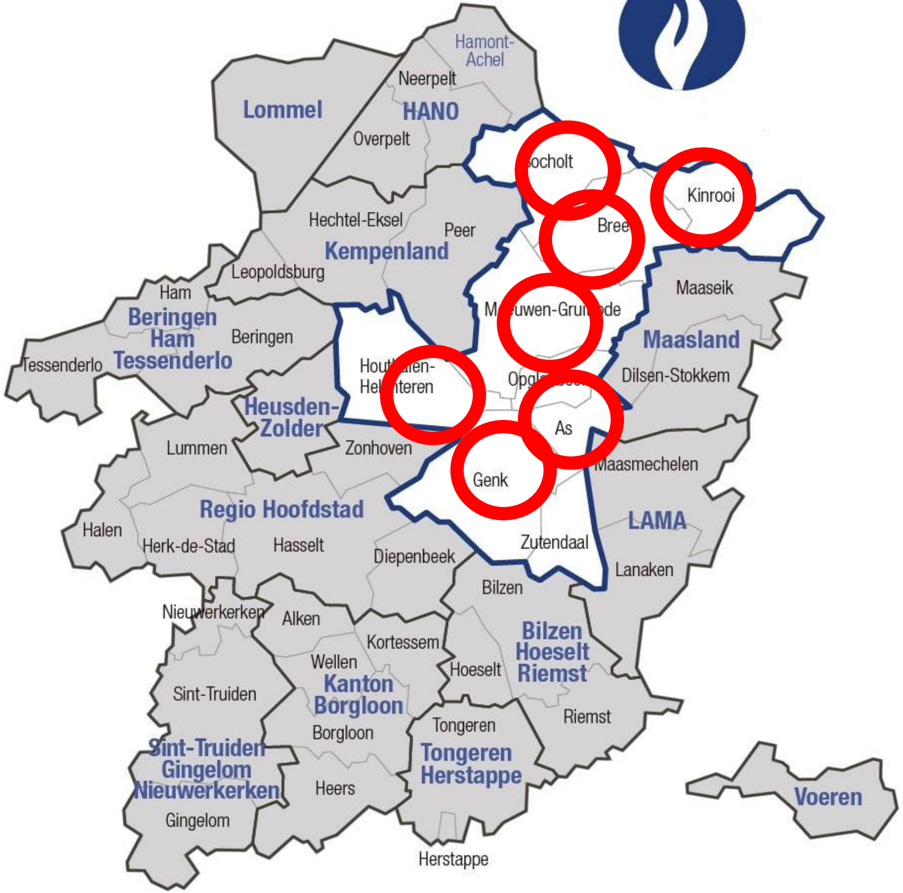
8 setups

2 DJI Drone in a box, type M3T

Control from 1 central point

AI input

Our entire Province ?



airhub

PIXELVISION

AERIALSOLUTIONS
Industrial UAV systems

PARTNERS

Politie
CARMA

Thank you !

bart.ramaekers@police.belgium.eu

peter.monnens@police.belgium.eu

Jason Day

Texas Department of Public Safety

Texas Department of Public Safety

CYBERSECURITY & AI RISK MANAGEMENT
IN PUBLIC SAFETY UAS OPERATIONS

TEXAS DPS UAS Program

- 320 remote pilots
- 350 unmanned aircraft
- 52,000 flights in 2023
- 150,000+ total flights since 2017

TEXAS DPS UAS Missions

- Accident reconstruction
- Border operations
- Tactical overwatch
- Fire mapping
- Search & Rescue
- Tower inspections
- Infrastructure photogrammetry
- Training documentation

Teams strategically located across the state

IDENTIFY

& characterize the risk

MANAGE

the risk through policy

COMMUNICATE

the risk to stakeholders

AIRISK

- False identification/positive
- Overconfidence in technology
- Pilot complacency
- Loss of human in the loop

CYBERRISK

- Loss of command & control
- Compromised mission
- Data privacy
- Inaccurate record keeping

IDENTIFY >


CNN
+ Follow
FBI and CISA warn companies to be wary of using Chinese-made drones over national security risks
Story by By Natasha Bertrand, CNN • 1w
U.S. Senators Take Another Shot at DJI: the
“Countering CCP
Act”
Posted By: Miriam McNabb
Cybersecurity Guidance: Chinese-Manufactured UAS
Publish Date: January 17, 2024
RELATED TOPICS:
AND ADVISORIES
Top FCC Official Calls For Ban of DJI Drones, Citing National Security Risk
OCT 20, 2021
JARON SCHNEIDER
Today Florida’s Chinese drone ban
into
effect, and police agencies are not
Seth Kurkowski | Apr 5 2023 - 10:14 am PT
5 Comments
Statewide Security Plan for Prohibited Technologies
.PDF (176.74 KB)
Statewide Security Plan for Prohibited Technologies
Tool/Template Last Updated: February 6, 2023
To protect the State’s sensitive information and critical infrastructure from technology that poses a threat to the State of Texas, this plan outlines objectives for each agency.

AIRISK

- Larger testing data sets
- Build redundancy into policy
- Hold remote pilots accountable
- Effective safety management program

CYBERRISK

- 3rd party vetted software
- Off agency network for updates
- Collaboration with agency Cyber division

IDENTIFY > **MANAGE >**

AI&CYBERRISK

- Effective collaboration
- Public/Private partnerships
- Texas Public Safety UAS Working Group
- Conferences & Summits
- Hugs & High Fives!

IDENTIFY > MANAGE > COMMUNICATE >

Jason L. Day

Director of Unmanned Aircraft

Texas Department of Public Safety

Aircraft Operations Division

jason.day@dps.texas.gov

512.221.6556

Resume at 10:45 am
(in 15 minutes)

A 15-minute Q&A will follow the break. Please submit questions via the Google Form through the QR code on your handout or through this link: https://bit.ly/UASWorkshopQandA

Break


Q&A
NIST
PUBLIC SAFETY
COMMUNICATIONS
RESEARCH

Resources, Regulation, Accreditation

- Billy Bob Brown Jr
  DHS CISA
- Stephen Luxion
  ASSURE
- Preet Bassi
  Center for Public Safety Excellence

Billy Bob Brown Jr.
Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

PUBLIC SAFETY, ARTIFICIAL INTELLIGENCE, & UNCREWED AERIAL SYSTEMS (UAS)

Executive Assistant Director Billy Bob Brown
February 28, 2024

CISA Roadmap for Artificial Intelligence

Source: CISA Roadmap for Artificial Intelligence

Public Safety & UAS

Benefits:

- Cost Savings
- Ability to Access Remote/ Dangerous Locations
- Force Multiplier
- Rapid Response

Challenges:

- Surveillance and Public Perception Concerns
- Flight Authorization and Limitations
- Staffing and Training
- Data Usage and Overload
- Reliability
- Cybersecurity

To earn more about the use of UAS, read the Public Safety Uncrewed Aircraft System Resource Guide

Resources

[Cybersecurity Guidance Chinese-Manufactured UAS]() *(Jan 2024)*

[Public Safety Uncrewed Aircraft System (UAS) Resource Guide]()

[Responding to Drone Calls:
Guidance for Emergency Communications Centers]()

Resources

[Public Safety Communications and Cyber Resiliency Toolkit]

cisa.gov/resources-tools/resources/communications-and-cyber-resiliency-toolkit

For more information:
www.cisa.gov

Questions?
Email: publicsafetycomms@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Stephen Luxion

Alliance for System Safety of UAS through Research Excellence (ASSURE)

The FAA's Center of Excellence for UAS Research

ASSURE

Alliance for System Safety of UAS through Research Excellence

Big Picture Overview
NIST PSCR UAS Workshop
February 7-8, 2024

Steve "Lux" Luxion, Colonel (USAF-Retired)

Executive Director, ASSURE

SLuxion@assure.msstate.edu

The FAA's Center of Excellence for UAS Research

ASSURE

Alliance of System Safety of UAS for Research Excellence

ASSURE's Strategic Framework

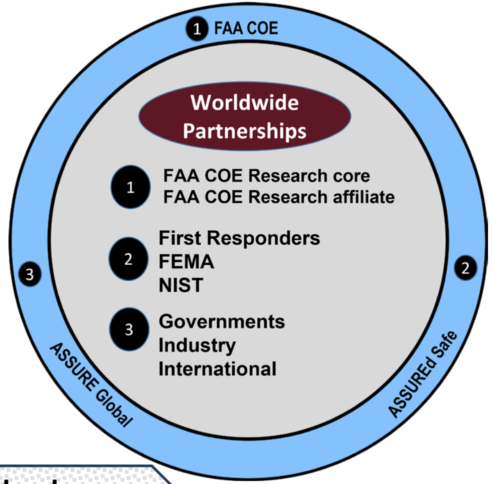
ASSURE is divided into three key sectors.

1 ***FAA Center of Excellence***

2 ***ASSUREd Safe***
(Training, Educating, and Certifying First Responders)

3 ***ASSURE Global***
(Independent Partnerships with Industries and Governments worldwide

Current Funding per Sector



1

FAA COE
$14M (per year FY18-22)
- 78 Total Projects
  30 active, 40 completed, 4 proposed

$70M Active Projects
$180M Total Level of Effort Since Inception

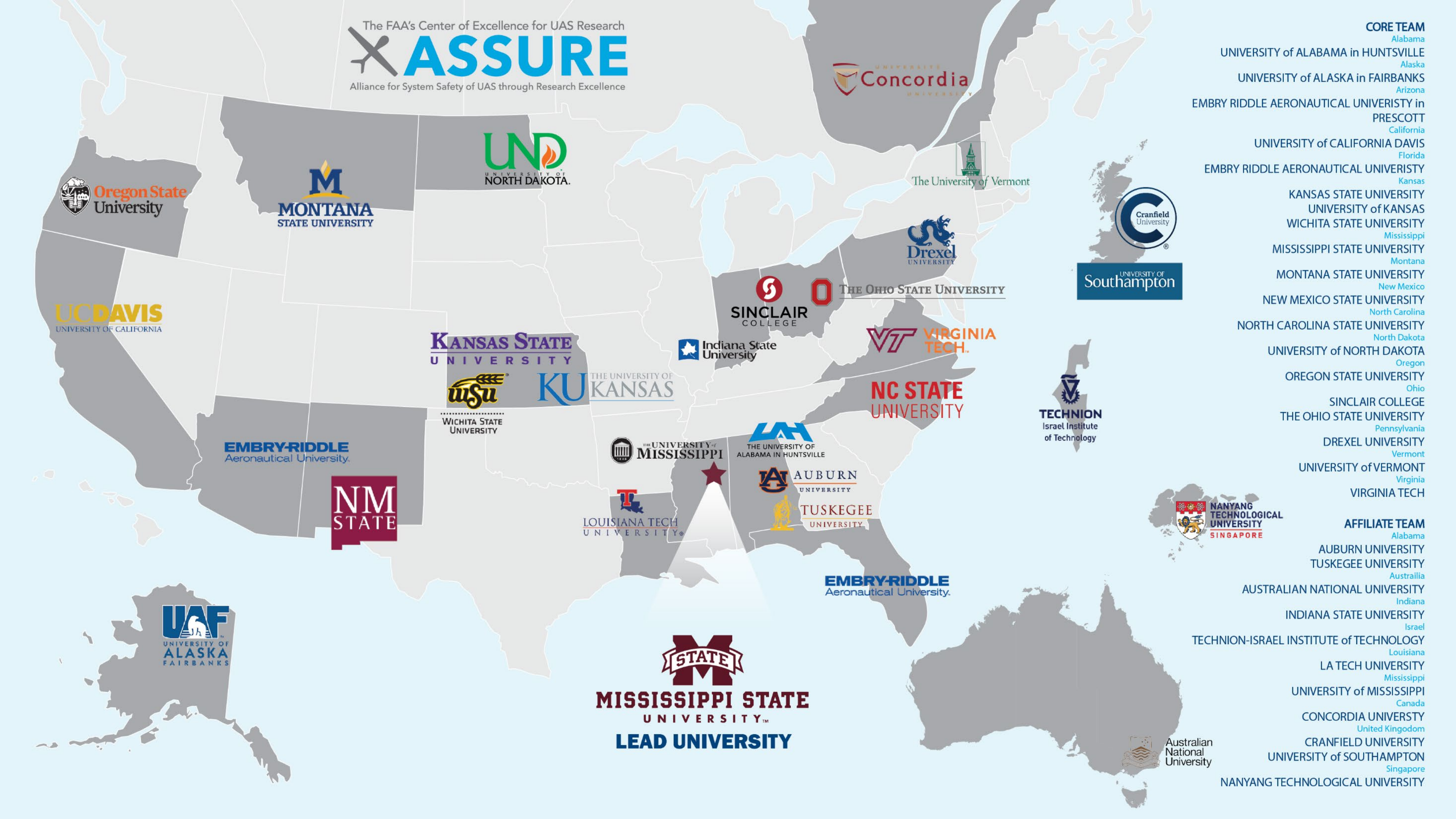
Non-COE/ASSURE Global

2

ASSUREd Safe
$6M FEMA (FY21-24)
$4M NIST

3

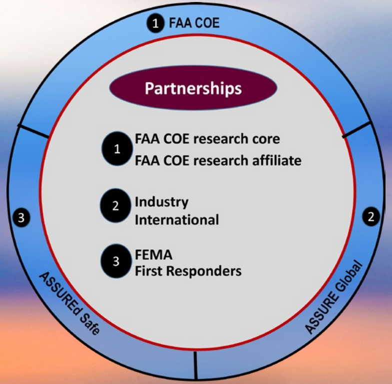
ASSURE Global
$4.6M (to date)
9 Total Projects


The FAA's Center of Excellence for UAS Research
ASSURE
Alliance for System Safety of UAS through Research Excellence
Concordia University
The University of Vermont
UND University of North Dakota
Oregon State University
Montana State University
Drexel University
The Ohio State University
Sinclair College
UC Davis University of California
Kansas State University
Indiana State University
Virginia Tech
The University of Kansas
Wichita State University
NC State University
The University of Mississippi
The University of Alabama in Huntsville
Embry-Riddle Aeronautical University
Auburn University
Tuskegee University
NM State
Louisiana Tech University
Embry-Riddle Aeronautical University
UAF University of Alaska Fairbanks
Mississippi State University
LEAD UNIVERSITY
Cranfield University
University of Southampton
Technion Israel Institute of Technology
Nanyang Technological University Singapore
Australian National University
CORE TEAM
Alabama
UNIVERSITY of ALABAMA in HUNTSVILLE
Alaska
UNIVERSITY of ALASKA in FAIRBANKS
Arizona
EMBRY RIDDLE AERONAUTICAL UNIVERISTY in PRESCOTT
California
UNIVERSITY of CALIFORNIA DAVIS
Florida
EMBRY RIDDLE AERONAUTICAL UNIVERISTY
Kansas
KANSAS STATE UNIVERSITY
UNIVERSITY of KANSAS
WICHITA STATE UNIVERSITY
Mississippi
MISSISSIPPI STATE UNIVERSITY
Montana
MONTANA STATE UNIVERSITY
New Mexico
NEW MEXICO STATE UNIVERSITY
North Carolina
NORTH CAROLINA STATE UNIVERSITY
North Dakota
UNIVERSITY of NORTH DAKOTA
Oregon
OREGON STATE UNIVERSITY
Ohio
SINCLAIR COLLEGE
THE OHIO STATE UNIVERSITY
Pennsylvania
DREXEL UNIVERSITY
Vermont
UNIVERSITY of VERMONT
Virginia
VIRGINIA TECH
AFFILIATE TEAM
Alabama
AUBURN UNIVERSITY
TUSKEGEE UNIVERSITY
Austrailia
AUSTRALIAN NATIONAL UNIVERSITY
Indiana
INDIANA STATE UNIVERSITY
Israel
TECHNION-ISRAEL INSTITUTE of TECHNOLOGY
Louisiana
LA TECH UNIVERSITY
Mississippi
UNIVERSITY of MISSISSIPPI
Canada
CONCORDIA UNIVERSITY
United Kingodom
CRANFIELD UNIVERSITY
UNIVERSITY of SOUTHAMPTON
Singapore
NANYANG TECHNOLOGICAL UNIVERSITY

1

ASSURE FAA COE

Research Capabilities



Related Work – Highlights

- Public Safety – Disaster Prep/Recovery
- Cyber Security – Oversight
- C-UAS – Safety to the NAS
- Beyond Visual Line of Sight Enablers
  - Detect & Avoid (DAA)
  - Right-of Way Rules
  - Shielding
  - Increase sUAS Conspicuity
- GPS & ADS-B Risks for UAS
- Multi-Aircraft Control
- Standards V/V (Remote ID, Detect & Avoid…)

Preet Bassi

Center for Public Safety Excellence

CPSE

Center for Public Safety Excellence

Fire and Emergency Service Regulatory Overview

Preet Bassi, CAE

Chief Executive Officer
Center for Public Safety Excellence

Environmental Context

Regulatory Impact

Mandates vs. Influence

- Minimal Federal Requirements
- Moderate State Oversight
- Significant Local Control

Fire and Emergency Service Departments

Organized at the local level

Function within cities or counties or operate as independent entities

Staffed as career, combination, or volunteer systems

Services provided:

- Firefighting: Structural, Wildfire, Marine and Shipboard, Aviation
- Emergency Medical Services, Technical Rescue, Hazardous Materials
- Domestic Preparedness
- Prevention, Public Education, Investigation

Fire and Emergency Service Organizations

MEMBERSHIP ORGANIZATIONS

STANDARDS DEVELOPMENT ORGANIZATIONS

CONFORMITY ASSESSMENT BODIES

TRAINING PROVIDERS

PRIVATE-SECTOR PRODUCT AND SERVICE VENDORS

Center for Public Safety Excellence Overview

CPSE Overview

The Center for Public Safety Excellence® (CPSE®) is a not-for-profit 501(c) (3) corporation.

CPSE helps high-performing fire and emergency service departments and professionals in their efforts to continuously improve. We do that in three main ways:

1. Fire and emergency service department accreditation
2. Credentialing fire and emergency service professionals
3. Education programs

ACCREDITATION

Fire department accreditation is a process in which departments undergo a thorough self-assessment focused on identifying strengths and weaknesses using data and information to continuously improve.

CFAI Commission on Fire Accreditation International®

311 Accredited Agencies

- 13% of US population protected by accredited agencies
- 19% of Canadian population protected by accredited agencies
- 82,000 total personnel

205 agencies working on accreditation

CREDENTIALING

Credentialing fire and emergency service professionals instills the principles of life-long learning and self-accountability and help them grow and plan for a successful career.

CPC Commission on Professional Credentialing®

3,353 Credentialed Officers

- 1,864 Chief Fire Officers
- 706 Fire Officers
- 237 Fire Marshals
- 227 Chief Training Officers
- 185 Chief EMS Officers
- 34 Public Information Officers

CURRENT STATE:
UAS, AI, CYBERSECURITY

UAS – NFPA 2400

- Details the minimum requirements for the safe operation, deployment, and implementation of sUAS including organization program criteria and considerations, professional qualifications for safety personnel, and elements of a maintenance program.
- Risk Assessment focuses on:
  - "The evaluation of the relative danger sUAS operations when taking into consideration mission objectives and goals, sUAS, professional qualification of the RPIC and visual observer, operational readiness of the crew, weather conditions, environmental conditions, regulatory requirements, potential hazards, and operations conditions.

