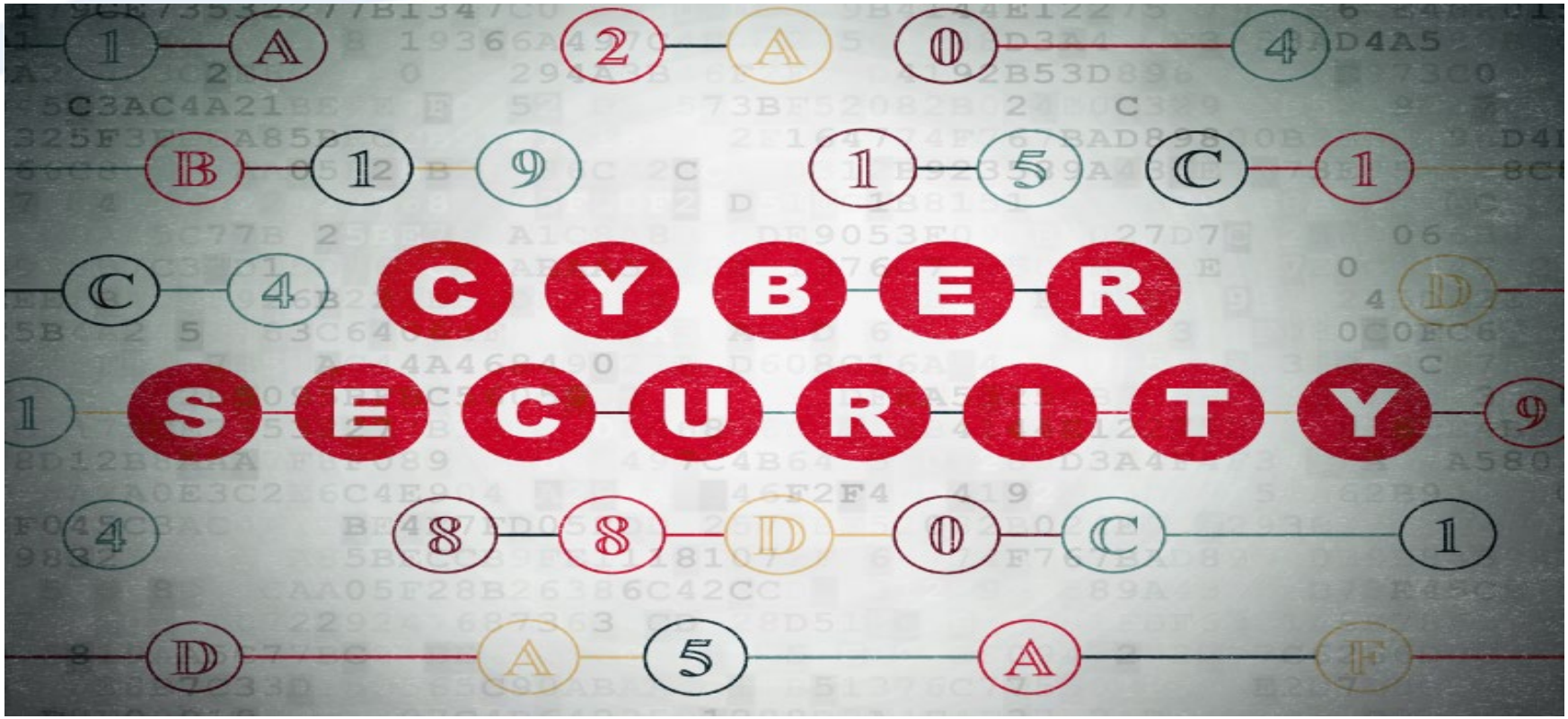
2019- 2023 FAA Cybersecurity R&D Plan



To: **Airports REDAC**

By: Isidore Venetos & Chuck Agava**,** ANG-E2, Aviation Research Division

Date: August 20, 2018

FAA

NextGEN

Today's Objective

Provide update on the FAA Cybersecurity R&D Plan

FAA Extension, Safety, and Security Act of 2016 Section 2111 Aviation Cybersecurity

Section 2111

(e) of the FAA Extension, Safety and Security Act of 2016, "…*the Administrator, … shall establish* a *cybersecurity research and development plan for the national airspace system…*"

