FAA Unmanned Aircraft Systems (UAS)

Cyber Security Initiatives

Presented To: Information Security and Privacy Advisory Board (ISPAB)

Presented By: Stephen George, Manager – Airworthiness, FAA UAS Integration Office

Date: February 11, 2015

Overview

1. **Understanding Stakeholders and their Needs**
2. **FAA Perspective on the Scope**
3. **Where Are We Today?**
   - FAA Regulatory Policy, Orders, and Guidelines
   - UAS Airborne Radio Standards Development
4. **Next Steps**

Stakeholders and their Needs

- **FAA**
- **Agencies For National Security**
- **Aircraft, Avionics OEMs**
- **UAS Owners and Operators**
- **Users of National Airspace System (NAS)**

- **Others (Society, Privacy Advocates, etc.)** 

FAA Perspective on the Scope

Security

- Threat to Critical National Assets
- FAA Systems
- UAS Systems
- Operational Information

Privacy

- UAS Operator's business
- Non-participants'/Personal

FAA Perspective on the Scope

- **We've used several terms for security from electronic attacks on aircraft networks and systems:**
  - Network security, information security, systems security, and cyber security
- **We are now trying to standardize on the term**
  - Aircraft Systems Information Security Protection (ASISP)
    - more to follow on ASISP

FAA Perspective on the Scope

- **We're talking here only about UAS: not air traffic services and providers**
  - U.S. governmental services have their own programs for information security
- **U.S. Governmental Air Traffic Services**
  - Have been certified and accredited in accordance with the Federal Information Security Management Act (FISMA), FAA Order 1370.82A Information Systems Security Program and the FAA Information Systems Authorization Handbook
- **For purposes of ASISP, we consider U.S. Government Air Traffic Services to be secure**

Where Are We Today?

1. **Current FAA Regulatory Policy, Orders, and Guidelines**
   - Non-Government Services
   - Aircraft System
   - Aircraft Operations
2. **UAS Airborne Radio Standards Development**
   - Safe, Secure and Efficient Integration into the NAS

Non-Government Services

- **Examples of non-government services**
  - Airline Networks (Airline Operations Centers)
  - Commercial Systems (e.g., Internet, Cellular Network)
  - Data Loaders (e.g., Maps, Flight Plans and Databases)
  - Wireless Aircraft Sensors and Sensor Networks
  - Ground Support Equipment
  - Command and Control System

Regulations, Policy, Standards and Guidance

- Information Security
  - There are many information processing standards and guidance that might be able to be used in the ASISP context
    - Federal Information Processing Standards (**FIPS**)
    - National Institute of Standards and Technology (**NIST**)
    - International Standards Organization (**ISO**)
  - RTCA SC-216 produced the following standard:
    - DO-355 *Information Security Guidance for Continuing Airworthiness*