Fire and Emergency Service & AI

Limited applications

Early tests in

- Wildfire
- Administration
- Data Mining

Fire and Emergency Service & Cybersecurity

Publications

- International Association of Fire Chiefs
  - Protecting Against Cyberattacks: A guide for Public Safety Leaders
- Multiple publications focusing on cybersecurity of systems

Professional Qualifications

- Existing standards focus on:
  - Technical skills of conducting a task or
  - Supervisory skills of being a higher-ranking officer
- NFPA 1022 focuses on:
  - Data Analysis
  - GIS Analysis
  - Business Analysis
  - Data and Analytics Management

CURRENT STATE

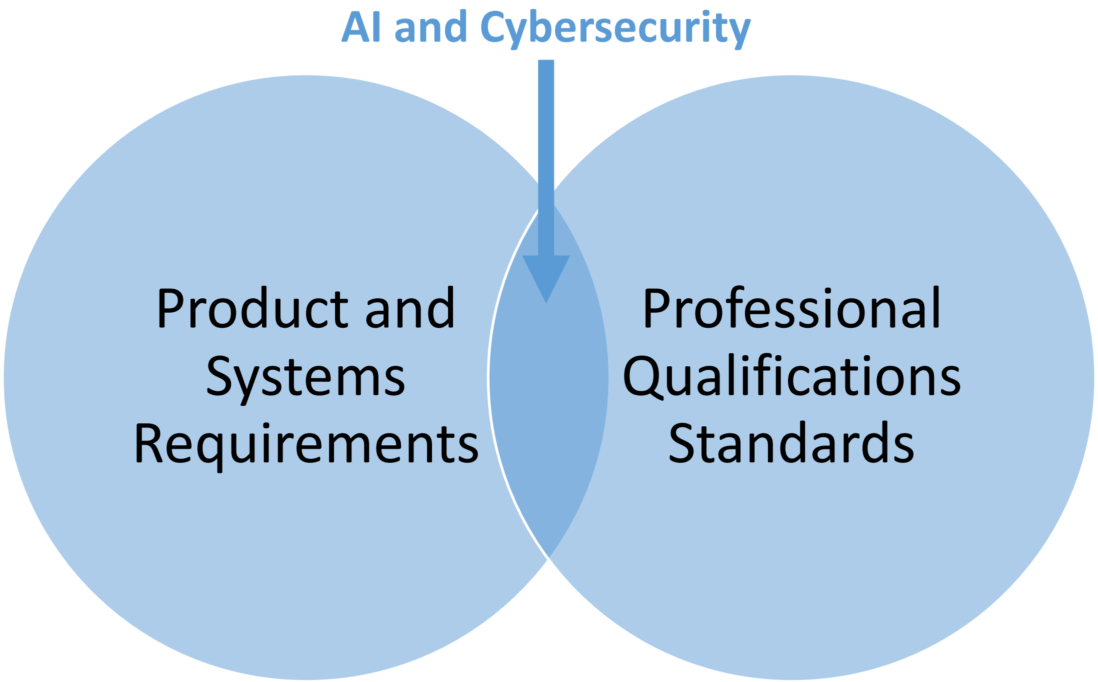
UAS Technical Operating Skills Requirements

AI and Cybersecurity Articles

Data Analysis Skills Requirements

UAS Procurement Articles

OPTIMAL STATE



Implementation Progression

Connect with CPSE

www.cpse.org
pbassi@cpse.org
703-691-4620
@CtrPubSafExc
CenterforPublicSafetyExcellence
center-for-public-safety-excellence

CPSE

Center for Public Safety Excellence

Cybersecurity and AI

- John Beltz
  NIST PSCR
- Donald Harriss
  NIST PSCR
- Jesse Dunietz
  NIST ITL
- Apostol Vassilev
  NIST ITL

John Beltz

NIST PSCR

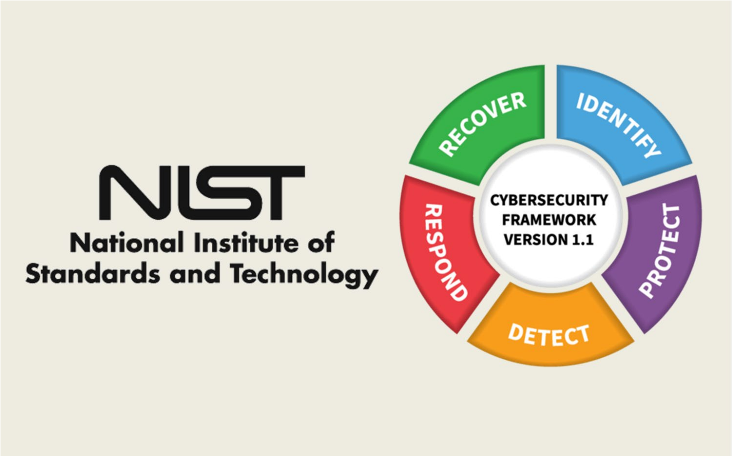
PUBLIC SAFETY COMMUNICATIONS RESEARCH

UNCREWED AIRCRAFT SYSTEMS

Cybersecurity Framework (CSF) 2.0

John Beltz

NIST PSCR Cybersecurity Lead



The NIST Cybersecurity Framework 2.0

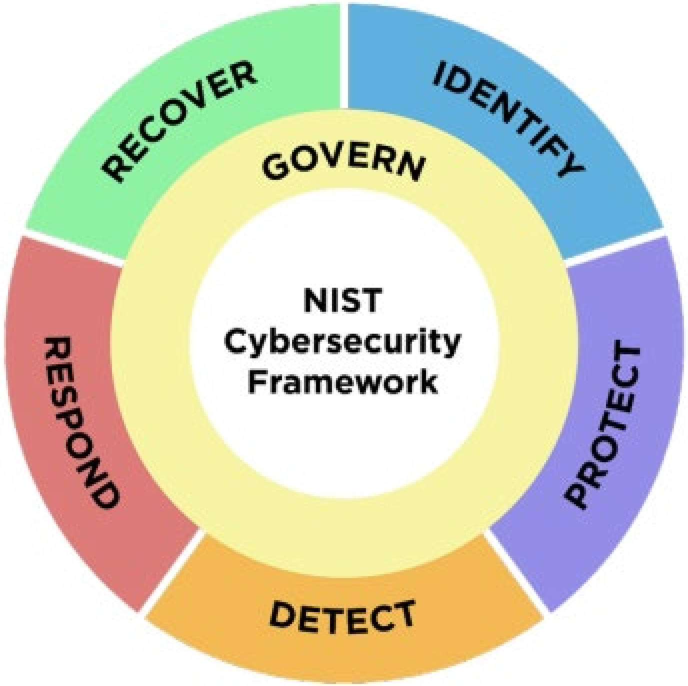
Initial Public Draft

National Institute of Standards and Technology

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.29.ipd

August 8, 2023

- Document and online tools
- Guidelines, best practices, and standards
- Identification of security and privacy controls needed to manage cybersecurity risks
- Common language for understanding, managing, and expressing cybersecurity risk, both internally and externally
- Flexible for size, sector, maturity



**CSF Functions as a wheel because all Framework Functions relate to one another and govern applies to all function

Govern: Establish and monitor the organization's cybersecurity risk management strategy

- **Identify:** What are we protecting?
- **Protect:** Safeguards to ensure delivery of services
- **Detect:** Identification of cybersecurity events
- **Respond:** Action regarding a detected incident
- **Recover:** Restoring capabilities or services

Additional Resources to Support Functions

Informative References are standards, guidelines, regulations, and other resources to help inform how an organization achieves the functions

- UAS Laws and regulations (FAA Regulations)
- NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)
- NIST SP 800-53 (5) Security and Privacy Controls for Information Systems and Organizations
- CJIS Security Policy
- Nist provides an Informative Reference Catalog

Implementation Examples provide notional examples of action-oriented steps to help achieve the desired outcomes in addition to the guidance provided by Informative References.

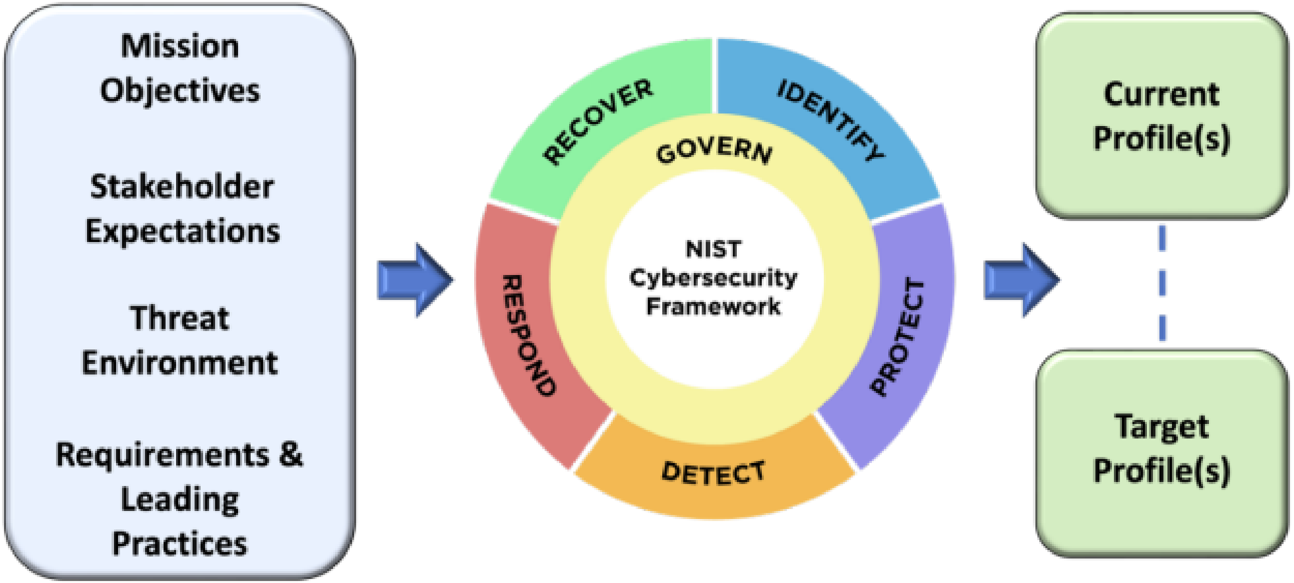
The following are links to each of the CSF 2.0 Function tables with Implementation Examples:

Table 1. **GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy**
Table 2. **IDENTIFY (ID): Help determine the current cybersecurity risk to the organization**
Table 3. **PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk**
Table 4. **DETECT (DE): Find and analyze possible cybersecurity attacks and compromises**
Table 5. **RESPOND (RS): Take action regarding a detected cybersecurity incident**
Table 6. **RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident**

Table 1. GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy

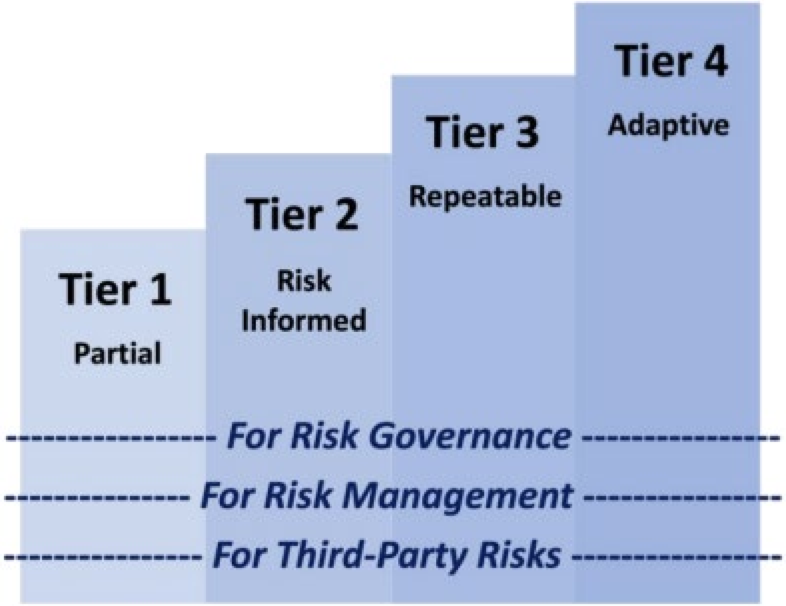
Category	Subcategory	Implementation Examples	Informative References
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)			
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission	

Current Profile to Target Profile

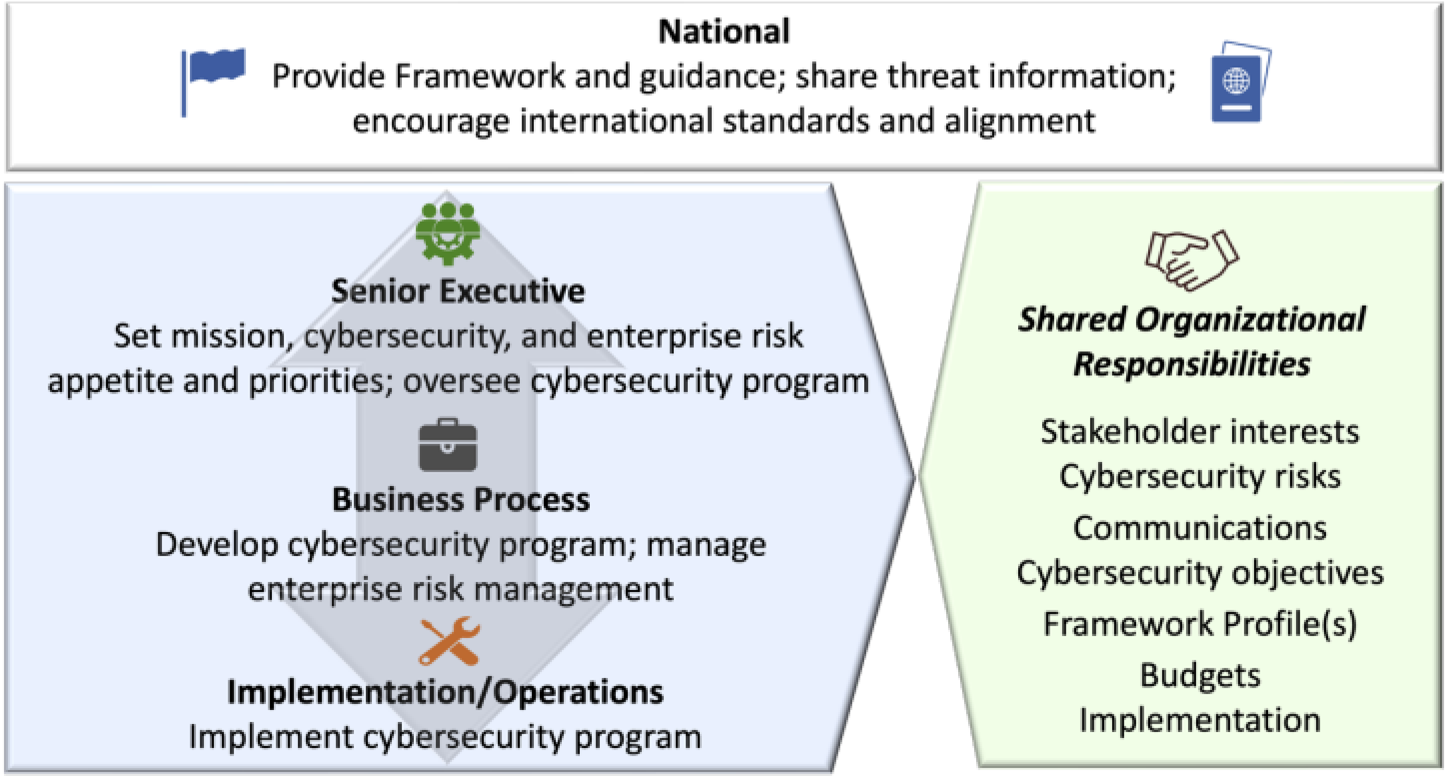


Framework Tiers

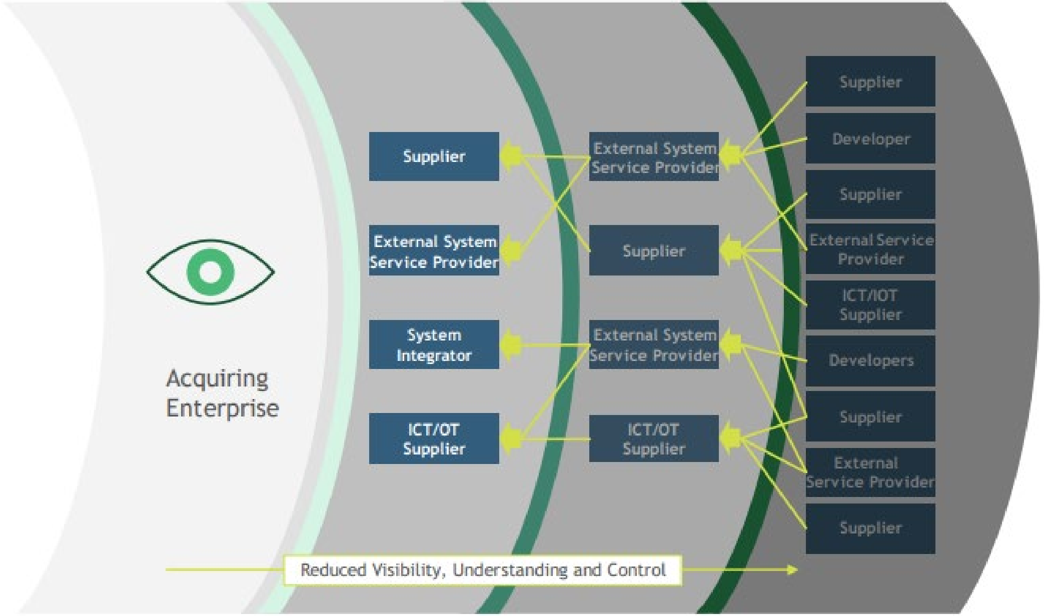
Determine the appropriate Tier to ensure the target profile meets the risk management strategy



Communication is Imperative



Managing Cybersecurity Risk in Supply Chains With the Framework



C-SCRM - Cybersecurity Supply Chain Risk Management

Integration with other Frameworks

- NIST Artificial Intelligence Risk Management Framework (AI RMF)
- Privacy Framework: NIST Privacy Framework
- Integrating Cybersecurity and Enterprise Risk Management
- Zero Trust Architecture
- NIST Cybersecurity for IoT Program

AI Security Controls

- AI is an application that requires securing as well as a tool to provide security