- *Cooperation with international partners*
- *Risks of cabin communications and cabin information technology*
- *Objectives, proposed tasks, milestones, and a 5-year budgetary profile*
- One year after the date of enactment of the Act (7/15/2016)

FAA Reauthorization Act of 2018

Section 736- Cybersecurity Research and Development Program

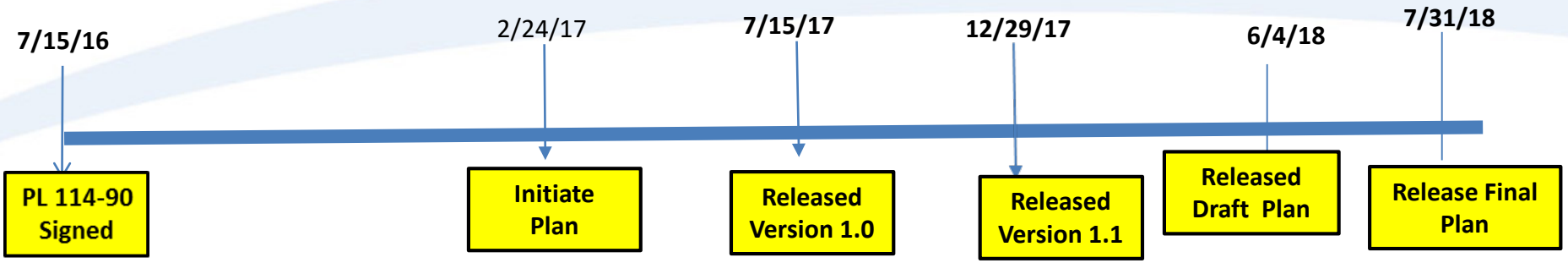
(a) Establishment- Not later than 6 months after the date of enactment of this act (5/7/2018), the FAA in consulation with other agencies as appropriate *shall establish* a *research and development program* *to improve the cybersecurity of civil aircraft and the national airspace system…"*

(a) Plan- Not later than 1 year after enactment of this act, the FAA shall develop a plan for the research and development program established under subsection (a) that contains Objectives, proposed tasks, milestones, and a 5-year budgetary profile

FAA

NextGEN

FAA Cybersecurity R&D Plan-Timeline



Milestones

- 2/24/17 ANG-E initiated action
- 4/21/17 Version 0.5 released for comments
- 4/24 – 5/26 Comments (~100) received and adjudicated
- **6/21/17** Briefed CSC
- **7/11/17** Briefed ANG-1 Staff
- **7/14/17** Released Version 1.0
- **8/17/17** Briefed ICCT
- **8/29 – 9/14** Briefed various REDAC Subcommittees
- 9/15 – 10/2 Comments (~100) received and adjudicated
- **10/11/17** Briefed REDAC
- **12/13/17** Briefed CSC
- **12/29/17** Released Version 1.1
- **4/30/2018** R&D Requirements Solicitation for 2019-2023 Plan
- **5/16/2018** Briefed CSC
- **5/17/2018** Briefed ICCT
- **6/20/2018** Briefed CSC
- 7/23/2018 Brief ANG-E
- 7/25/2018 Brief ANG-1

To Do

Align to R,E&D, F&E and AIP budget cycles

Align to Aviation Ecosystem

FAA Cybersecurity R&D Plan - Approach

Assessment

Discovery

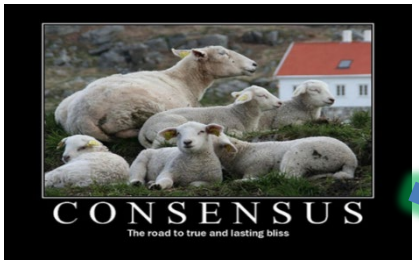
Cybersecurity Strategy 2017-2022
National Aviation Research Plan
FAA Budget Narratives
FY 2019 Budget Estimates
FAA Research Leads

Comments / Concurrence

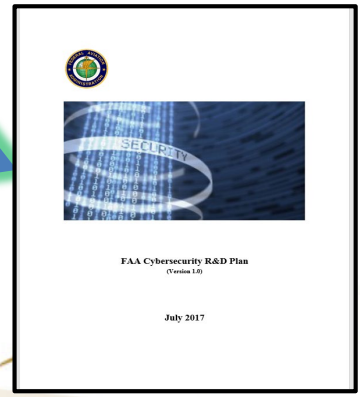
FAA (CSTAs and SMEs)
FAA Organizations

- Aviation Safety
- NextGen
- Air Traffic Organization
- Finance & Management
- Security & Hazardous Materials Safety