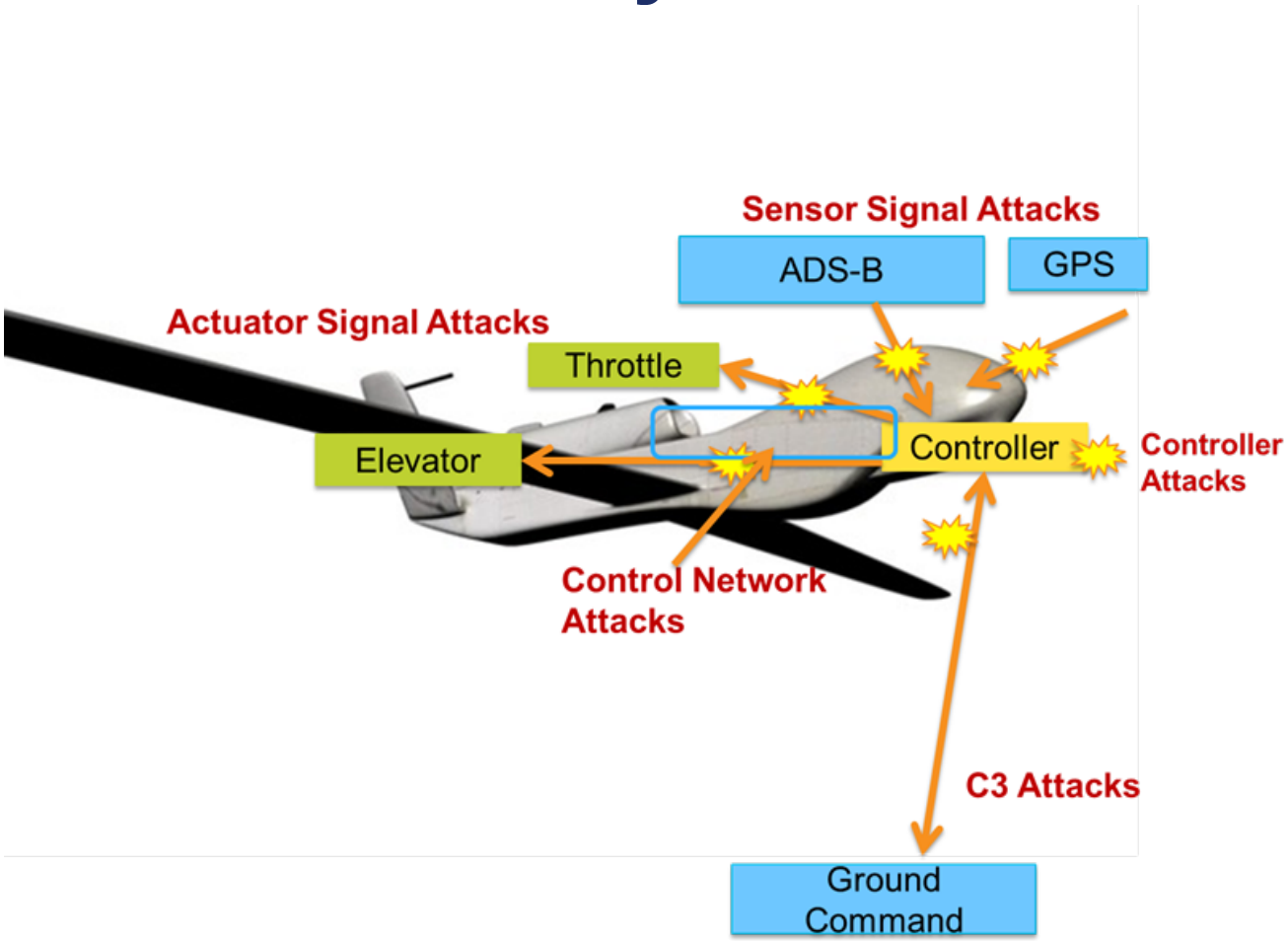
Regulations, Policy, Standards and Guidance

- Aviation Security
  - There are industry activities such as:
    - ARINC 811 *Commercial Aircraft Information Security Concept of Operation and Process*
    - ARINC 835 *Guidance for Field Loadable Software Using Digital Signatures*
    - ARINC 842 *Guidance for Using Digital Certificates*
    - ARINC Network Infrastructure and Security (NIS) Subcommittee (drafts/reports)
    - ARINC AGIE/MAGIC Subcommittee (drafts/reports)
  - RTCA SC-216 also produced the following standard:
    - DO-356 *Airworthiness Security Methods and Considerations*