- AI can supplement and provide enhancement for security analyst

- Detect threats

- AI applications still require security and privacy controls

Donald Harriss

NIST PSCR

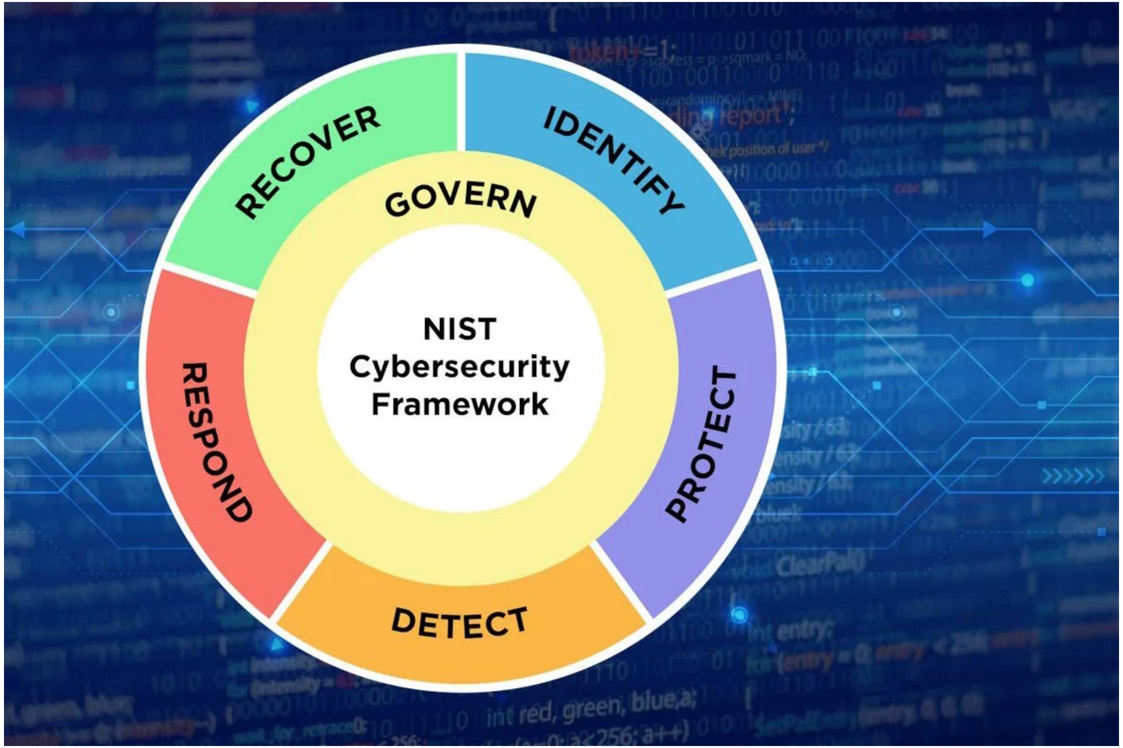
NIST PUBLIC SAFETY COMMUNICATIONS RESEARCH

UNCREWED AIRCRAFT SYSTEMS

Security and Privacy Controls for Information Systems

Don Harriss

NIST PSCR UAS Technical Lead

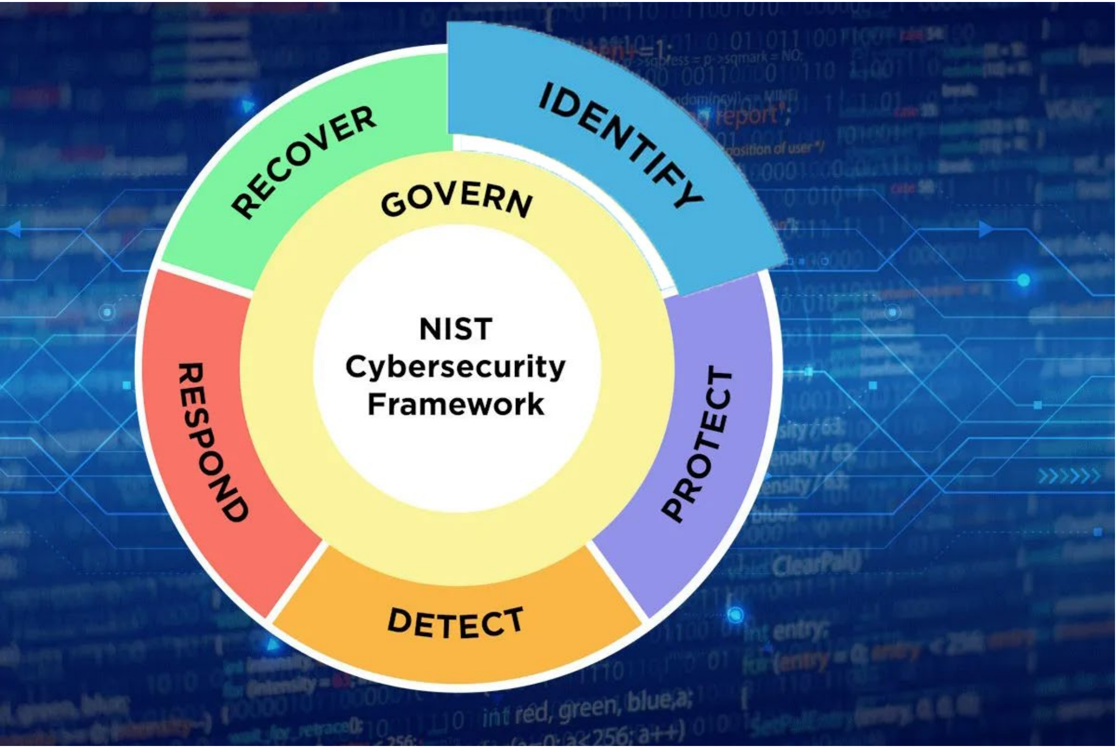


- CFS Functions Correlation to Security and Privacy Controls for Information Systems and Organizations NIST SP 800-53
- Supports the identification of security and privacy controls needed to manage risk
- Meets current and future protection needs
- Identify - Protect - Recover

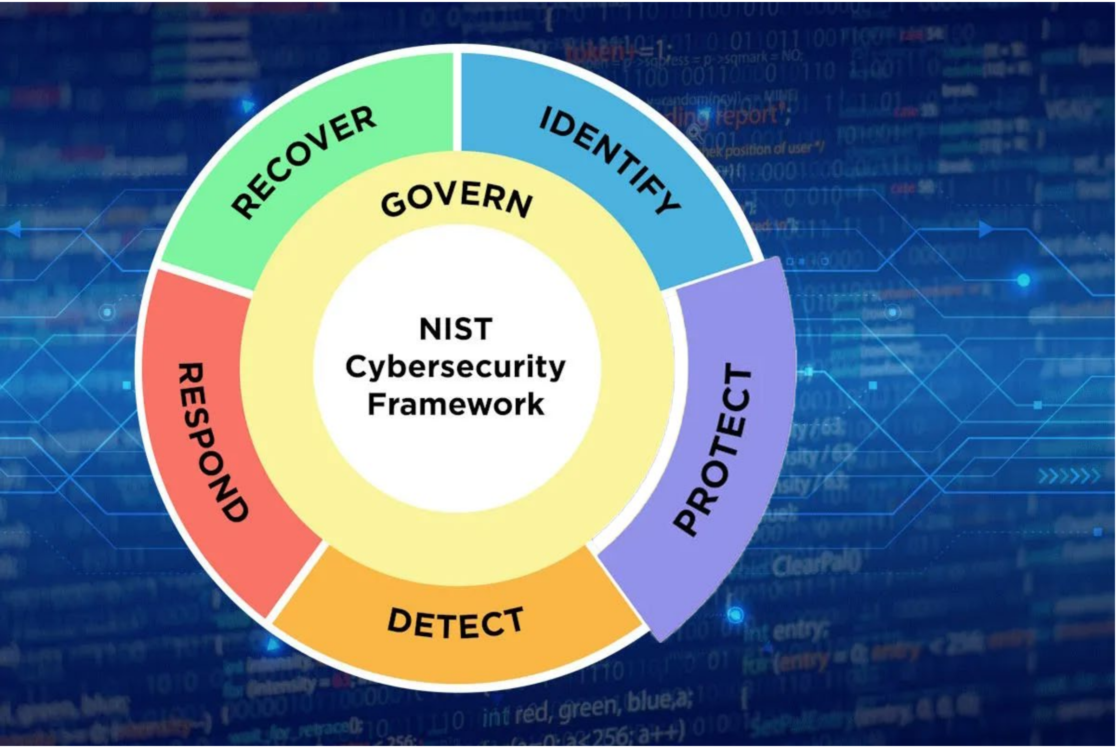
ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Security and Privacy Control Families,
NIST SP 800-53

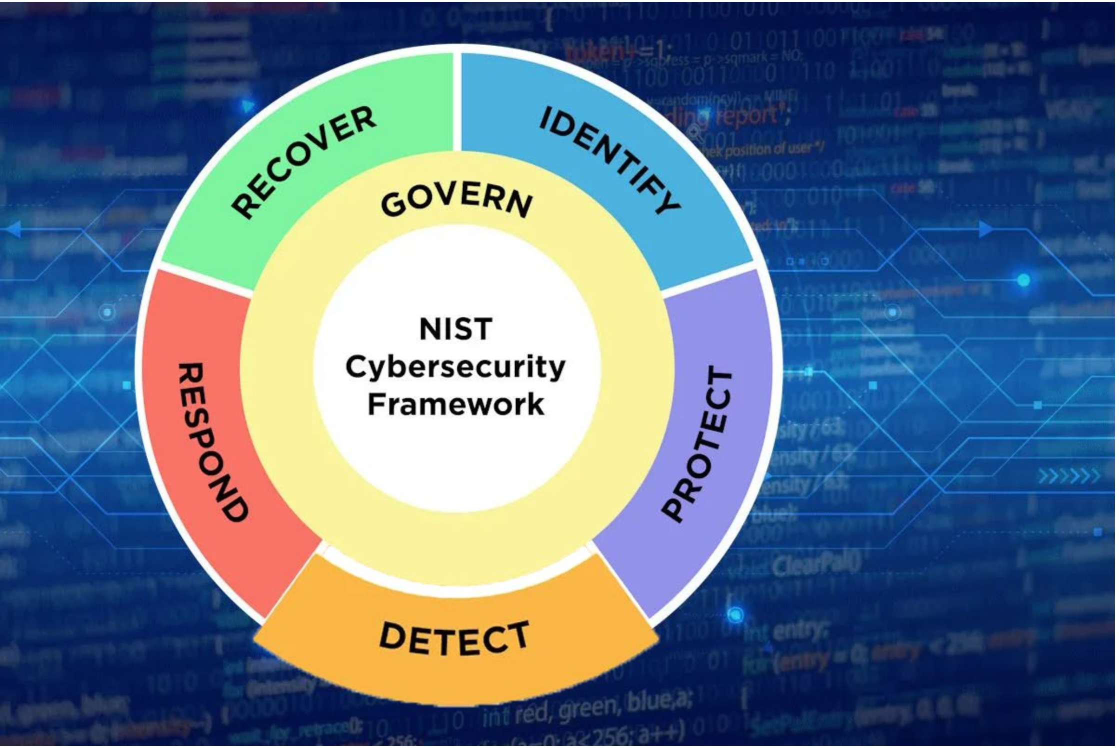
- Each family contains base controls and enhancements to provide greater protection integrity
- A control contains definitions and high-level technical discussions of the control
- Defines implementation role responsibilities and approaches
- Controls are agnostic to specific systems



- Auditing known assets
- Risk Assessment
- Supply Chain Risk Management
- Sensitive Information
- Physical and Cyber Assets
- Improvements
- Contingency Planning



- Access Controls
- Identification and Authentication
- Platform Security
- Data Protection
- Maintenance
- Technology Resilience
- Awareness and Training
- Configuration Management
- System Integrity



- Audit and Accountability
- Authorization and Monitoring
- Event Analysis

Secure Configuration

UAS and AI Implications

- Vetting of applications and software sources
- Hardware and software trusted supply chain
- Secure on-premise and cloud assets
- Secure credentialing databases
- Data protection
- Physical asset security

AI Cybersecurity Applications

Identification of People - Identity Management

Identification of Devices

Credentialing Mechanisms

Federation

AI Security Controls

- AI is an application that requires securing as well as a tool to provide security
- AI can supplement and provide enhancement for security analyst
- Detect threats
- AI applications still require security and privacy controls


Thank You
NIST
PUBLIC SAFETY
COMMUNICATIONS
RESEARCH

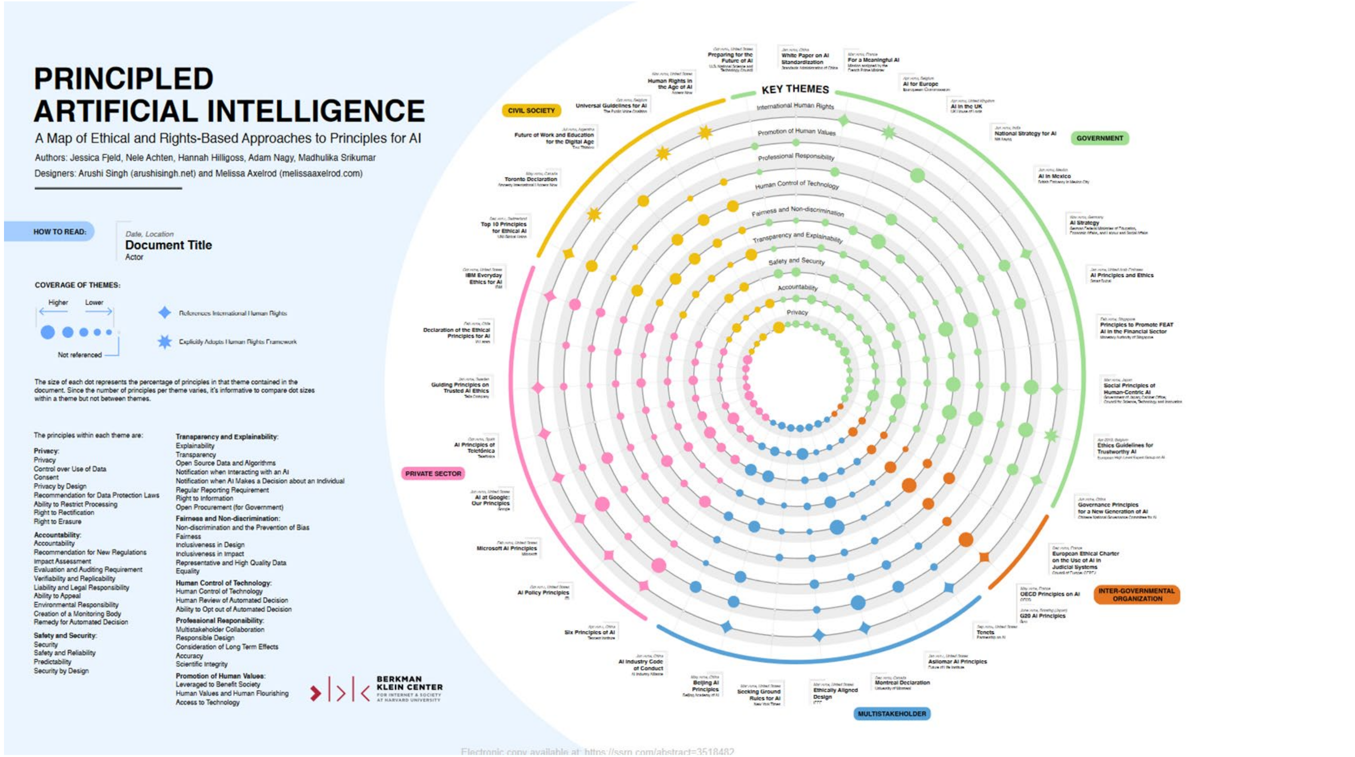
Jesse Dunietz

NIST ITL

The Artificial Intelligence Risk Management Framework (AI RMF 1.0)

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

As risks from AI became more apparent, many frameworks of principles emerged—but they remained too high-level for implementers.



The AI RMF offers voluntary guidance to operationalize principles for AI governance into concrete targets and actions.

NIST

Table 1: Categories and subcategories for the GOVERN function.

Categories	Subcategories
GOVERN 1: Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented	GOVERN 1.1: Legal and regulatory requirements involving AI are understood, managed, and documented. GOVERN 1.2: The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices. GOVERN 1.3: Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance. GOVERN 1.4: The risk management process and its outcomes are established through transparent policies, procedures, and other

Table 2: Categories and subcategories for the MAP function.

Categories	Subcategories
MAP 1: Context is established and understood.	MAP 1.1: Intended purposes, potentially beneficial uses, context-specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics. MAP 1.2: Interdisciplinary AI actors, competencies, skills, and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their par-

Table 3: Categories and subcategories for the MEASURE functi

Categories	Subcategories
MEASURE 1: Appropriate methods and metrics are identified and applied.	MEASURE 1.1: Approaches and metrics for meas risks enumerated during the MAP function are selec mentation starting with the most significant AI ri or trustworthiness characteristics that will not – o measured are properly documented. MEASURE 1.2: Appropriateness of AI metrics an of existing controls are regularly assessed and upd reports of errors and potential impacts on affected MEASURE 1.3: Internal experts who did not serv developers for the system and/or independent as

Table 4: Categories and subcategories for the MANAGE functi

Categories	Subcategories
MANAGE 1: AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.	MANAGE 1.1: A determination is made as to w system achieves its intended purposes and stated whether its development or deployment should pr MANAGE 1.2: Treatment of documented AI risk based on impact, likelihood, and available resourc MANAGE 1.3: Responses to the AI risks deemed h identified by the MAP function, are developed, pla umented. Risk response options can include mitig ring, avoiding, or accepting. MANAGE 1.4: Negative residual risks (defined as unmitigated risks) to both downstream acquirers

- ✓ Detailed
- ✓ Flexible
- ✓ Systematic
- ✓ Sensitive to actors and context

Agenda

Motivation

AI RMF Overview

Tools for AI RMF Implementation

Managing risk entails several key challenges.