ICCT



Output



FAA

Updates to 2019-2023 R&D Plan

- **Included three new Research Requirements**
  - **Two UAS Requirements (Remote Data Link Identification, and UAS High Performance Command and Control (C2) Link Systems and Networks**
  - **NAS Cybersecurity Virtualization**
- **Revised Existing Research Requirements**
  - **Position, Navigation and Timing (PNT)**
  - **Flight Deck Data Exchange.**
  - **Aircraft System Information Security Protection (ASISP)**
  - **Identify and Authorization Management (IAM) Interoperability (IAM)**
  - **Situational Awareness Visualization/Threat Assessment**
- **Updated 5 year funding profile**
  - **Updated funding profile for UAS Cybersecurity Requirements**
  - **Updates to include FY 23 funding estimates**
- **Updated the Section on Technical Collaborations/Partnerships**

FAA

NextGEN

Cybersecurity Research Program- Lifecycle Strategy

R&D Landscape

We are here

Planning

- Projects: allocate to Portfolio Areas
- Resources: optimize workforce, budget & capabilities

No Duplication

Execution

FAA
Partner
(industry/academia /gov't)
Private sector

Collaboration, Partnerships & Private

Outcome

NARP Goals Annual Review

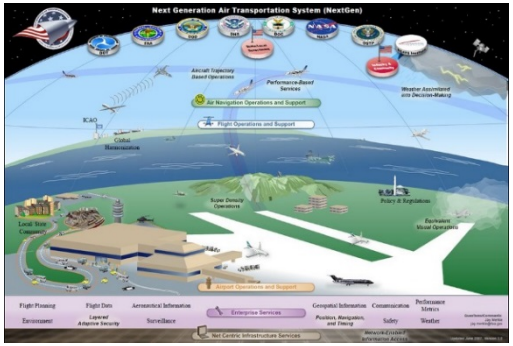
Communicate results

Evaluate R&D Outcomes

FAA

NextGEN

Notional Representation of Aviation Cyber Landscape



Aviation Eco-System

"Aviation Eco-system is an extensive multi-layered network of intersecting elements with integral roles in the Aviation Domain and the Six A's (6As) comprising the ecosystem include Airports, Airlines, Aircraft, Airlift, Actor and Aviation Management". NAS falls under the aviation management and the aviation ecosystem represents a more holistic, robust description of the reality of modern aviation and more fully captures the global scope and complexity of the industry"- National Strategy for Aviation Security (NSAS), May 2018

Alignment to CSC Strategic Plan: 2018 - 2023

CSC Steering Committee

- FAA Chief Information Security Officer
- Office of Aviation Safety
- Security & Hazardous Materials Safety
- Air Traffic Organization
- NextGen
- DOT Chief Information Security Officer

Core Cybersecurity Goals 2018-2023

Governance • Vulnerability Management • Security Architecture, Policy, and Standards • Systems and Applications Security • Continuous Diagnostics and Monitoring • Security Operations