UAS Standards – Safe, Secure, Efficient

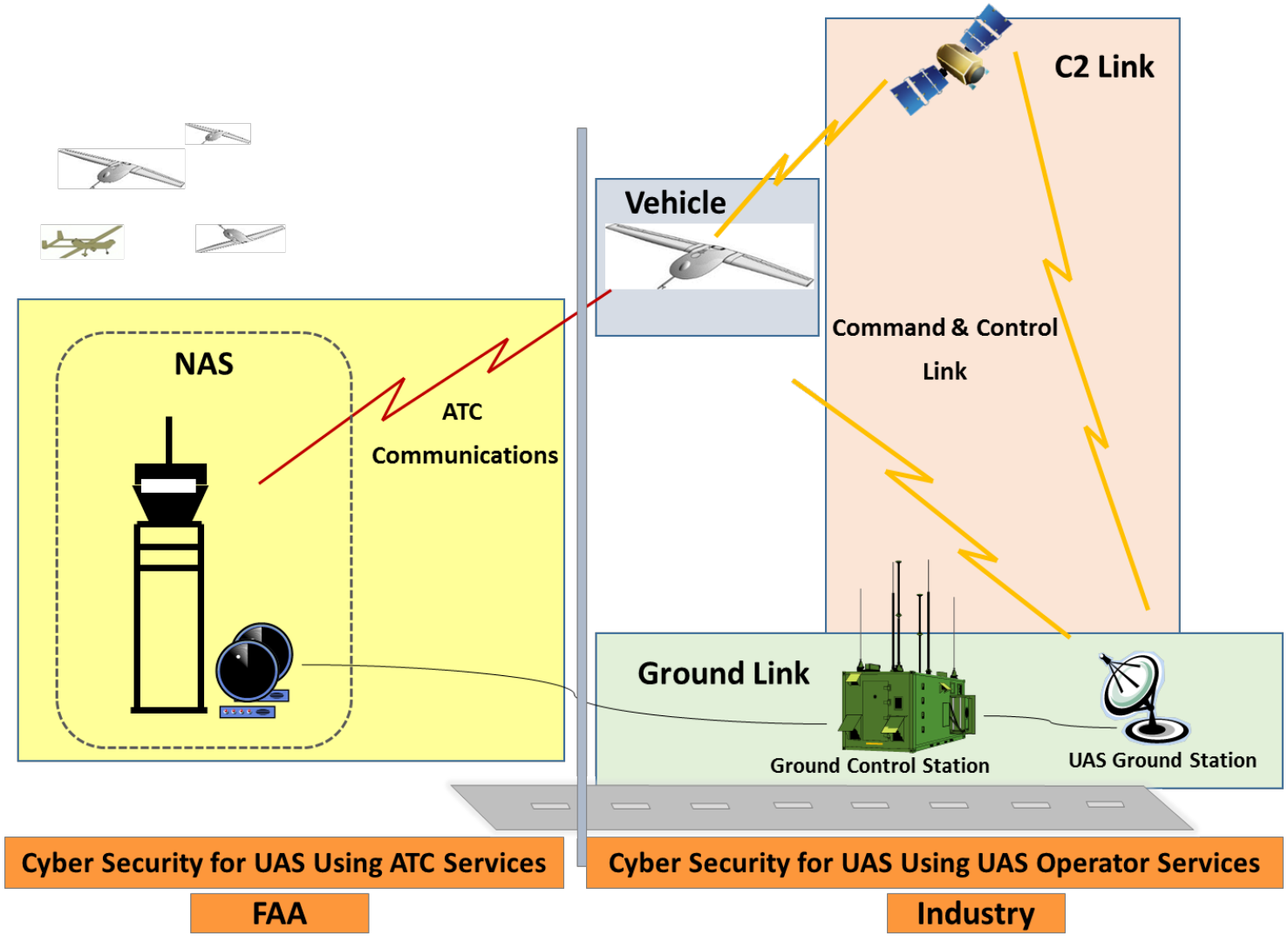
- **In December 2013, FAA tasked RTCA to develop Minimum Operational Performance Standards for C3 radio link**
  - Phase I standards expected in 2016