Risk is hard to measure

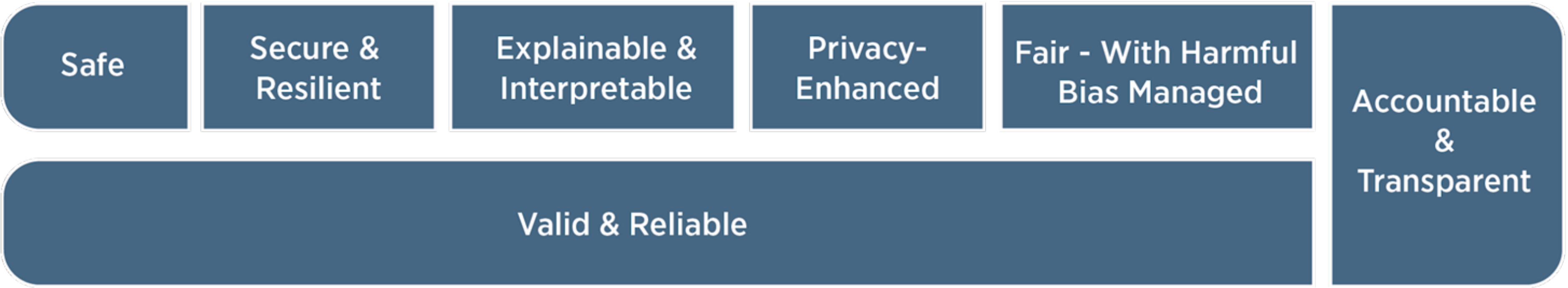
Risk tolerances vary

Risks must be prioritized

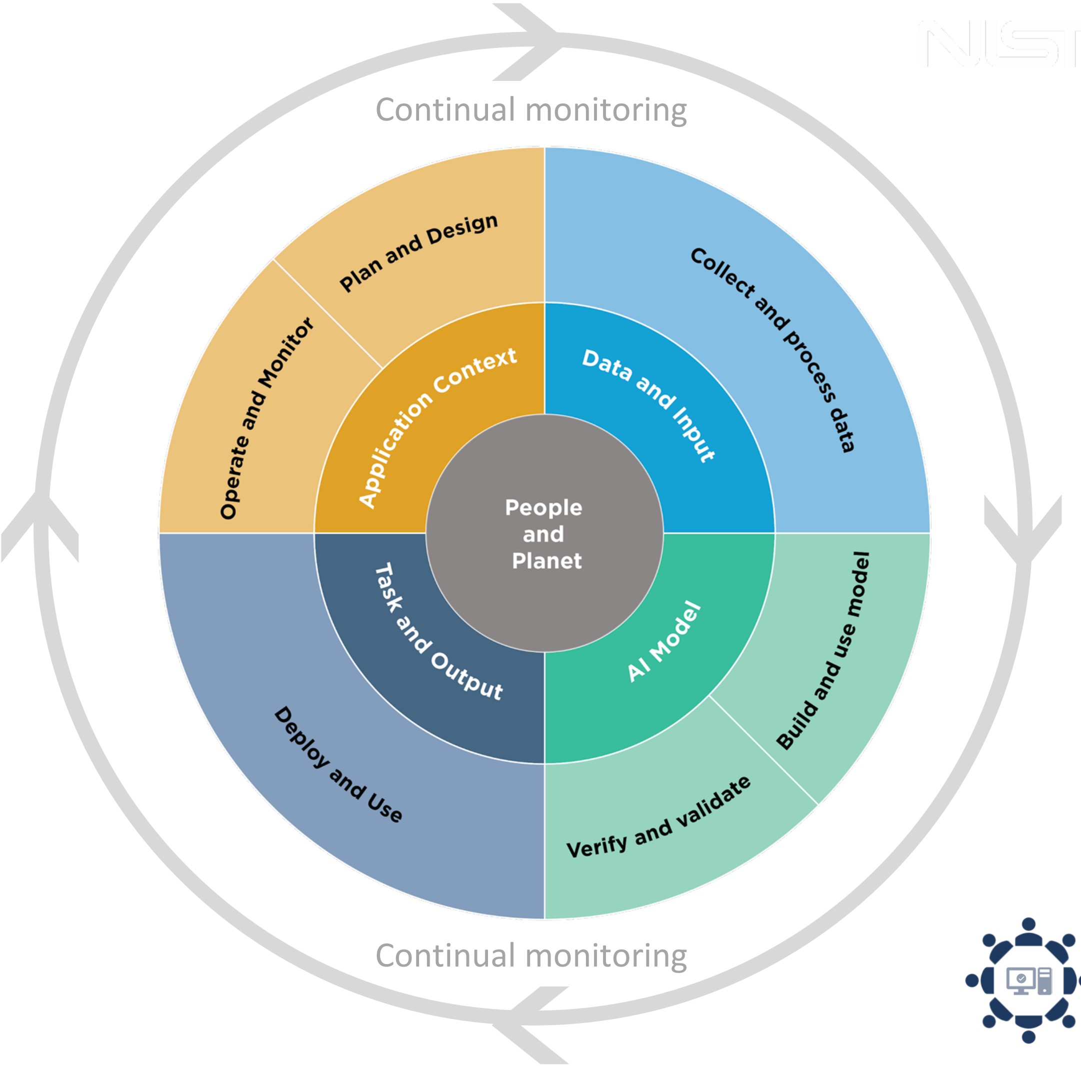
Risk management must be integrated

The core precept of the AI RMF is AI system trustworthiness within a culture of responsible AI practice and use.

AI system trustworthiness can be defined in terms of well-understood characteristics.

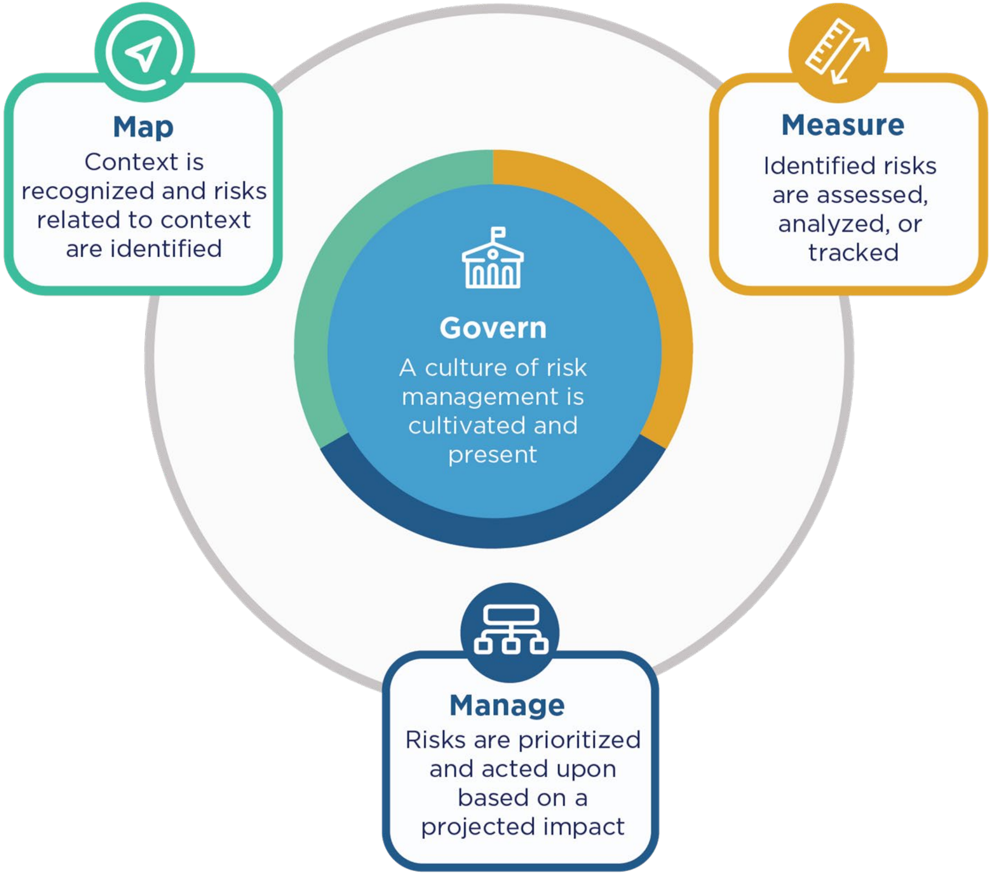


Beyond the system, a culture of responsible practice and use must pervade activities across the entire AI lifecycle.



NIST

The AI RMF Core lays out four organizational functions to facilitate trustworthy systems and responsible practice and use.



The GOVERN function is about fostering a risk-aware culture.

GOVERN 2: Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.

GOVERN 4: Organizational teams are committed to a culture that considers and communicates AI risk.

GOVERN 5: Processes are in place for robust engagement with relevant AI actors.

The **Map** function establishes the context in which risks could materialize.

Map 1: Context is established and understood.

Map 3: AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.

Map 5: Impacts to individuals, groups, communities, organizations, and society are characterized.

The MEASURE function sets up objective, repeatable, and scalable processes for test, evaluation, verification, & validation (TEVV).

MEASURE 1: Appropriate methods and metrics are identified and applied.

MEASURE 2: AI systems are evaluated for trustworthy characteristics.

MEASURE 3: Mechanisms for tracking identified AI risks over time are in place.

MEASURE 4: Feedback about efficacy of measurement is gathered and assessed.

The **Manage** function is how organizations forestall **Map**ped and **Measure**d risks, and respond to them when they materialize.

Prevention measures

- Data management
- Risk transfer mechanisms (e.g., insurance, warranties)
- System modification (e.g., model editing)
- Software quality assurance

Response measures

- Decommissioning mechanisms ("kill switches")
- Incident response plans
- Recourse and feedback mechanisms
- Monitoring (bias, performance, security)
- Information sharing

Agenda

Motivation

AI RMF Overview

Tools for AI RMF Implementation

The RMF is accompanied by a suite of tools in the Trustworthy and Responsible AI Resource Center (AIRC).

Crosswalk Documents

NIST AI RMF Crosswalks are produced by by NIST or other organizations and are intended to provide a mapping of concepts and terms between the AI RMF and other guidelines, frameworks, standards and regulation documents. Organizations are encouraged to submit crosswalks to NIST at aiframework@nist.gov for potential posting on this page. The below list includes crosswalks that have been submitted, reviewed and accepted to date.

Glossary

NIST is releasing "The Language of Trustworthy AI: An In-Depth Glossary of Terms". This effort seeks to promote a shared understanding and improve communication among individuals and organizations seeking to operationalize trustworthy and responsible AI through approaches such as the NIST AI Risk Management Framework (AI RMF). The Glossary is being released in beta format as a spreadsheet, as approaches to visualize the relationships between and among these terms continues. A final glossary release will be launched at a later date.

Technical and Policy Documents

The section provides direct links to NIST documents related to the AI RMF (NIST AI-100) and NIST AI Publication Series, as well as NIST-funded external resources in the area of Trustworthy and Responsible AI. New documents will be added as they are completed.

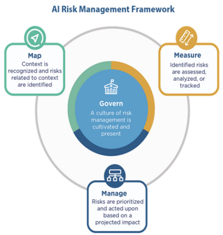
NIST AI RMF Playbook

The Playbook provides suggested actions for achieving the outcomes laid out in the AI Risk Management Framework (AI RMF) Core (Tables 1–4 in AI RMF 1.0). Suggestions are aligned to each sub-category within the four AI RMF functions (Govern, Map, Measure, Manage).

The Playbook is neither a checklist nor set of steps to be followed in its entirety.

Playbook suggestions are voluntary. Organizations may utilize this information by borrowing as many–or as few–suggestions as apply to their industry use case or interests.

Govern | Map | Measure | Manage



...

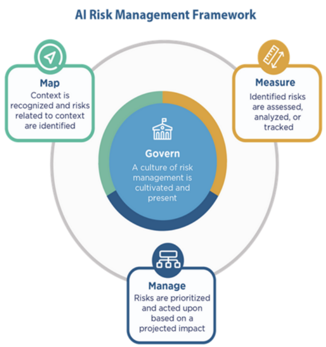
The Playbook was developed to give organizations a more detailed how-to for achieving the outcomes described in the Framework Core.

NIST AI RMF Playbook

The Playbook provides suggested actions for achieving the outcomes laid out in the AI Risk Management Framework (AI RMF) Core (Tables 1–4 in AI RMF 1.0). Suggestions are aligned to each sub-category within the four AI RMF functions (Govern, Map, Measure, Manage).

The Playbook is neither a checklist nor set of steps to be followed in its entirety.

Playbook suggestions are voluntary. Organizations may utilize this information by borrowing as many–or as few–suggestions as apply to their industry use case or interests.



Govern | Map | Measure | Manage

Download the NIST AI RMF Playbook

Playbook PDF | Playbook CSV | Playbook Excel | Playbook JSON

The AI RMF is being implemented at many scales, from individual systems'/organizations' "use cases" to "profiles" for entire sectors or technologies.

Criminal justice profile

Bank X's use case for its facial recognition in customer onboarding

Financial lending profile

City Y government's use case (applying to all its AI tools)

Large language models profile

Procurement profile

For more information, we encourage you to access NIST resources, or reach out directly!

NIST

https://ww.nist.gov/itl/ai-risk-management-framework

https://airc.nist.gov/

AIFramework@nist.gov

Apostol Vassilev

NIST ITL

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

Lessons Learned from the NIST Automated Vehicle Program

and How They May Apply to Uncrewed Aircraft Systems

Apostol Vassilev

February 1, 2024

Overview

NIST

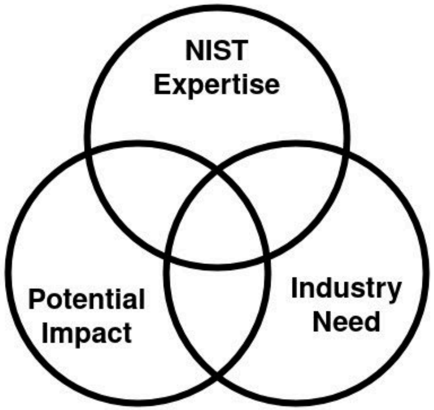
❖ Automated Vehicles Program*

- ❖ SERI (Strategic and Emerging Research Initiatives)
- ❖ Focus:
  - ❖ Address system technology performance and measurement methods
    - ❖ System technologies: Perception sensors, AI, Cybersecurity, and Communications (onboard and offboard)
  - ❖ Design and establish a systems interaction testbed
- ❖ Goals:
  - ❖ Provide the metrology and standards to increase the safety and security of automated vehicles (Avs)
  - ❖ Allow industry to better understand and characterize their AVs' performance
  - ❖ Provide Government agencies the knowledge to create regulations

* https://www.nist.gov/programs-projects/nist-automated-vehicles-program

Industry voices

Within NIST scope and expertise/infrastructure is available	Within NIST scope and expertise/infrastructure is lacking (NIST can support agencies)	Not within NIST scope
Develop novel individual and fused sensor measurement science solutions for vehicles	Define the data that should be measured before, during, and after operation of automated vehicles	Create and enforce a baseline for AV safety systems testing
Help define testing guidance for stakeholders to meet regulatory agency requirements	Provide reference materials for what infrastructure investment state and local governments should invest in	Enforce sensor specs that should be used in AVs
Develop mitigation standards for adversarial AI	Collect standardized data from the DoT from accidents to develop representative testing environments	Create regulation on periodic testing and updating
Develop AV simulation-based measurement science	Provide classification and levels for AV components	
Advance standards with SAE, 3GPP, and Teleoperation Consortium		
Develop measurement science for traffic infrastructure that can support AVs		
Develop metrics to identify what aspects of AVs should be measured to ensure safety		
Create test models and measurement science for AV communications		
Foster a community of stakeholders to agree on common taxonomies and standards		
Be a one-stop-shop for pointers to relevant autonomous vehicle standards		
Measure how different parts of an AV work together		
"Do you know that NIST cybersecurity framework? Just do that for autonomous vehicles."		



Outcomes

2023 Standards and Performance Metrics for On-Road AVs Workshop

September 5-8, 2023 (virtual)[Y]

- 619 attendees
- Overall keynote speaker:

Ann Carlson (NHTSA)

- Keynote speakers:

Anuja Sonalkar (STEER)
Cybersecurity

Rajeev Thakur (Ouster)
Perception

David Agnew (Dataspeed Inc)
Systems Interaction

Jim Misener (Qualcomm)
Communication

Aleksander Madry (MIT)
Artificial Intelligence

Ed Straub (SAE)
Infrastructure

[Y] https://www.nist.gov/news-events/events/2023/09/standards-and-performance-metrics-road-automated-vehicles-workshop

Artificial Intelligence

- ## Artificial Intelligence

Develop mitigation standards for adversarial AI

- ## Contacts:

  - Apostol Vassilev (apostol.vassilev@nist.gov)
  - Send feedback to ai-100-2@nist.gov

Artificial Intelligence

NIST

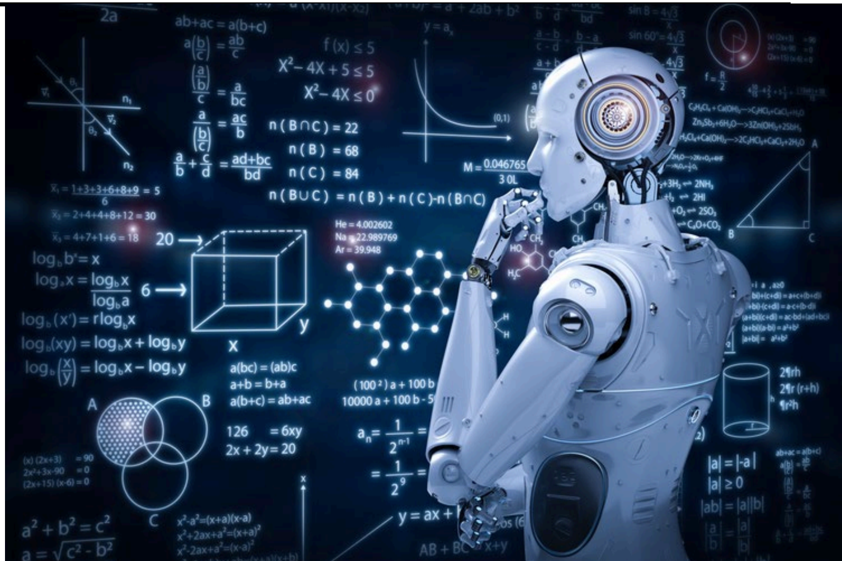
❖ Adversarial Machine Learning (AML)

Work on establishing a methodology for assessing risks and mitigations of attacks on AI models

- **NIST AI 100-2**[†] defines a taxonomy of attacks and mitigations in AML.
- Can be used in conjunction with the **NIST AI RMF**[‡] to identify and manage risks.