Goal 1	Goal 2	Goal 3	Goal 4	Goal 5
Refine and maintain a cybersecurity governance structure to enhance cross-domain synergy	Protect and defend FAA networks and systems to mitigate risks to FAA missions and service delivery	Enhance data-driven risk management decision capabilities	Build and maintain workforce capabilities for cybersecurity	Build and maintain relationships with external partners in Government and industry to sustain and improve cybersecurity in the aviation domain
Objectives	**Objectives**	**Objectives**	**Objectives**	**Objectives**
1.1 Maintain cross-organization processes for cybersecurity strategic planning and budget development 1.2 Codify and maintain FAA-wide Cybersecurity Roles & Responsibilities 1.3 Improve understanding of cybersecurity risk for FAA owned, contracted and regulated systems 1.4 Increase integration of cybersecurity activities across Domains 1.5 Update and maintain FAA-wide information security policies 1.6 Implement the NIST Cybersecurity Framework to Manage Risk	2.1 Improve cyber threat intelligence collection, processing, dissemination, and reporting 2.2 Improve FAA cyber monitoring, detection and response capabilities 2.3 Improve privileged user control, monitoring and visibility 2.4 Improve capabilities for detection and mitigation of threats, internal and external 2.5 Leverage cybersecurity research and development across FAA domains and systems 2.6 Ensure FAA Information Security Controls, Policies and Processes are aligned with current NIST Standards and Guidelines	3.1 Continue development and enhancement of an enterprise cyber threat modeling capability 3.2 Expand Information Security Continuous Monitoring capabilities for NAS and non-NAS IP systems 3.3 Integrate threat, attack and vulnerability data with mission focus to prioritize risks 3.4 Reduce the time required to address high value threats and vulnerabilities	4.1 Enhance FAA-wide cybersecurity training, education and awareness program 4.2 Support cyber workforce training through participation in exercises 4.3 Ensure personnel having cybersecurity responsibilities receive appropriate role-based training 4.4 Enhance FAA competitiveness in cybersecurity hiring and retention through adoption of current Federal IT Job Series	5.1 Expand participation in cyber exercises with external partners 5.2 Increase collaboration with other Government, industry and private sector cybersecurity teams 5.3: Ensure cybersecurity requirements are addressed in the AMS and all FAA contract vehicles (ACQ) 5.4 Expand information sharing with appropriate external partners including through automated cyber threat indicator sharing 5.5 Leverage regulatory role to identify and address cybersecurity risks in aircraft systems as well automation of aircraft, equipment and technology 5.6 Represent the United States in global engagement on aviation cybersecurity through partnership and engagement with international partners

FAA

Cybersecurity R&D Plan- Funding Profile

Research Requirement	Research Area	2019 Requested	2020 Planned	2021 Estimate	2022 Estimate	2023 Estimate
Aircraft Systems Information Security Protection	Security & Resiliency	$2,100K	$2,600K	*$2,500K*	*$2,500K*	*$2,300K*
Cybersecurity Risks of Cabin Communication	Security & Resiliency	$0K	$2,000K	$2,000K	$2,000K	TBD
Command and Control Beyond Radio Line of Sight Networked Systems Security Protection	Security & Resiliency	*$465K*	*$480K*	*$485K*	*$0K*	*$0K*
Comprehensive UAS Cybersecurity Risk Management Framework	Security & Resiliency	*$1,500K*	*$1,000K*	*$1,000K*	*$1,000K*	*TBD*
UAS Remote Identification	Security & Resiliency	*$0K*	*TBD*	*TBD*	*TBD*	*TBD*
UAS High Performance Command and Control (C2) Link Systems and Networks	Security & Resiliency	$0K	$600K	*$600K*	*TBD*	*TBD*
ASISP Response and Recovery	Response & Recovery	*$0K*	*$0K*	*$1,000K*	*$1,500K*	*$1,500K*
Cybersecurity NAS Virtualization	Data Analytics & Informatics	*$1,000K*	*$1,500K*	*$1,500K*	*$1,000K*	*$1,000K*
Flight Deck Data Exchange	Data Analytics & Informatics	$1,000K	$2,100K	*$2,200K*	*$2,200K*	*$1,000K*
NextGen Information Security	Data Analytics & Informatics	$1,230K	$1,000K	*$1,000K*	*$1,000K*	*TBD*
Identity and Authorization Management Interoperability	Data Analytics & Informatics	*$3,250K*	*$3,250K*	*$3,000K*	*$1,000K*	*$0K*
Unmanned Aircraft Systems Security Capability	Data Analytics & Informatics	$0K	$550K	*$685K*	*$685K*	*TBD*
Cyber Positioning, Navigation and Timing	Data Analytics & Informatics	$0K	$500K	*$800K*	*$800K*	*$800K*
Unmanned Aircraft Control Station Ground to Ground Communication with the NAS	Data Analytics & Informatics	*$0K*	*$750K*	*$500K*	*$500K*	*TBD*
Situational Awareness Visualization, Threat Assessment and Compliance	Response & Recovery	*$1,000K*	*$2,000K*	*$1,500K*	*$500K*	*$0K*
Total		**$11,545K**	**$18,330K**	**$18,770K**	**$14,685K**	**$8,100K**

Key Takeways

- **Align the R&D Plan to the Aviation Ecosystem and 2019-2024 Cybersecurity Strategy Goals**
- **Annual updates to the plan aligned to R,E&D, F&E and AIP budget cycles**

FAA

NextGEN

For more information, contact:

Isidore Venetos
Manager, Aviation Cybersecurity R&D, Aviation Research Division
609-485-5207
isidore.venetos@faa.gov

Chuck Agava
Aerospace Engineer
ANG-E2, Aviation Research Division
609-485-5357
chakradhar.agava@faa.gov

FAA

NextGEN

Cybersecurity R&D Plan – Research Requirements

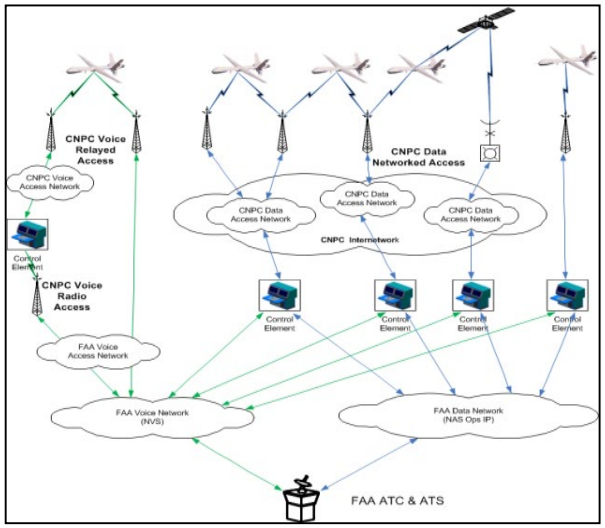
Research Area: Security and Resiliency

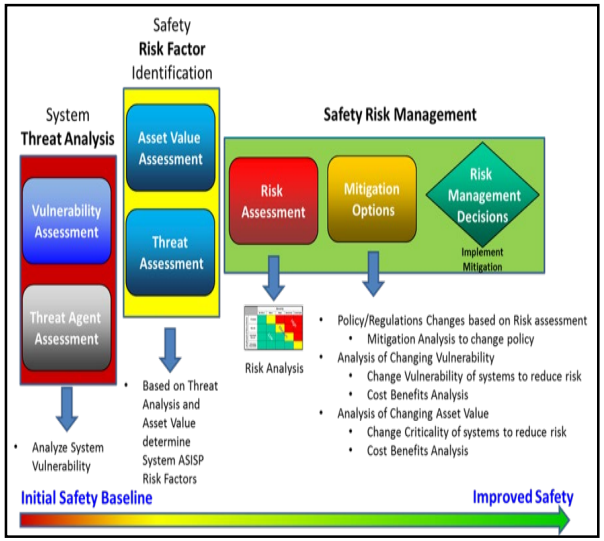
Develop methods to enhance FAA's ability to prevent, detect, and respond to cyber attacks

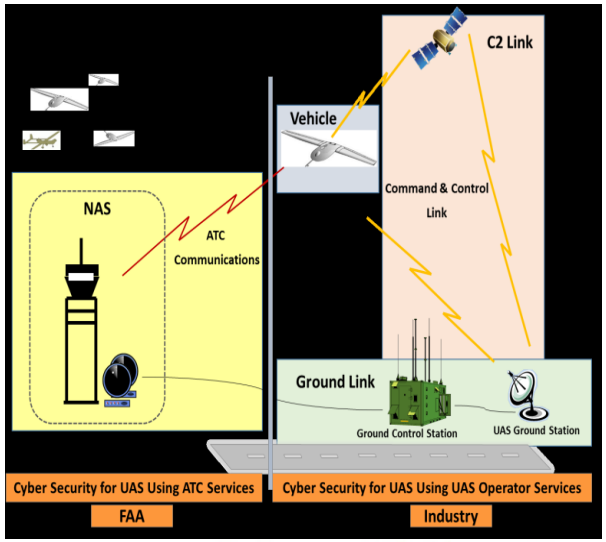
- ✓ **UAS C2 Link Systems Security Protection** research directly supports the development of FAA new TSO requirements and AC guidance for UAS new, unique and safety critical C2 Beyond Line of Sight (BLOS) networked terrestrial and satellite Link Systems security control.