UAS Vulnerability Overview



- Diverse attack vectors – from intercepting communications to firmware exploits

Components of UAS Security



Next Steps

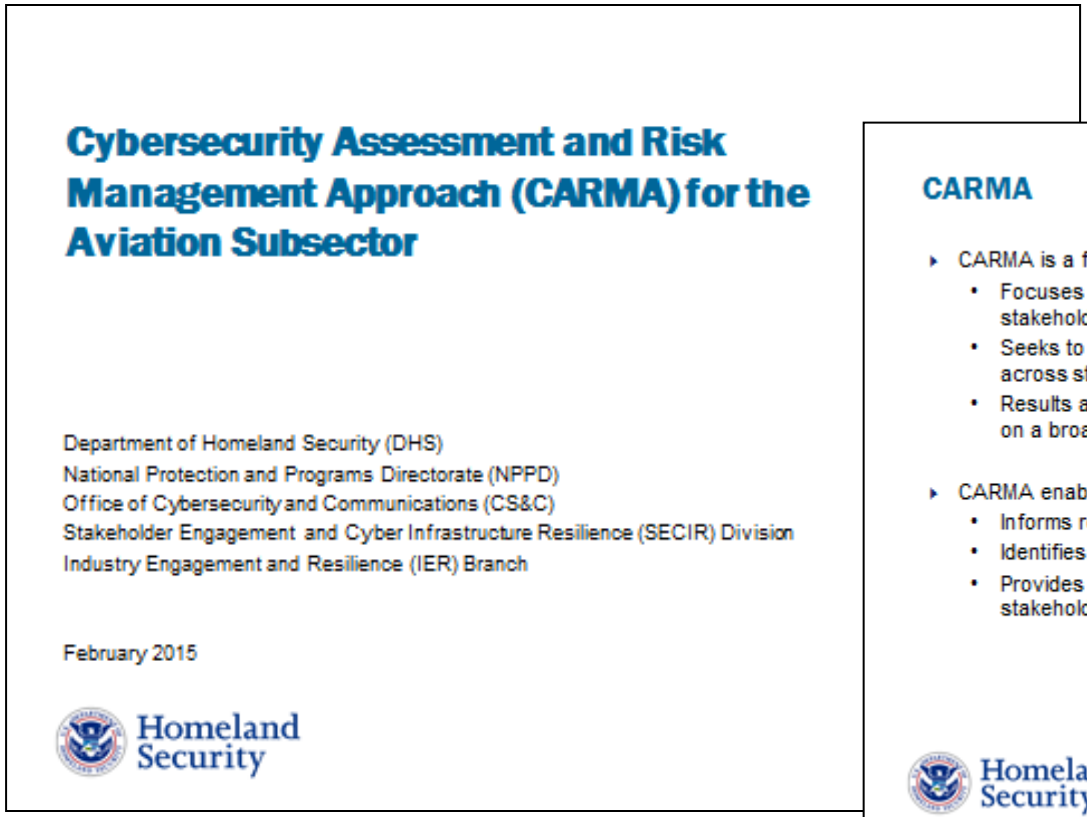
- **Advisory and Rulemaking Committee (ARAC)**
- **Learn from other government agencies**
- **Continued participation with industry**
- **Integrated Project Plan**

Next Steps…
Advisory and Rulemaking Committees

- **Aircraft Systems Information Security/Protection (ASISP)**
  - The FAA issued a notice of assignment for Aviation Rulemaking Advisory Committee (ARAC) on February 3, 2015: reference https://federalregister.gov/a/2015-01918
  - Assigned the Aviation Rulemaking Advisory Committee (ARAC) a new task to provide recommendations regarding Aircraft Systems Information Security/Protection (ASISP) rulemaking, policy, and guidance on best practices for airplanes and rotorcraft, including both certification and continued airworthiness.
  - Issue: without updates to regulations, policy, and guidance to address ASISP, aircraft vulnerabilities may not be identified and mitigated, thus increasing exposure times to security threats.
  - In addition, a lack of ASISP-specific regulations, policy, and guidance could result in security related certification criteria that are not standardized and harmonized between domestic and international regulatory authorities.

Next Steps… Learn from others

- Risk Management Process Applied to Aviation Sector Critical Infrastructure
  - The CARMA Approach