[†] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

[‡] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf



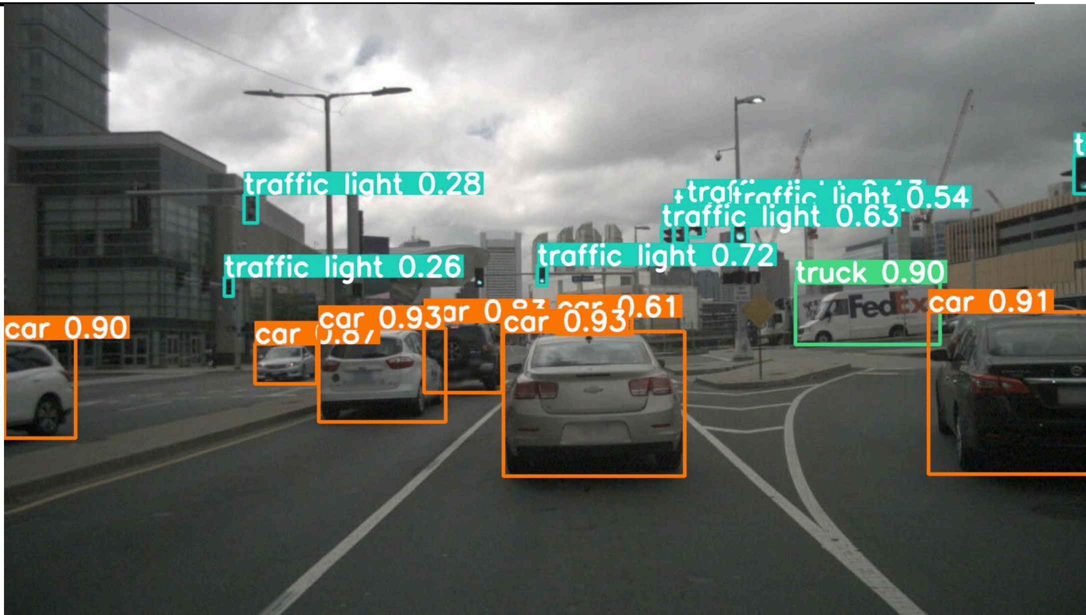
Artificial Intelligence

NIST

❖ Uncertainty Estimation for AI in AVs

Work on establishing a methodology for assessing robust measurement of uncertainties in AI models used in the perception and other systems of the vehicle

- ❖ Predictive Uncertainty Estimation helps to reduce the cascading propagation of risk in the systems of the car
- ❖ This effort will allow quantification of risk in AI for AVs and UAS



❖ Next Steps

Investigate the dependency of uncertainty on vehicle speed and distance to object

- ❖ View from a far, high speed, time T_0
- ❖ Dashed line box indicates the positional uncertainty around an object
- ❖ The model does not distinguish yet the car and the truck in front

Example w/ Gaussian YOLO v3

❖ Next Steps

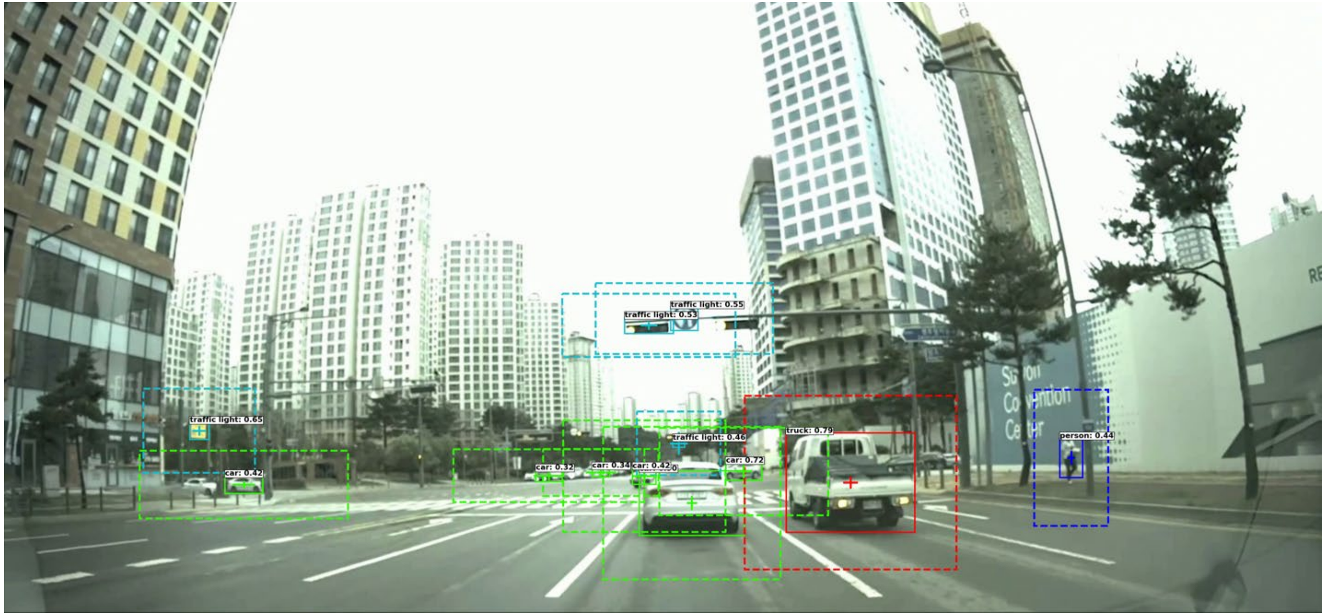
Investigate the dependency of uncertainty on vehicle speed and distance to object

- Getting closer, high speed, time T_1
- The model is now able to detect the two objects but the truck in front is misclassified as a car, a bush misclassified as a person
- Large uncertainty boxes

❖ Next Steps

Investigate the dependency of uncertainty on vehicle/system speed and distance to object

- ❖ Getting close, low speed, time T_2
- ❖ The model's object detection improves and picks up multiple objects: pedestrian (in blue), cars (in green), a truck (in red), etc.
- ❖ Smaller uncertainty boxes around the closest objects
- ❖ Larger uncertainty boxes around far objects



Artificial Intelligence

NIST

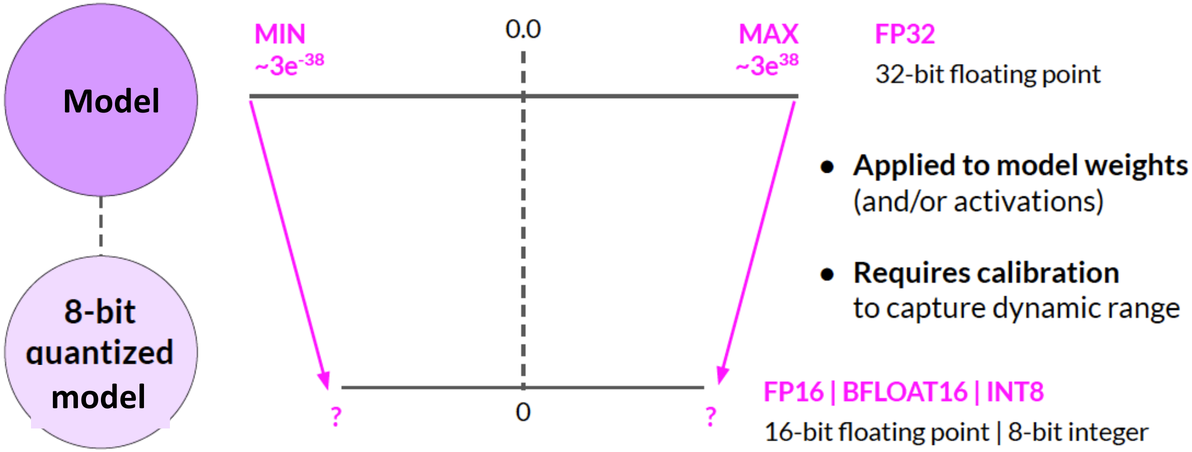
❖ Quantization

*Investigate the effects of **quantization** on the robustness and security of AI models used in UAS*

Post-Training Quantization (PTQ)

Reduce precision of model weights

- ❖ **Quantization** helps to fit AI models into the constrained computational resources of the UAS
- ❖ However, **quantized models** DO inherit the vulnerabilities of the original models and bring in additional weaknesses
- ❖ Quantized models are **vulnerable** to adversarial attacks.



Thank you !

❖ Questions and comments

Send to: apostol.vassilev@nist.gov

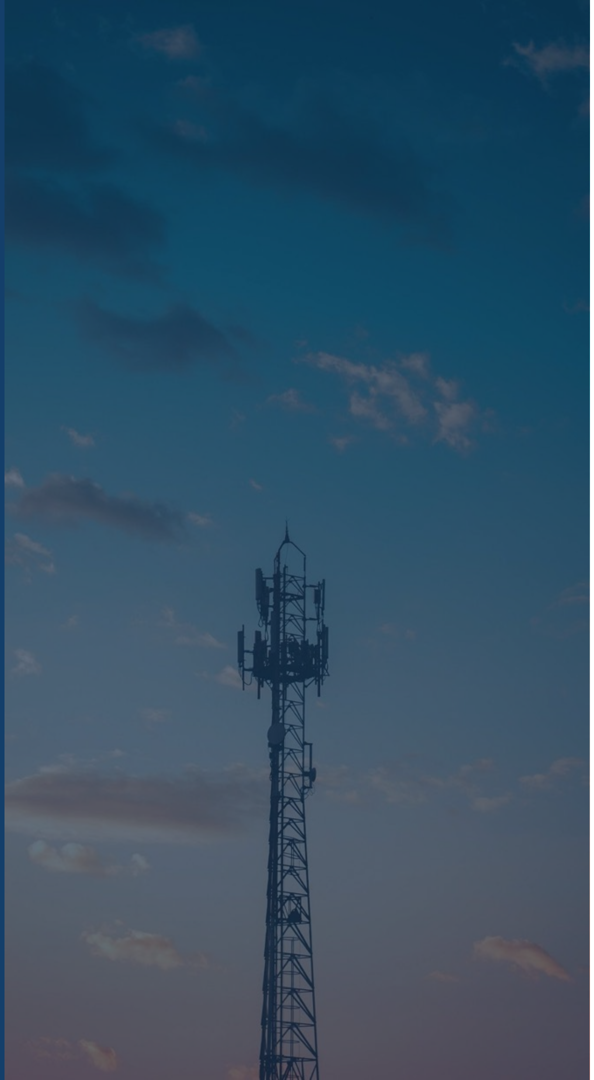
Artificial Intelligence Disclaimer

❖ Disclaimer

Certain commercial hardware, open source software, and tools are identified in this presentation in order to explain our research. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor does it imply that the software tools identified are necessarily the best available for the purpose.

Resume at 1:45 pm
(in 1 hour)

A 15-minute Q&A will follow the lunch break. Please submit questions via the Google Form through the QR code on your handout or through this link: https://bit.ly/UASWorkshopQandA



Lunch


Q&A
NIST
PUBLIC SAFETY
COMMUNICATIONS
RESEARCH

Connected Systems and Society

- Jay Stanley
  ACLU
- Dorothy Spears-Dean
  Virginia Dep’t of Emergency Management
- Ryan Bracken
  DroneSense
- Michelle Lea Desyin Hanlon
  Center for Air and Space Law
- Stephen Luxion
  ASSURE

Jay Stanley

American Civil Liberties Union

Domestic Drones:
10 Issues to be aware of

Jay Stanley
Senior Policy Analyst
Speech, Privacy and Technology Program
jstanley@aclu.org | @JayCStanley

ACLU
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION

Issues

1. Mass surveillance

Mass surveillance

Image: SHYCITYNikon via Flickr

Issues

1. Mass surveillance
2. **Importance of democratic process**

Democracy

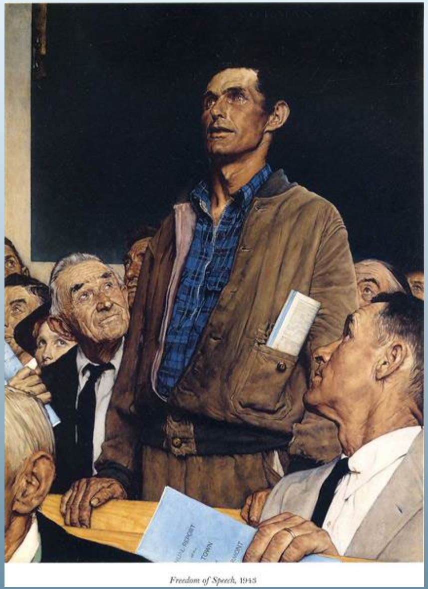
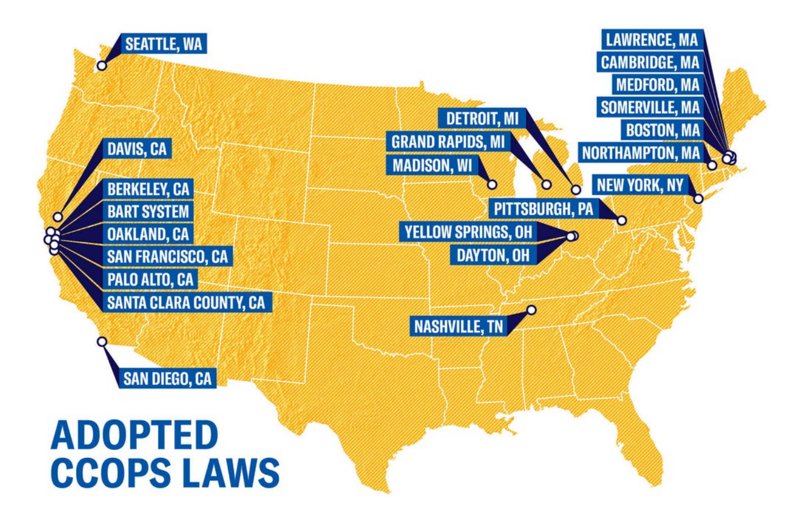


Image: Norman Rockwell via WikiArt



Local News

Seattle grounds police drone program

Originally published February 7, 2013 at 9:33 pm | *Updated February 8, 2013 at 8:52 am*

The Police Department had purchased two 3.5

Share story

Share

Email

Tweet

even before it got off the ground.

In a brief statement Thursday, McGinn said he and police Chief John Diaz agreed that it was time to end the program so the Seattle Police Department

THE BALTIMORE SUN

Report of secret aerial surveillance by Baltimore police prompts questions, outrage

By KEVIN RECTOR and LUKE BROADWATER

PUBLISHED: August 24, 2016 at 10:22 p.m. | UPDATED: June 29, 2019 at 10:53 a.m.

Issues

1. Mass surveillance
2. Importance of democratic process
3. **Chilling effects**

Trooper filming Selma march, 1965.

Photo by Alfred M. Loeb; used by permission.

Issues

1. Mass surveillance
2. Importance of democratic process
3. Chilling effects
4. **Don’t assume no privacy in public**

Do we have any privacy rights when we’re in public?

Image: JOH_2136 via Flickr

Used to be simple…

Image: Devlyn via Flickr

United States v. Jones (2012)

United States v. Jones (2012)

"GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."

Riley v. California (2014)

Image: houstonwiPhotos mp via Flickr

“Digital is different”

Roberts in *Riley*

The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items...That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.

Carpenter v. United States (2018)

The New York Times

How a Radio Shack Robbery Could Spur a New Era in Digital Privacy

Roberts in Carpenter:

- The Fourth Amendment's purpose is to "assure preservation of <u>that degree of privacy against government that existed when the Fourth Amendment was adopted</u>." (quoting Scalia in *Kyllo v US)*

- "like GPS monitoring, cell phone tracking is **remarkably easy, cheap, and efficient compared to traditional investigative tools**."

Leaders of a Beautiful Struggle v. Baltimore Police Department.
(4th Cir. 2021)

Image: Bloomberg

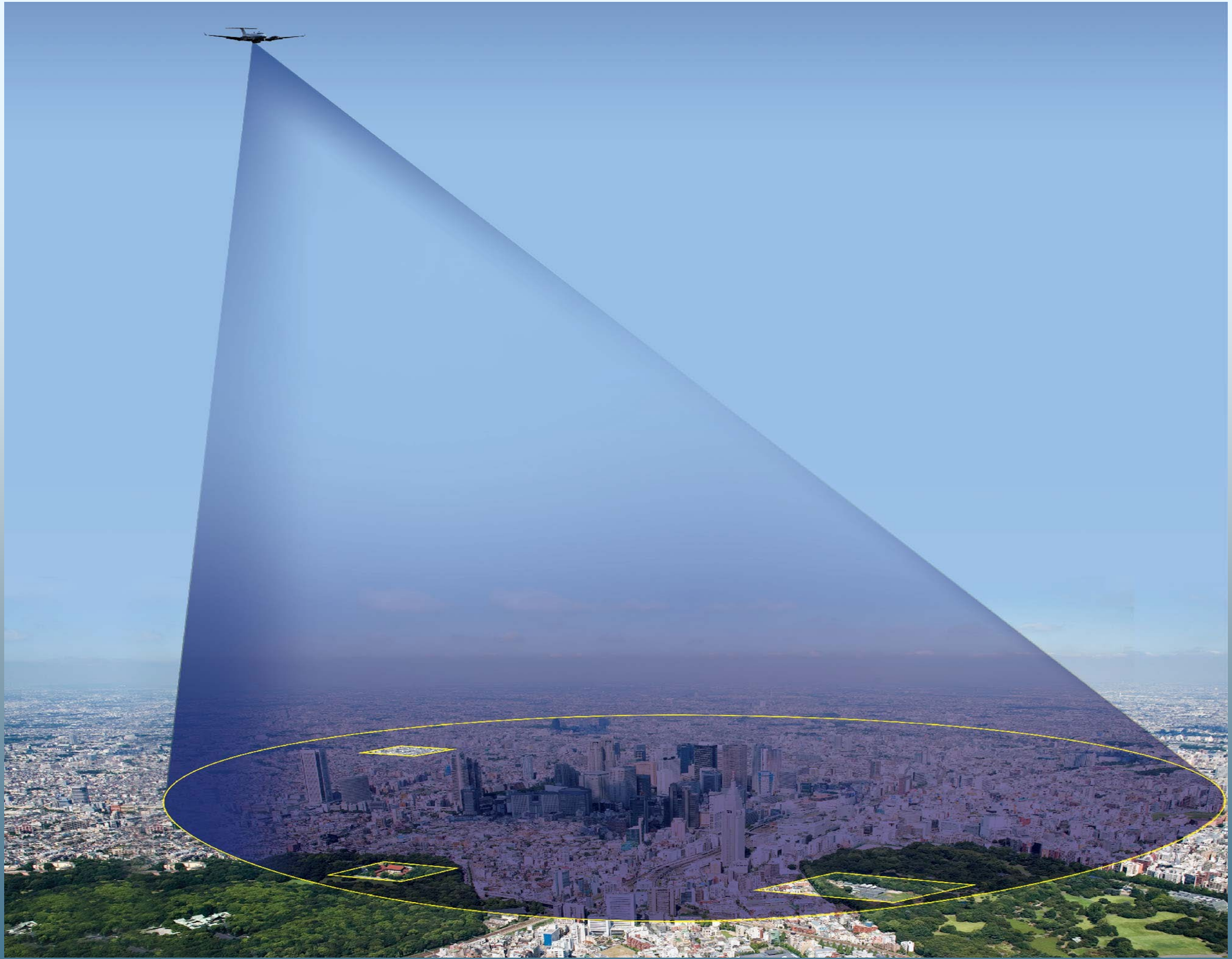


Image: Harris Corp

Leaders of a Beautiful Struggle v. Balt. Police Dep't. (4th Cir. 2021)

"because the AIR program enables police to deduce from <u>the whole of individuals' movements</u>, we hold that accessing its data is a search, and its warrantless operation violates the Fourth Amendment"

Issues

1. Mass surveillance
2. Importance of democratic process
3. Chilling effects
4. Don’t assume no privacy in public
5. **Usage limits**

Limits on drone usage

- True Emergencies (inc. DFR programs)
- Grounds to believe will collect evidence of wrongdoing
- With a warrant
- Not routinely over gatherings

Letter to editor,
Mountain Xpress, Asheville, NC

Aug 23, 2023

"When I was at the Rally for Reproductive Justice and Bodily Autonomy, there was one of their large drones flying overhead. When I was at the May Day Rally, there was one of their large drones flying overhead. When I was at a gathering of about 20 people discussing the force and neck-pinning used against Devon Whitmire? Drone overhead. When the city and county teachers associations gathered to demand higher pay? Drone overhead."