- ✓ **The ASISP** research will assess/analyze wired and wireless connectivity to aircraft systems to identify information-security-protection vulnerabilities and risks that could adversely affect the safety of an aircraft

- ✓ **The Cabin Communications** research will provide insights into information-security-protection vulnerabilities of, and risks to, cabin communication and information technology systems, associated components/networks







FAA

NextGEN

Cybersecurity R&D Plan – Research Requirements

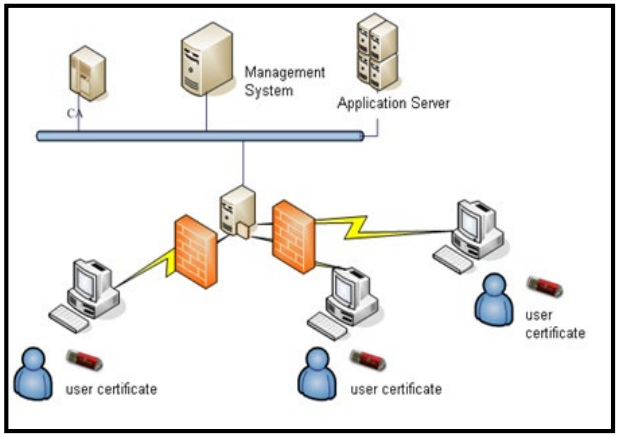
Research Area: Data Analytics and Informatics

Develop analytical capabilities for aggregating and correlating current data with the intent of understanding, predicting, and responding to cyber attacks for system-wide safety assurance

- ✓ **The Flight Deck Data Exchange** research supports enhanced data exchange between onboard avionics systems and ground systems to enable Trajectory Based Operations (TBO)

- ✓ **The Identify and Authorization Management (IAM)** research will assess, and analyze the expansion of IAM with domestic and international Public Key Infrastructure (PKI) systems, and recommend solutions for interoperability, capacity, and architectural issues that arise with domestic, and international aviation partners.

- ✓ **The NextGen Information Security** research supports the FAA's overall cyber security posture through development of advanced tools, techniques and processes that can be adapted for use in the NAS.



FAA

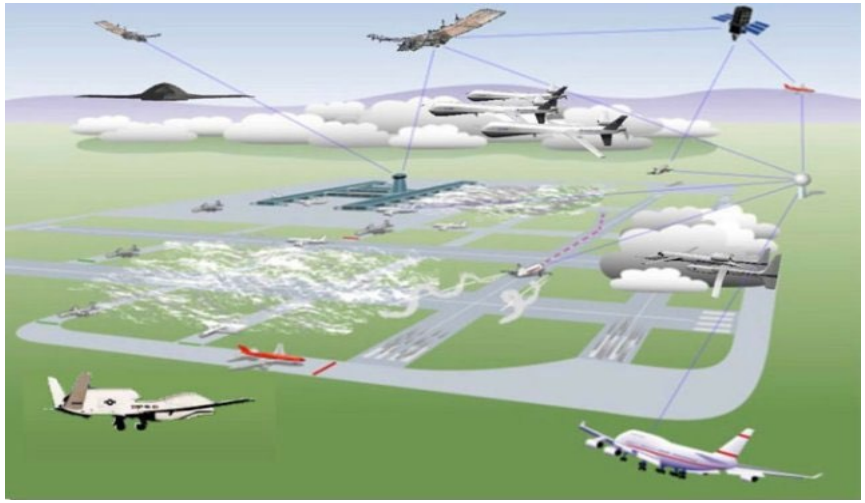
NextGEN

Cybersecurity R&D Plan – Research Requirements

Research Area: Response and Recovery

Develop and validate algorithms, policies, training, and procedures to detect and respond to cyber attacks

- ✓ **The Situational Awareness Visualization** research will identify, integrate, evaluate, and provide recommendations for products that enhance the situational awareness visualizations available to operators and maintainers of NAS