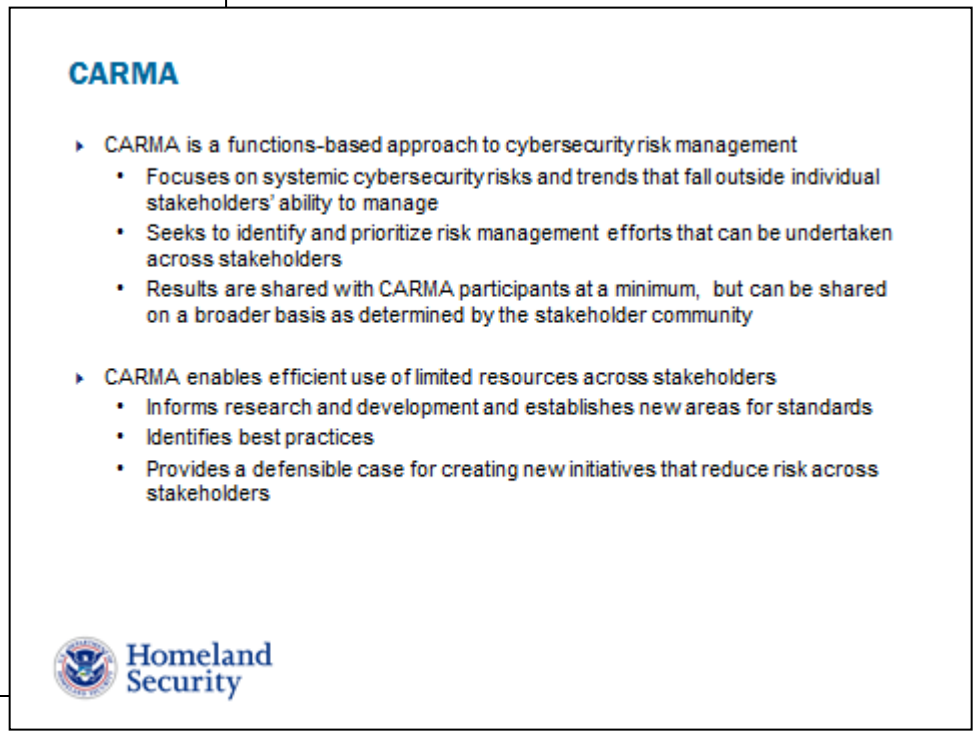


Cybersecurity Assessment and Risk Management Approach (CARMA) for the Aviation Subsector

Department of Homeland Security (DHS)
National Protection and Programs Directorate (NPPD)
Office of Cybersecurity and Communications (CS&C)
Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) Division
Industry Engagement and Resilience (IER) Branch

February 2015

Homeland Security



CARMA

- CARMA is a functions-based approach to cybersecurity risk management
  - Focuses on systemic cybersecurity risks and trends that fall outside individual stakeholders' ability to manage
  - Seeks to identify and prioritize risk management efforts that can be undertaken across stakeholders
  - Results are shared with CARMA participants at a minimum, but can be shared on a broader basis as determined by the stakeholder community
- CARMA enables efficient use of limited resources across stakeholders
  - Informs research and development and establishes new areas for standards
  - Identifies best practices
  - Provides a defensible case for creating new initiatives that reduce risk across stakeholders

Homeland Security

Questions, Discussion, Suggestions

Backup

Background on ARAC-ASISP

- **ARAC**
  - As a result of the December 18, 2014 ARAC meeting, the FAA assigned the ARAC a new task to provide recommendations regarding ASISP rulemaking, policy and guidance on best practices for aircraft systems including both certification and continued airworthiness
- **Policy**
  - The FAA issued a Policy Statement for ASISP: PS-AIR-21.16-02, *Establishment of Special Conditions for Cyber Security*, March 6, 2014
- **Guidance**
  - We're focusing in, for the most part, on connectivity to the outside of aircraft.

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

January 14, 2015

The Representative at FAA

On behalf of the Information Security and Privacy Advisory Board (ISPAB) and its Chairman, Dr. Peter Weinberger, we would like to invite you to speak to the Board. The Board looks forward to hearing from you on Unmanned Aircraft Systems (Drones). At the last meeting on October 23, 2014, the Board was presented different perspectives from a panel presenting on Drones and Privacy http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-10/october-2014.html. The Board would like to continue the discussion to include FAA presentation.

The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy. ISPAB advises the Secretary of Commerce and the Director of the Office of Management and Budget on emerging information security and privacy issues pertaining to Federal Government Information Systems. You can locate additional information about the ISPAB on its website: http://csrc.nist.gov/groups/SMA/ispab/index.html. Copies of the current list of members and their bios, the Board's charter and past Board activities are among the items you will find posted there.

The meeting is being held on February 11, 12, and 13, 2015, at the US Access Board, 1331 F Street N.W., Suite 800, Washington, DC, 20004. It is located next to block from Metro Center Station. I look forward to receiving your confirmation. Please get in touch with me if you have any further questions.

Thank you.
Regards,
Annie W. Sokol
IT Specialist
Computer Security Division, Information Technology Laboratory (ITL)
&
Federal and Industrial Relations Office, ITL
National Institute of Standards and Technology (NIST)
Department of Commerce
301-975-2006 (Voice)