Issues

1. Mass surveillance
2. Importance of democratic process
3. Chilling effects
4. Don’t assume no privacy in public
5. Usage limits
6. **Recording limits**

Recording limits

- Monitoring ≠ recording
- DFR operations to & from
- Over gatherings, only to record illegal activities

Issues

1. Mass surveillance
2. Importance of democratic process
3. Chilling effects
4. Don’t assume no privacy in public
5. Usage limits
6. Recording limits
7. **Transparency**

Transparency

- DFR: routes & reasons
- Capabilities & payloads
- Policies
- Performance
- Video

Issues

1. Mass surveillance
2. Importance of democratic process
3. Chilling effects
4. Don’t assume no privacy in public
5. Usage limits
6. Recording limits
7. Transparency
8. **Auditing and effectiveness tracking**

Democracy

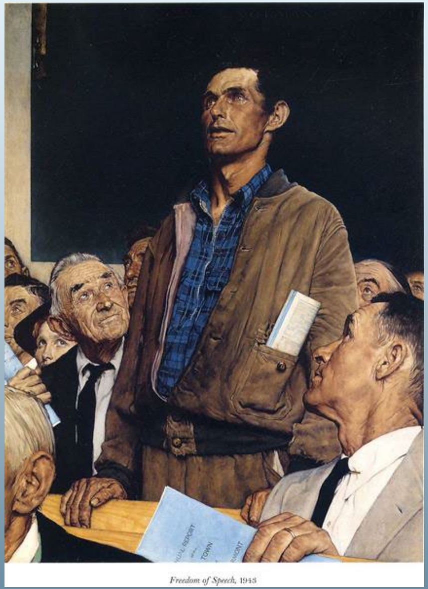


Image: Norman Rockwell via WikiArt

Issues

1. Mass surveillance
2. Importance of democratic process
3. Chilling effects
4. Don’t assume no privacy in public
5. Usage limits
6. Recording limits
7. Transparency
8. Auditing and effectiveness tracking
9. **Use and disclosure of video**

Use and disclosure of video

- No use of video to identify participants of gatherings except to investigate illegal activity (DC law)
- No AI analytics, sharing, or retention for other than a short period
- Exception: where video is evidence
- Exception: where video captures police use of force, or incident that is subject of a complaint against an officer.
- In those cases, video must be released to the public or complainant.
- What is released should not be up to discretion of law enforcement

Issues

1. Mass surveillance
2. Importance of democratic process
3. Chilling effects
4. Don’t assume no privacy in public
5. Usage limits
6. Recording limits
7. Transparency
8. Auditing and effectiveness tracking
9. Use and disclosure of video
10. **Crowding out other drone uses**

NEW YORK POST

NEWS EXCLUSIVE

2 drones in near-miss with NYPD chopper

By Larry Celona

Published July 7, 2014, 9:19 p.m. ET

The NYPD pilots "observed flying object[s] at 2,000 feet in vicinity of the George Washington Bridge, then circling heading toward the helicopter,'' a police report said.

"The officers were forced to change their course to avoid a collision."

One source called it a "very dangerous" scenario.

"Although [drones] may only weigh a few pounds, that's all birds weigh, and look what they did to the Sully Airbus," the source said, referring to 2009's "Miracle on the Hudson," in which a bird strike forced US

MOTHERBOARD
TECH BY VICE

NYPD Helicopter Flew at a Drone and Never Feared Crashing, Recording Confirms

A police officer said he had no idea whether or not a crime was even committed.

Listen to this article now 7 min listen
00:00 1.0x -06:59
Powered by Trinity Audio

By Jason Koebler

Clueless Cops Fly Helicopter At Drone, Arrest The Drone Pilots

By Raphael Orlove Published July 11, 2014 | Comments (289)

Two guys were arrested on Monday for flying a drone at an NYPD helicopter. It now sounds like it was the cops who flew their chopper at the drone.

Drone operators Mendoza and Remy Castro were arrested on felony reckless endangerment charges for flying "very close" to an NYPD chopper near the George Washington Bridge, as *Motherboard* reports. The chopper had

BROOKINGS Election '24

COMMENTARY

How to regulate police use of drones

Faine Greenwood
September 24, 2020

What's more, police drones are a highly effective way for law enforcement to "mark" the aerial territory over news-worthy events. While plenty of journalists and activists use drones to collect their own aerial information, they're often reluctant to fly when there's a chance they could be accused of interfering with a drone or a helicopter operated by police.

Issues

1. Mass surveillance
2. Importance of democratic process
3. Chilling effects
4. Don’t assume no privacy in public
5. Usage limits
6. Recording limits
7. Transparency
8. Auditing and effectiveness tracking
9. Use and disclosure of video
10. Crowding out other drone uses

Thank you!

Jay Stanley
Senior Policy Analyst
Speech, Privacy and Technology Program
jstanley@aclu.org | @JayCStanley

ACLU
AMERICAN CIVIL LIBERTIES UNION FOUNDATION

Dorothy Spears-Dean

Virginia Department of Emergency Management

Virginia Department of Emergency Management

Connected Systems and Society: 9-1-1 and GIS

Date: February 7, 2024
Presenter: Dorothy A. Spears-Dean, VDEM

9-1-1, GIS and Drone Technology

- Aerial photography
- Disaster management
- Live streaming or aerial images from an emergency or disaster site
- Safeguarding of first responders
- Mapping of difficult or inaccessible terrain
- Swift water rescues
- Law enforcement pursuits
- Structural fires
- Addressing for 9-1-1

Case for Change

- The adoption of drone technology is changing from a “nice to have” to a “must (or need to) have”
- Fueled by the convergence of systems
- Disruptive technologies impact public safety
- It’s has become part of the public safety consciousness and a tool in the responder toolbox
- Life saving applications
- Efficiency and effectiveness
- Existing evaluative frameworks

User-Centered Design Guidelines*

1. Improve current technology
2. Reduce unintended consequences
3. Recognize “one size does not fit all”
4. Minimize “technology for technology’s sake”
5. Lower product/service costs
6. Require usable technology

* [Voices of First Responders: Communication Center & 9-1-1 Services (nist.gov)]

Questions?

Dorothy A. Spears-Dean
(804) 840-7260
Dorothy.spearsdean@vdem.virginia.gov

THANK YOU!

Ryan Bracken

DroneSense

DRONESENSE

Public Safety Drone Cyber and AI Risk

Ryan Bracken

Ryan Bracken

Chief Product Officer and CISO
DroneSense

Product Vision and Security

12 years as FBI Special Agent in Counterterrorism, Cyber, and Aviation Operations

Aerospace Engineer, US Air Force

BS and MS Aeronautical Engineering

FAA Commercial/instrument and Part 107 Remote Pilot Certificates

DroneSense

Software-as-a-service drone platform for Public Safety

- Flight Control App
- Video Streaming
- Fleet Management
- Remote Operations

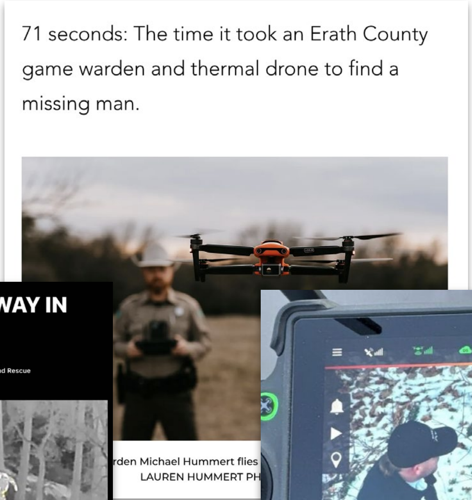
Public Safety Drone Ops are Saving Lives


FOX5 Live News Weather Things To Do Good Day Contests More

New drone video shows Montgomery County police fighting crime in real time

By Ayesha Khan | Published January 10, 2024 | Montgomery County | FOX 5 DC |

New drone video shows Montgomery County police fighting crime in real time


71 seconds: The time it took an Erath County game warden and thermal drone to find a missing man.

rden Michael Hummert flies

LAURENN HUMMERT PH


POLICE DRONES SAVE 50 LIVES IN NORWAY IN 2023

Haye Kesteloo / January 18, 2024 / Drone Technology, Drones, Drones For Good, Norway, Police, Police Drones, Search And Rescue


81%
88%
KN
0:24:19
RNG
20.00 ×
FPV
M30
02:21
POLICE
89.9 FT
41.498335, -111.98416
MAP
CURRENT: Manual operation
4°
34°
368.5 FT
GIMBAL ANGLES
DRONE/HOME DIST
145°
WIND
4.3
MPH
NEXT: N/A
SPEED
HRZ
0.0 MPH
VRT
0.0 MPH
HEIGHT
AGL
157.8 FT
HAT
74.3 FT
dji

But Drones Introduce Risk Too

The Drone Cyberattack That Breached a Corporate Network

CYBERSECURITY / 10.21.22 / Bruce Sussman

No one at the investment firm must have noticed the whirring of drone blades overhead — or heard the two miniature aircraft landing on the rooftop — if they made any noise at all.

But once there, the attack drones began carrying out their secret mission: breaking into the

This Hacker Tool Can Pinpoint a DJI Drone Operator's Exact Location

Every DJI quadcopter broadcasts its operator's position via radio—unencrypted. Now, a group of researchers has learned to decode those coordinates.

PHOTOGRAPH: EVGEN KOTENKO/GETTY IMAGES

Public Safety Risk Assessment

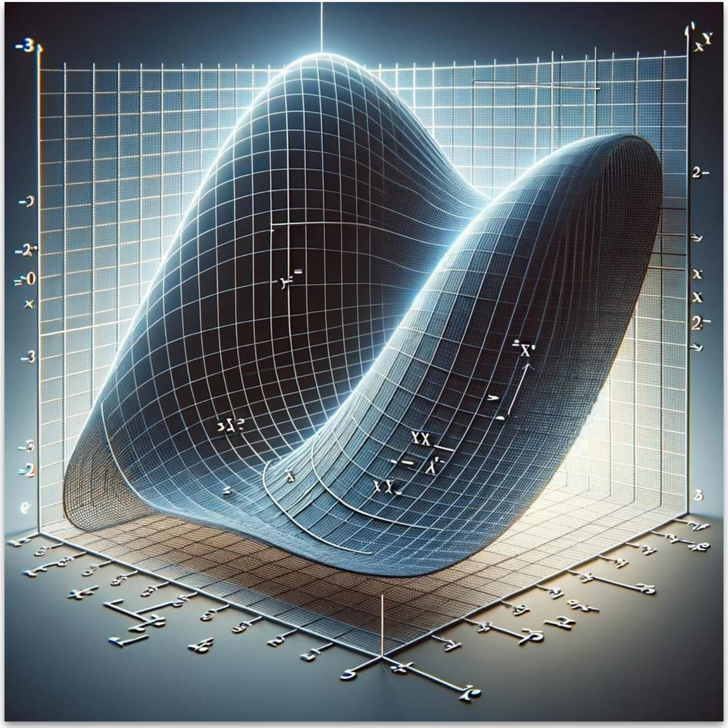
An agency needs an honest assessment of Cyber and AI risk

- Neither fit neatly in traditional cyber risk assessments
- Early adopters accept greater technical risk
- Local risk may increase while global risk decreases

Apples and Oranges

As a community member, I might have a different risk equation:

- Fear of crime or hazards
- Trust for Law Enforcement
- Is a drone going to fall on me?
- Is a drone going to collide with an aircraft I'm in?
- Am I willing to pay more taxes?



Let’s Start with Cyber Risk

Address the Confidentiality, Integrity, and Availability individually and as a complete system:

- Hardware
- Software
- Network and Communication links
- Server architecture

Public Safety Requirements

- Affordable
- Cutting Edge
- Secure/Reliable


Public Safety Requirements

- Affordable
- Cutting Edge
- Secure/Reliable

$\left.\right\}$ Pick Any Two

Assessing Cyber Risk

Use appropriate industry-standard accreditations:

- SOC 2
- ISO 27001
- FedRAMP

Assessing Cyber Risk

Use appropriate industry-standard accreditations:

- SOC 2
- ISO 27001
- FedRAMP

...but be realistic

AI is Something Completely Different

Or is it?

- Fundamentally still software
- Runs on servers
- Should have all the same cyber protections

…but Public Safety must understand the unique risks with AI

AI is Creating Enormous Opportunities for Public Safety

National Institute of Justice breaks AI opportunities for Public Safety into four key areas:

- Video and Image Analysis
- DNA Analysis
- Gunshot Detection
- Crime Forecasting

AI is Creating Serious Challenges for Public Safety

Cops bogged down by flood of fake AI child sex images, report says

Investigations tied to harmful AI sex images will grow "exponentially," experts say.

by **Ashley Belanger** - Jan 31, 2024 12:08 pm

(credit: SB Arts Media | iStock / Getty Images Plus)

AI, facial recognition technology causing false arrests across nation

Calls for regulation grow as Black men across U.S. wrongfully jailed.

Black men across the U.S. are being wrongfully jailed through facial recognition technology.

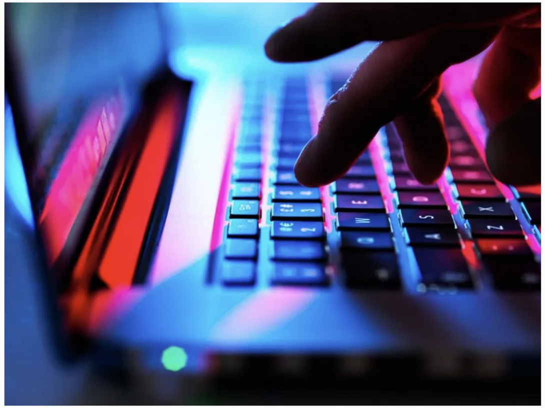
By Ciara Cummings
Published: Nov. 30, 2023 at 4:23 PM EST | Updated: Dec. 1, 2023 at 9:16 AM EST

AI And Cybercrime Unleash A New Era Of Menacing Threats

Rabiul Islam Former Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

Jun 23, 2023, 05:45am EDT

Rabiul Islam is a seasoned cybersecurity specialist. He is also the founder, CEO and managing director of TechForing Ltd.



AI Benefits and Risks are Greater When Coupled with a Drone

A drone gives AI an ability to act

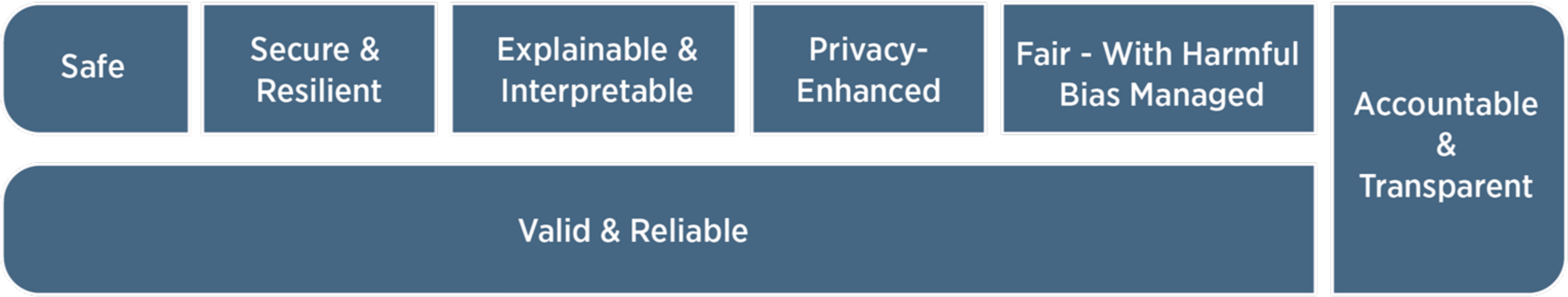
- Target recognition and tracking
- False positives/negatives
- Unpredictable “edge” cases

The Real AI Weapons Are Drones, Not Nukes

Hollywood imagined that computers would launch a nuclear missile, but self-guided aircraft are what’s truly changing the nature of combat.

By Phillips Payson O’Brien

Rely on Existing Frameworks



NIST AI Risk Management Framework

AI Impact Assessment

Examples AI use at various potential Impact Levels

- Enhanced administrative reporting (Low)
- Predictive maintenance (Medium)
- Flight Control (High)

Back to Basics

Define the risk posed by a drone or AI system:

1) the possible negative impact, or magnitude of harm

2) the likelihood of occurrence

AI Risks for Public Safety

Some sample questions for Public Safety to ask purveyors of AI-enhanced systems

- What does it actually do? How does it work?
- How will it use our data?
- How (and how often) is the model updated?
- How could it impact us if it goes wrong?

Must be able to answer these questions using absolutely NO JARGON

Privacy, Bias, and Community Trust

UAS platforms must be secure and reliable but how do we measure the less tangible effects on society?

- How does the system protect privacy?
- What elements could create biases?
- Is my deployment model equitable?

Privacy, Bias, and Community Trust

UAS platforms must be secure and reliable but how do we measure the less tangible effects on society?

- How does the system protect privacy?
- What elements could create biases?
- Is my deployment model equitable?

Am I using this thing correctly?

Privacy, Bias, and Community Trust

UAS platforms must be secure and reliable but how do we measure the less tangible effects on society?

- How does the system protect privacy?
- What elements could create biases?
- Is my deployment model equitable?

→ Am I using this thing correctly?

DRONESENSE

Michelle Lea Desyin Hanlon
Center for Air and Space Law, University of Mississippi School of Law

CHALLENGES OF AUTONOMOUS SYSTEMS

Michelle L.D. Hanlon
University of Mississippi

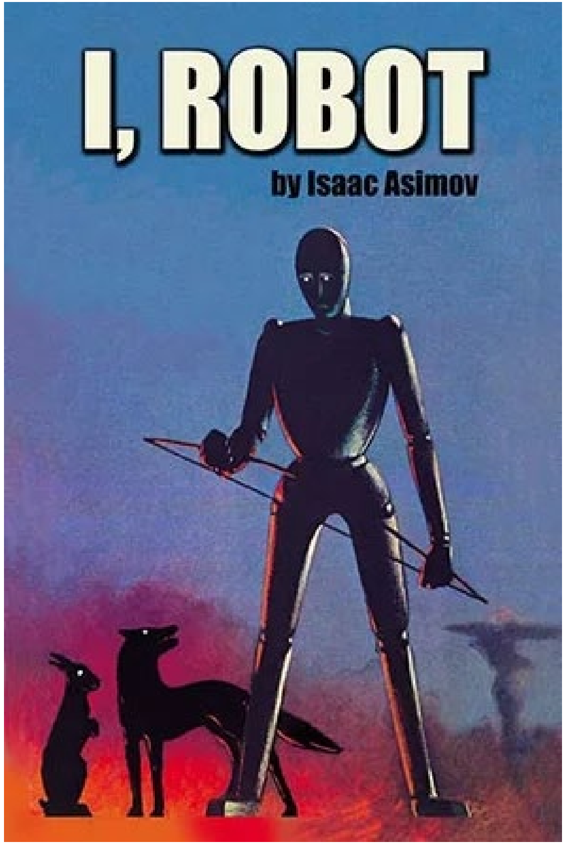
2024 PSCR UAS Portfolio Workshop
February 7, 2024

CENTER FOR AIR & SPACE LAW
THE UNIVERSITY of MISSISSIPPI
SCHOOL OF LAW

The Center for Air and Space Law is leading research efforts to provide viable solutions that assure that humans take full advantage of the many benefits offered by drone technologies, while preserving privacy, safety and security.