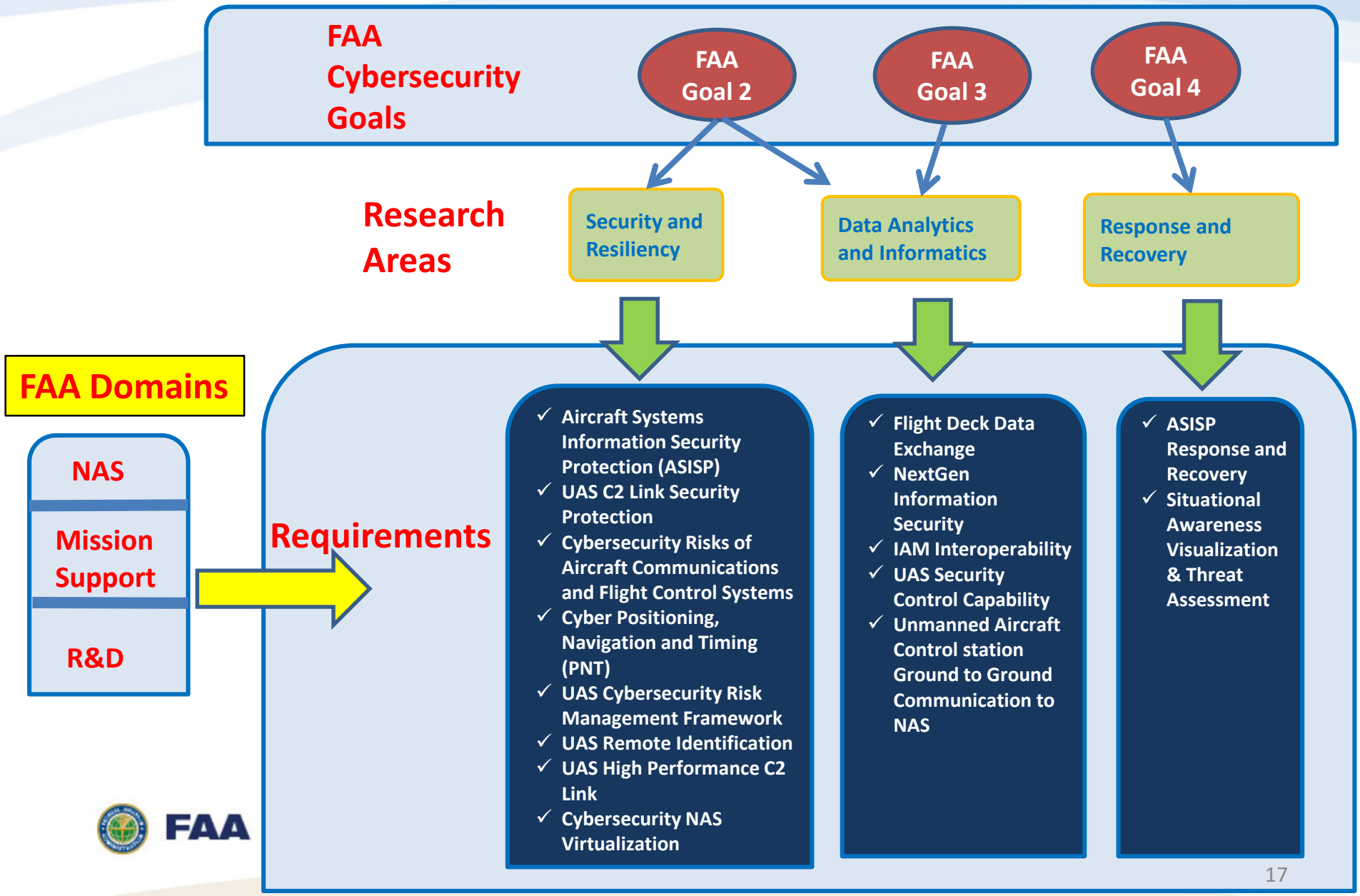


- ✓ **The ASISP Response and Recovery** research will provide human factors data and context to study pilot responses to cyber-attacks

FAA

NextGEN

Cybersecurity R&D Plan- Framework



FAA

Cybersecurity R&D Plan - Partnerships

CRDAs

FFRDCs

RTCA

SC-216

SC-222

SC-223

SC-228

ASSURE

BOEING

Astronautics Corporation of America

Industry & Academia

Aviation Safety

Security & Hazardous Materials

Finance and Management

Air Traffic Organization

NextGen

International

ICAO · OACI · ИКАО

EASA European Aviation Safety Agency

SESAR

Government Agencies

NIST National Institute of Standards and Technology U.S. Department of Commerce

DHS

NASA

Cybercom

DOD

FAA

NextGEN

SC-216 - Aeronautical Systems Security
SC-223 - Internet Protocol Suite (IPS) and AeroMACS

SC-222 - Minimum Aviation Performance Standards
SC-228 – Minimum Performance Standards- UAS

Integrated Cyber Risk Management Framework

Holistic Approach to Assessing and Mitigating Cyber Threats

FAA

NextGEN