CENTER FOR AIR & SPACE LAW

Three Fundamental Rules of Robotics



One, a robot may not injure a human being, or, through inaction, allow a human being to come to harm. . ..

Two, … a robot must obey the orders given it by human beings except where such orders would conflict with the First Law.

And three, a robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

ISSAC ASSIMOV, Roundabout, in I. ROBOT (1950).

CENTER FOR AIR & SPACE LAW

What is AI?

Nersessian and Mancha thoughtfully categorize AI as follows:

- (i) Automation AI: Characterized by known pathways and defined characteristics, replacing known and repetitive human activities (e.g. sales chatbots, or repetitive tasks in manufacturing).
- (ii) Augmentation AI: Designs based on known interactions with human operators- helping workers to recall and analyze data but leaving judgment and strategizing to necessary human counterparts (e.g. surgical robots, or the augmented reality game Pokemon Go).
- (iii) Autonom[ous] AI: Machine learning based on unknown interactions and environments, where the machine itself makes important, high stakes decisions- only primitive forms currently exist (e.g., today's "self-driving" vehicles), but autonomy will be the inevitable result of AI increasingly gaining the ability to deal with unstructured data and complex settings.

CENTER FOR AIR & SPACE LAW

Primary AAI Vulnerabilities

- Loss of Privacy and Data Security
- Manipulation and hijacking
- The Black Box of Machine Learning
- Bias
- Phantoms and Hallucinations

https://www.nbcnews.com/tech/tech-news/self-driving-uber-car-hit-killed-woman-did-not-recognize-n1079281

https://www.brookings.edu/articles/how-emergency-responders-are-using-drones-to-save-lives/

Stephen Luxion

Alliance for System Safety of UAS through Research Excellence (ASSURE)

The FAA's Center of Excellence for UAS Research

ASSURE

Alliance for System Safety of UAS through Research Excellence

Big Picture Overview
NIST PSCR UAS Workshop
February 7-8, 2024

Steve "Lux" Luxion, Colonel (USAF-Retired)

Executive Director, ASSURE

SLuxion@assure.msstate.edu

ASSURE Global

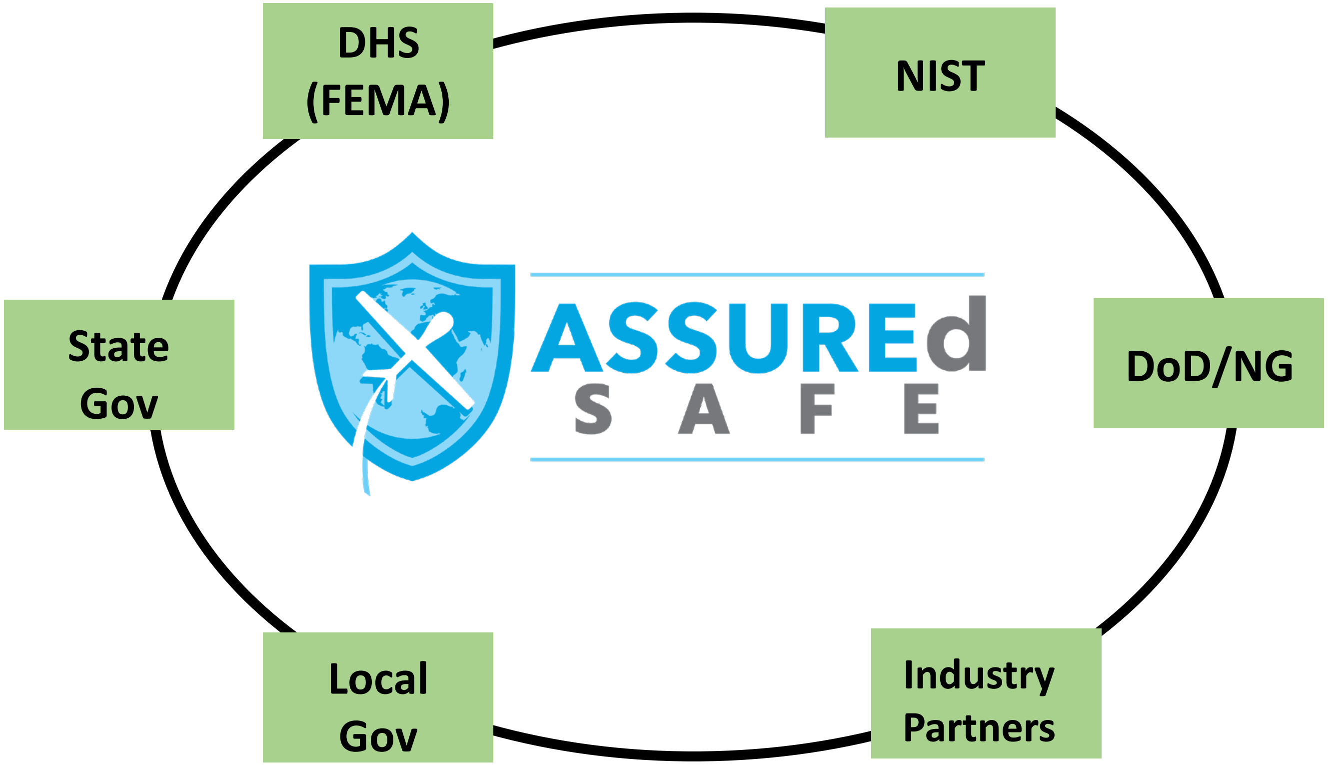
ASSUREd Safe
First Responder UAS

ASSUREd Safe Guiding Principles

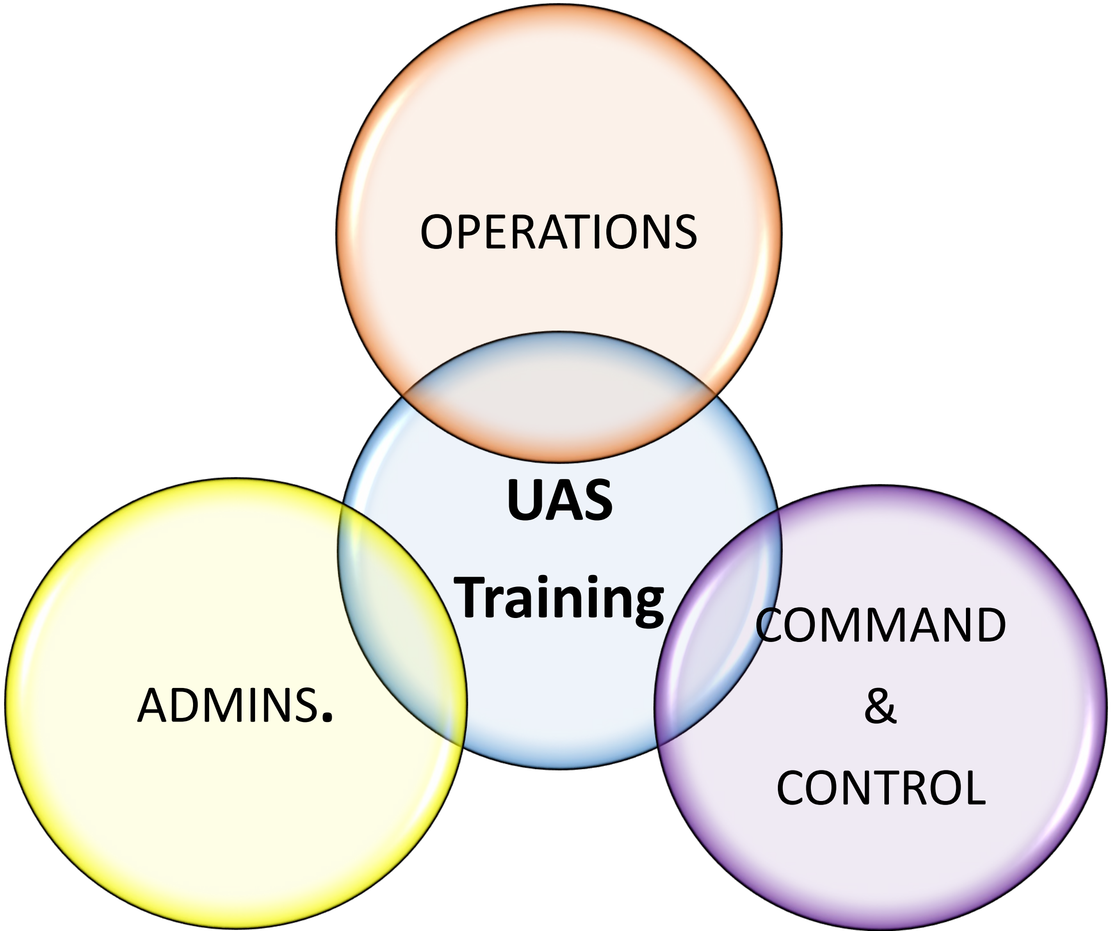
Vision

ASSUREd Safe is a federated ecosystem to educate, train, test, certify and ultimately credential first responders' use of uncrewed aircraft systems (UAS).

ASSUREd Safe Strategic Environment



ASSUREd Safe Training



ASSUREd SAFE

Training Focus

OPERATIONS
Fire
Law Enforcement
Emergency Medical Services
Support Personnel

ADMINISTRATIVE
Chiefs
Commanders
Coordinators
Safety Officers

COMMAND & CONTROL
EMA/EOC Directors
Incident Commanders
Air Bosses

ASSUREd SAFE

Curriculum Pathway (Flying Pilots)

Certified Pilot = Core Courses + Agency Track

ASSUREd Safe Pilot Core Courses
Part 107 Certification (to be submitted by student)
UAS Flight Operations Core Courses – First 4* Levels (4 Modules in each Level)
UAS Data Analytics Core Courses – First 2* Levels (4 Modules in each Level)
UAS Natural Disaster Response Applications – 6 Modules
UAS Search and Rescue Applications – 2 Modules
Laws and Regulations

*These Levels are "module" based. The number of levels/course is TBD based on what constitutes "adequate" knowledge.

Police Track
Introduction to Law Enforcement Drone Operations
Surveillance and Reconnaissance with Drones
Crime Scene Documentation and Evidence Collection
Tactical Operations and Incident Response with Drones
Advanced Search and Rescue Operations with Drones

EMS Track
Introduction to EMS Drone Operation
Rapid Scene Assessment and Triage with Drones
Medical Supply Delivery and Logistics
Aerial Medical Patient Monitoring
Disaster Response and Resource Management

Fire Track
Introduction to Fire Department Drone Operation
Drone-Assisted Fire Response Scenarios
Advanced Fire Incident Mapping with Drones
Drone-Assisted Search and Rescue Operations
Advanced Thermal Imaging and Fire Behavior Analysis

The ASSUREd Safe Course Plan

- Available Course
- Available FY 24/FY25
- Available FY 25/FY26
- FEMA or NIST course (available now)

Foundational

- Flight Operations
- Data Processing and Analysis
- Incident Command System
- Environmental OPS
- Fleet Management
- NIST UAS Test Method

Advanced

- Program
- Management
- Imagery Collection
- Day-Night Operations
- UAS Forensics
- Mapping and GIS
- Damage Assessments
- Air Boss
- Accident Reconstruction
- NIST UAS Test Method – Adv
- NIST Confined Space
- NIST Proctor Course

Endorsements/Electives

- Search & Rescue (Urban)
- Weather damage (water, wind)
- Fire - Urban Force
- Police
- Search & Rescue (Rural, Mtn, Forest)
- Fire – Volunteer Force
- Hazmat
- Dept of Defense - Assist
- National Guard
- DHS (FEMA, CBP, CISA)
- Chem/Bio/Nuc

The ASSUREd Safe Future Process

Learning Management System

- Courses: Onsite, Remote, and Hybrid
- Opportunity to earn “UAS Credentialed” status of various skills levels
- Opportunity to earn “Endorsements” for additional UAS skills:
    - Law Enforcement
    - Fire Service
    - Emergency Management
- Access to database of individual progress

E-Commerce Site

- One-stop shop
- Discover training opportunities and credentialing requirements
- Enroll and pay for courses

First Responder UAS Credentialing Database

- Sole source secure registry of UAS credentialed First Responders
- Database access available to authorized users to:
    - Validate UAS credentialed status
    - Locate UAS credentialed personnel geographically or by position qualification

FY2023

FY2024

FY2025

FY2026

NASA – Command, Control, & Communications (C3)

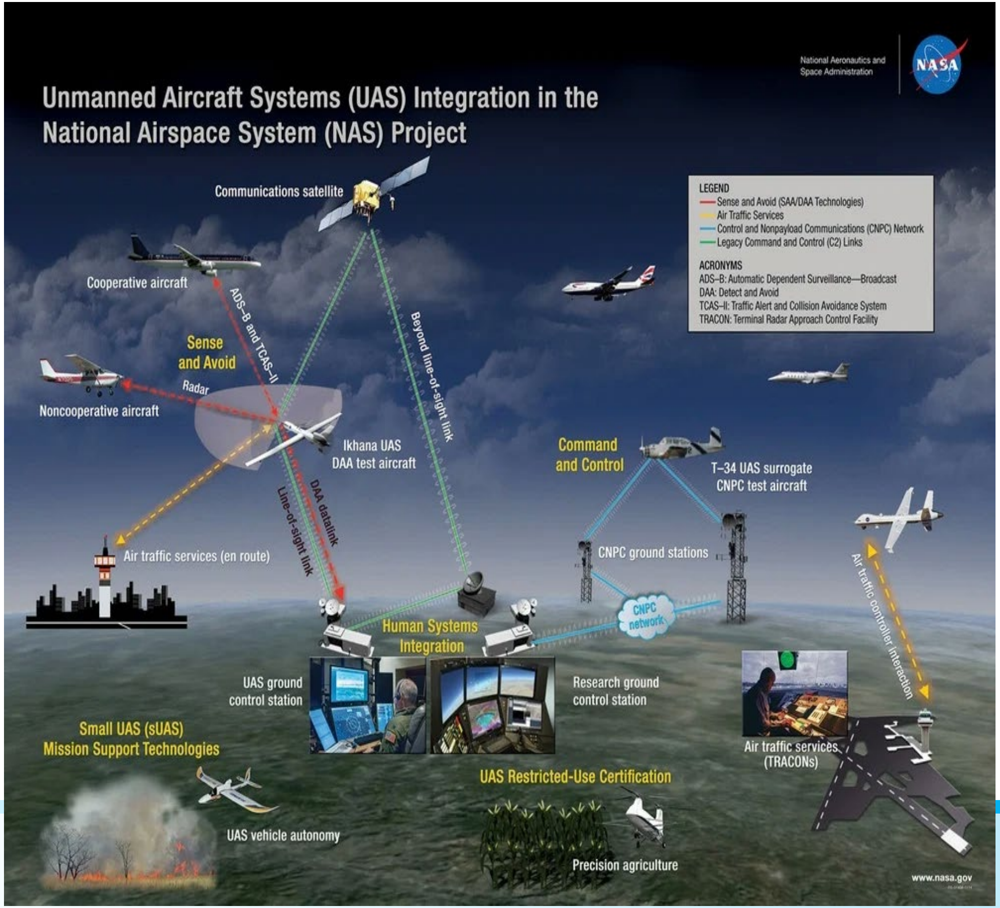
C3

- Comprehensive Assessment
- Denied/Degraded Environs
- UTM Spectrum Considerations

Multi-Vehicle Ops Approaches

DAA & BVLOS

Low Altitude WX Forecasting



The FAA's Center of Excellence for UAS Research
ASSURE
Alliance for System Safety of UAS through Research Excellence

International

Harmonize regulations, standards, and guidelines to collaborate around the globe

FAA International Regulator Roundtable on Research

Growing international network includes potential for future collaboration with first responders globally:

- UK (Cranfield)
- Singapore (Nanyang Tech Univ.)
- Australia (ANU), NZ (in-work)
- S. Korea and some efforts in Spain

EASA

Member of Advisory Board for BVLOS Demonstrations

Questions/Comm
ents

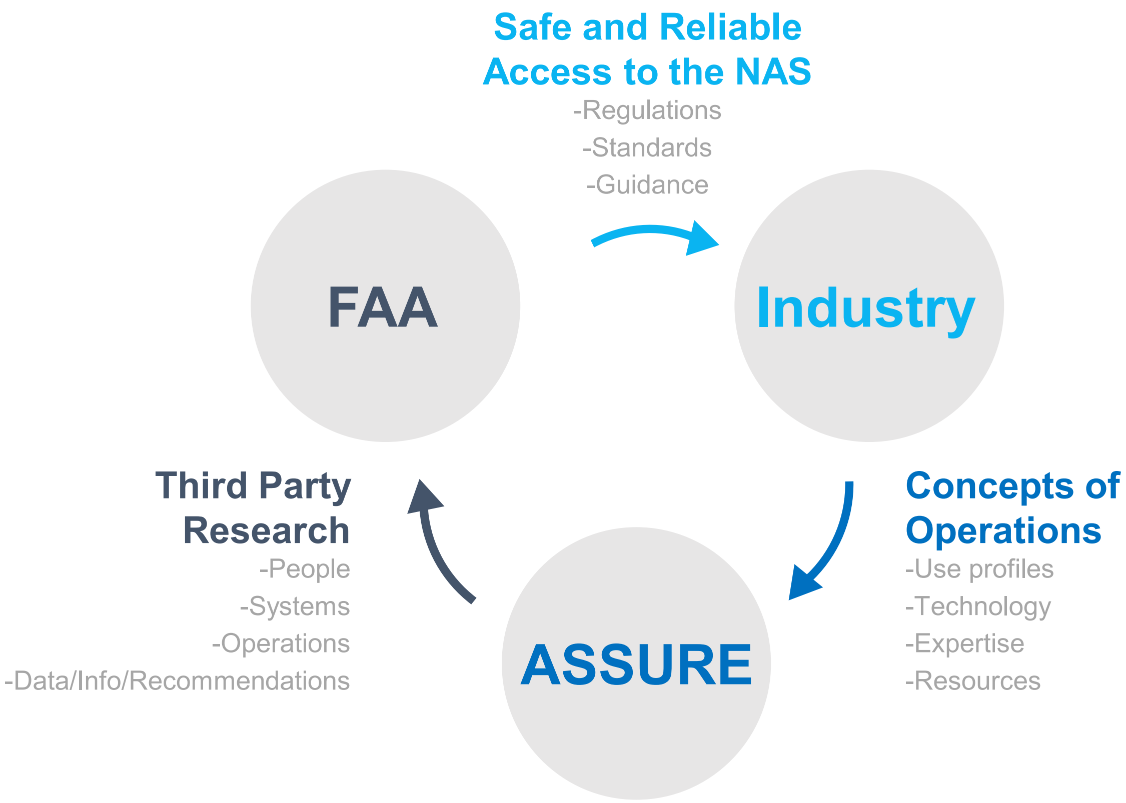
ASSUREuas

ASSURE UAS

www.ASSUREuas.org

sluxion@assure.msstate.edu

ASSURE's Direction from the FAA



ASSURE Global

Solve Problems and seek opportunities outside the FAA

Leverages ASSURE alliance and its relationships, in addition to the knowledge and experience gained from FAA research

ASSURE GLOBAL

One contract and NDA, if required

- ASSURE does the rest to leverage our teammates
- Master Teaming Agreement w/partners
- Execute through Task Orders

Another mechanism to conduct FAA and government work

Currently supporting NASA, DoD, State DoTs, and Foreign Governments

Working with ASSURE (General Info)

Collaborate with ASSURE COE partners

- Join ASSURE through website: www.ASSUREuas.org
- Participate & influence research

IDIQ Contracts with the FAA and DHS

- Align/Fit into 11 FAA UAS Research Areas
- Memo between Federal Agencies
- MIPR Funds: FAA will contract and provide program management

ASSURE (Global)Non-Profit

- Single contract vehicle w/Miss State University;
    - We do the rest through Master Service Agreements with our schools & partners
- Leverages
    - ASSURE Alliance and its relationships
    - Knowledge and experience gained from FAA research
- No Cost: ad hoc teaming based on need
- **DHS – MSU Contract Vehicle** New

Breakout Session 1:
Getting to know the problems.

Check your badge for group

One city
Five scenarios
15 minutes each

Share your expertise and experience

Don’t try and solve the problems!
That’s for tomorrow.

Breakout Session 1: 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)**
- We'll repeat this process with distinct scenarios
- For each scenario, consider the gaps in tools, technologies, procedures, etc. that may have led to the issues identified

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 is the most likely or plausible worst-case result or outcome?
- What are the potential tools ***currently*** available (technology, procedures, alternative method, etc.)?
- What are the ***current*** operational constraints (gaps in tools, technology, procedures, safety, timing, risks, etc.)?

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 is the most likely or plausible worst-case result or outcome?
- What are the potential tools ***currently*** available (technology, procedures, alternative method, etc.)?
- What are the ***current*** operational constraints (gaps in tools, technology, procedures, safety, timing, risks, etc.)?

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 is the most likely or plausible worst-case result or outcome?
- What are the potential tools ***currently*** available (technology, procedures, alternative method, etc.)?
- What are the ***current*** operational constraints (gaps in tools, technology, procedures, safety, timing, risks, etc.)?

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 is the most likely or plausible worst-case result or outcome?
- What are the potential tools ***currently*** available (technology, procedures, alternative method, etc.)?
- What are the ***current*** operational constraints (gaps in tools, technology, procedures, safety, timing, risks, etc.)?

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 is the most likely or plausible worst-case result or outcome?
- What are the potential tools ***currently*** available (technology, procedures, alternative method, etc.)?
- What are the ***current*** operational constraints (gaps in tools, technology, procedures, safety, timing, risks, etc.)?

Breakout Session 1:

Following the presentations and breakout sessions today, what AI and cybersecurity risks concern you the most as a member of the UAS ecosystem?

Slido

Grab your phone and head to
slido.com

Enter the code:
#1910 124

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

Discussion

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

- **Q&A Tomorrow, February 8**
  - Have a question from day 1 that wasn't answered? Let us know here: https://bit.ly/UASWorkshopQandA
  - We'll be answering submitted questions from 9:30 – 10:15 tomorrow morning.

Tomorrow

- Summary of Day 1
- Q&A
- Experiences with Self-Driving Cars
- Breakout Session 2: Proposing Solutions
- Prioritization Exercise
- Next steps

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

Logistics

Safety

Conduct

Comfort

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.

Introductions

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

- 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

Day 1 Summary

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

Day 1 Summary

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

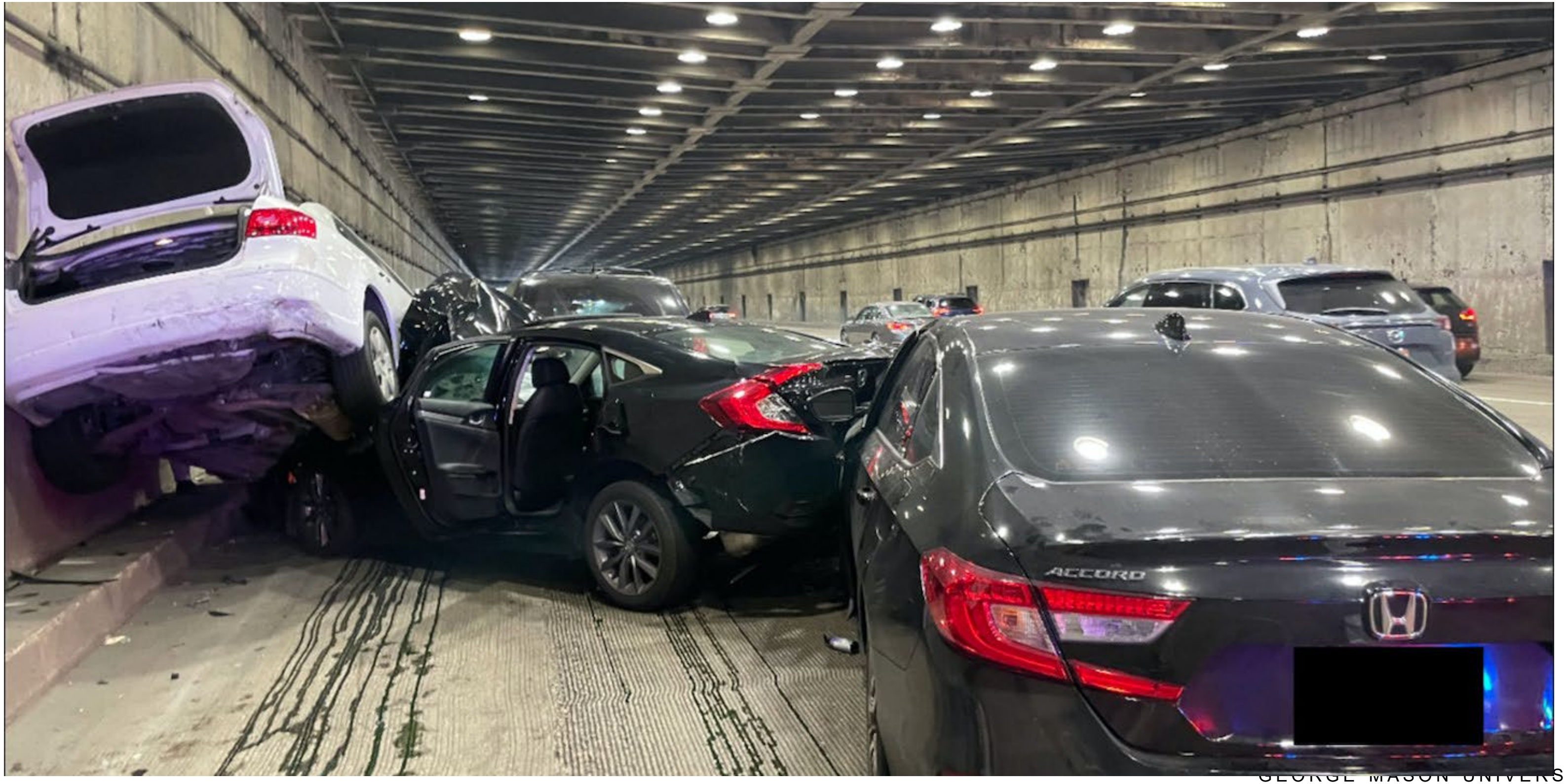
George Mason University

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

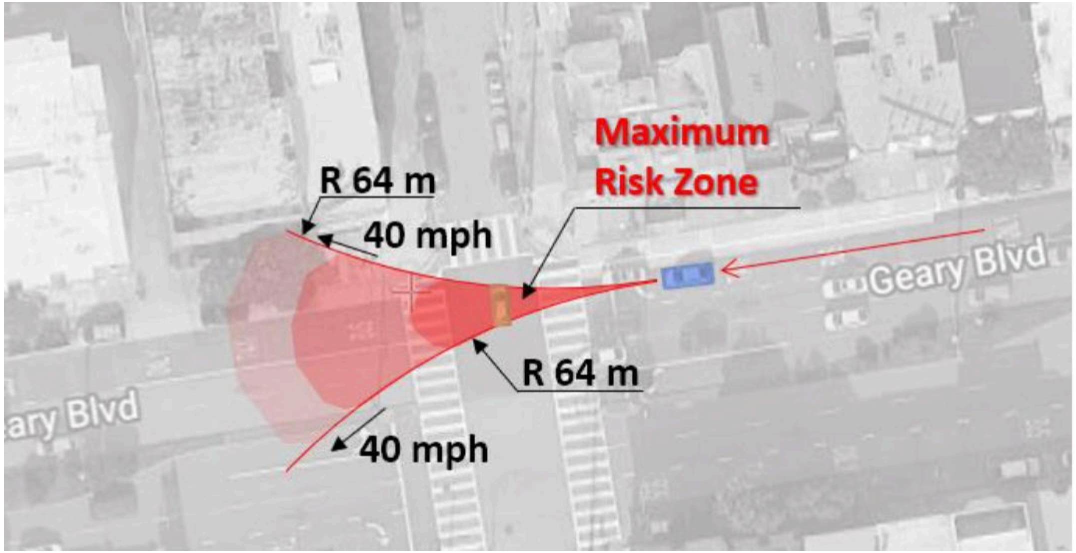
- Human errors in operation get replaced with human errors in coding
- Failure modes can be surprising
- Probabilistic estimates do not approximate judgment under uncertainty
- Maintaining AI is just as important as creating AI
- AI should be implemented with an understanding of system-level implications

Human errors in operation get replaced with human errors in coding

Failure modes can be surprising



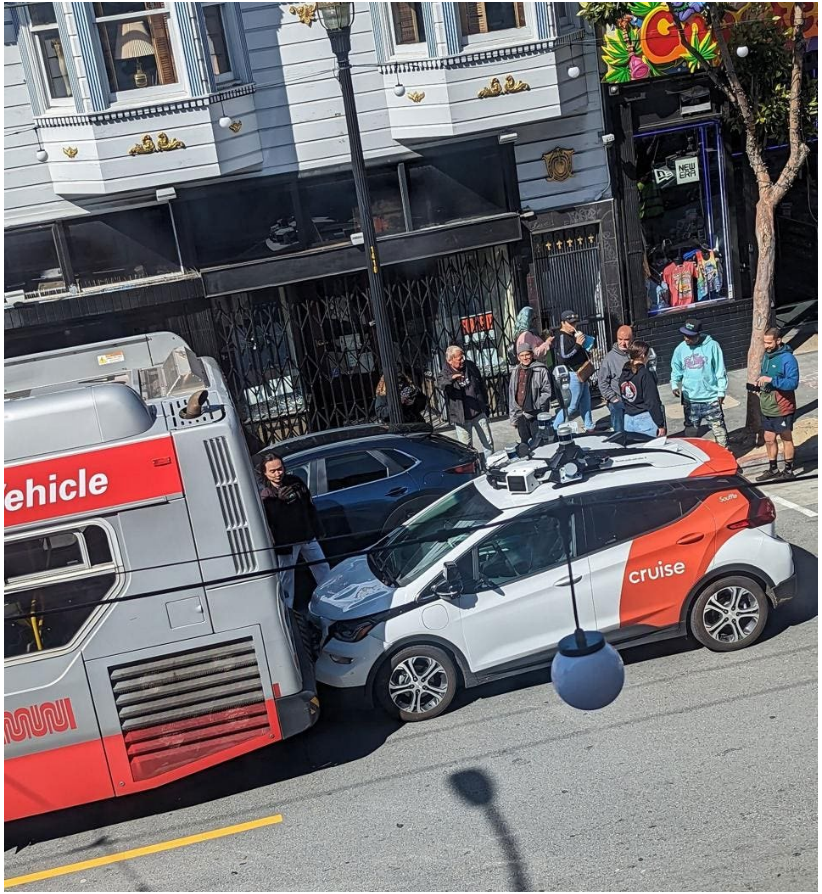
Probabilistic estimates do not approximate judgment under uncertainty



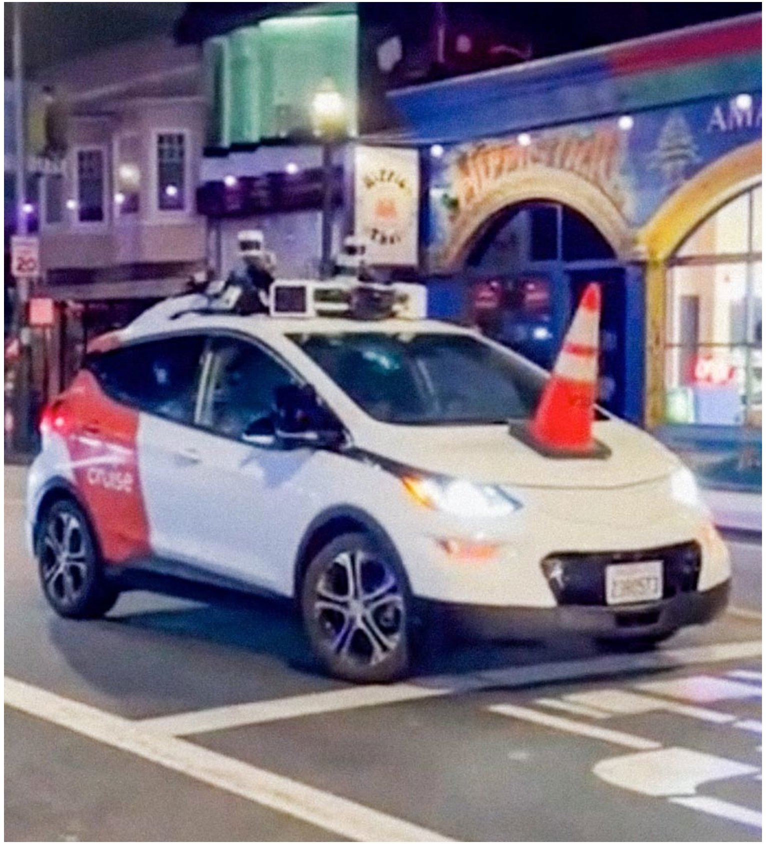
"The Cruise AV had to decide between two different risk scenarios and chose the one with the least potential for a serious collision."

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



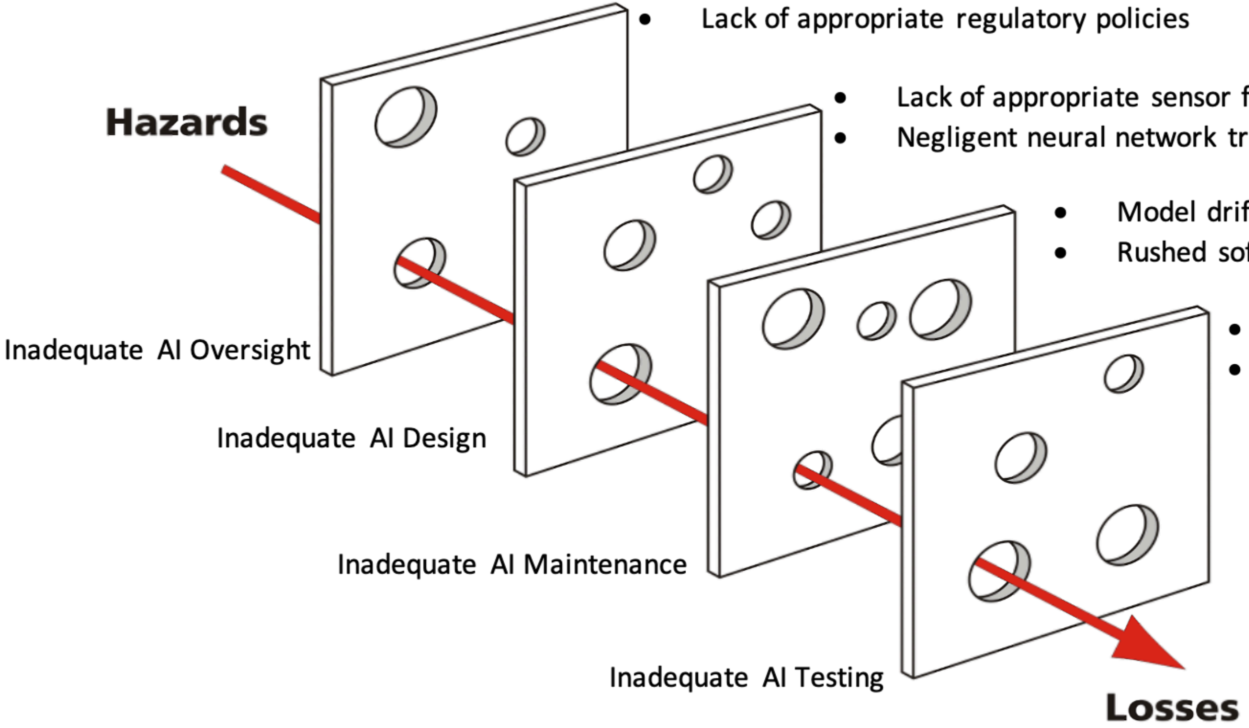
AI & Hazard Analysis

- 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.

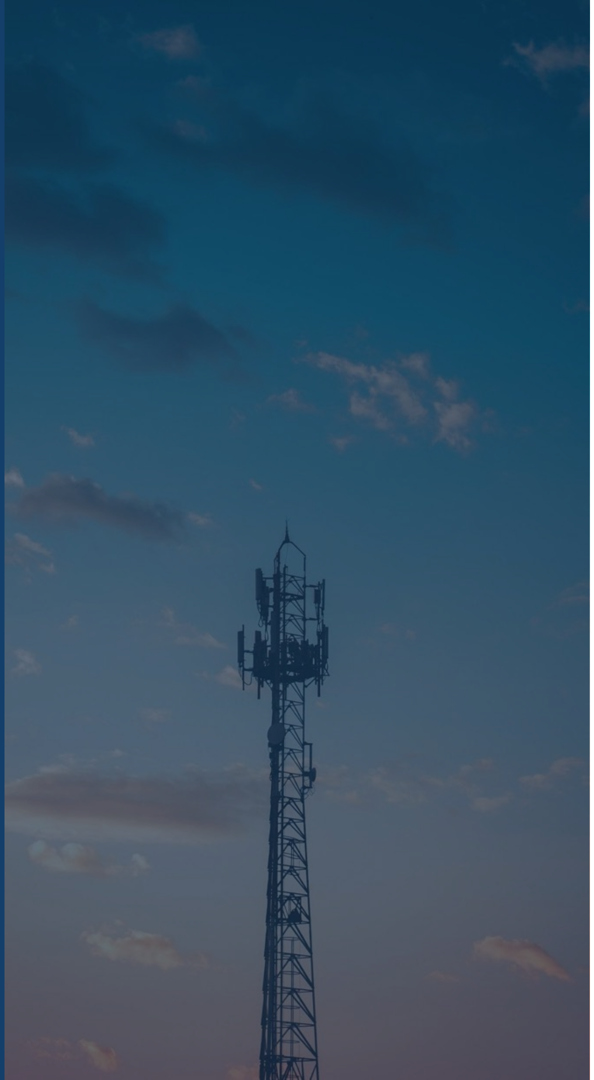
Slido

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


Thank You!
NIST
PUBLIC SAFETY
COMMUNICATIONS
RESEARCH