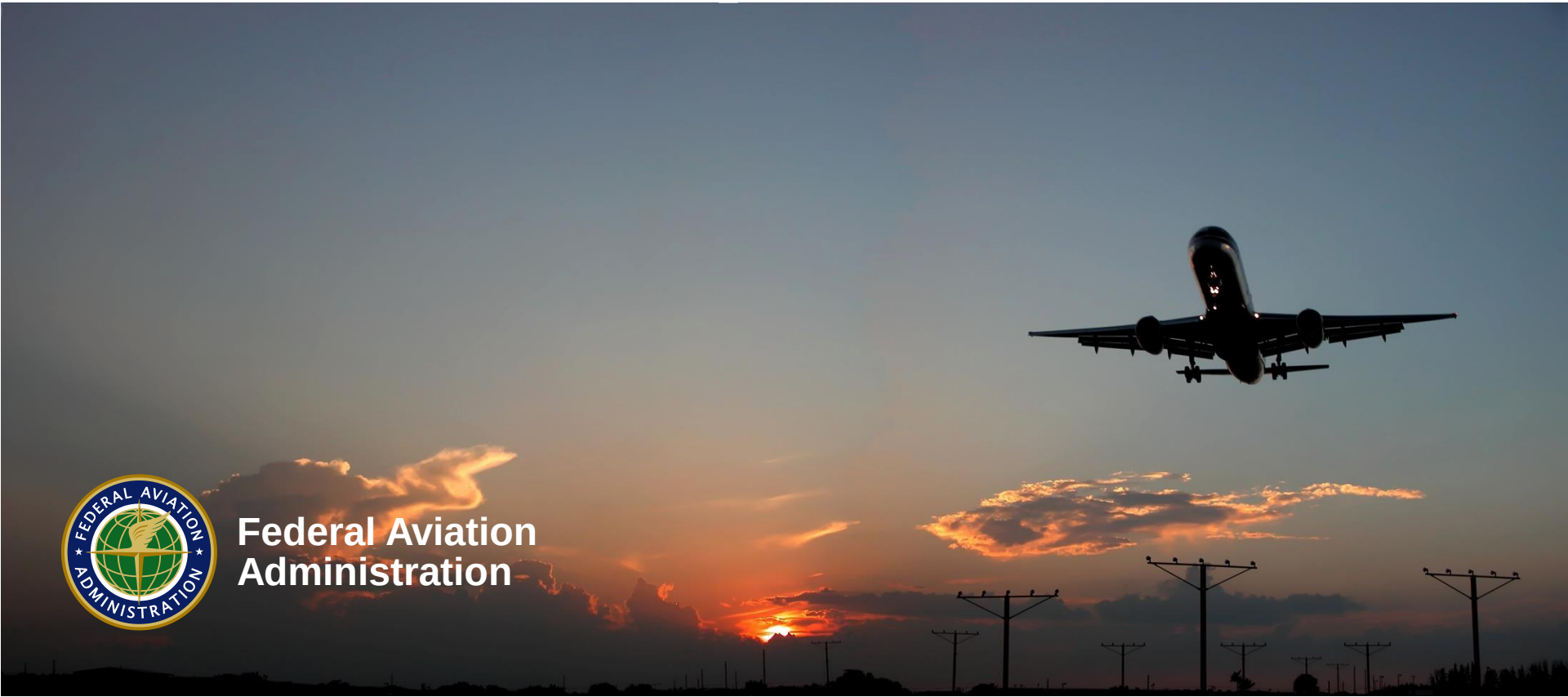
2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem | "Cyber Hygiene"

NAS Cyber Operations

Date: October 20, 2020



NAS Cyber Operations

- Mission Statement
  - Minimize the impact of cyber security events and incidents in support of availability and restoration requirements for NAS critical and essential services.
- Mission Essential Tasks (METs):
  - Monitor NAS cyber environments
  - Conduct NAS cyber event analysis
  - Create the Cyber-Common Operation Picture (C-COP)
  - Support mission assurance
  - Conduct active cyber defense
  - Coordinate cybersecurity NAS event/incident response
  - Track incident mitigation implementation and closure

NAS Cyber Operations

- Governed by the following FAA Notices and Orders
  - **FAA Notice JO 1370.50**, NAS Information Security Incident Detection, Reporting and Response, designated the NCO as the focal point for NAS Cybersecurity activities
  - **FAA Order 6000.15**, General Maintenance Handbook for NAS facilities, requires reporting of suspected NAS cyber security events to the NCO
- Staffed to support 24/7/365 operations since August 2013
  - Located at the Air Traffic Control System Command Center (ATCSCC) in Warrenton, VA

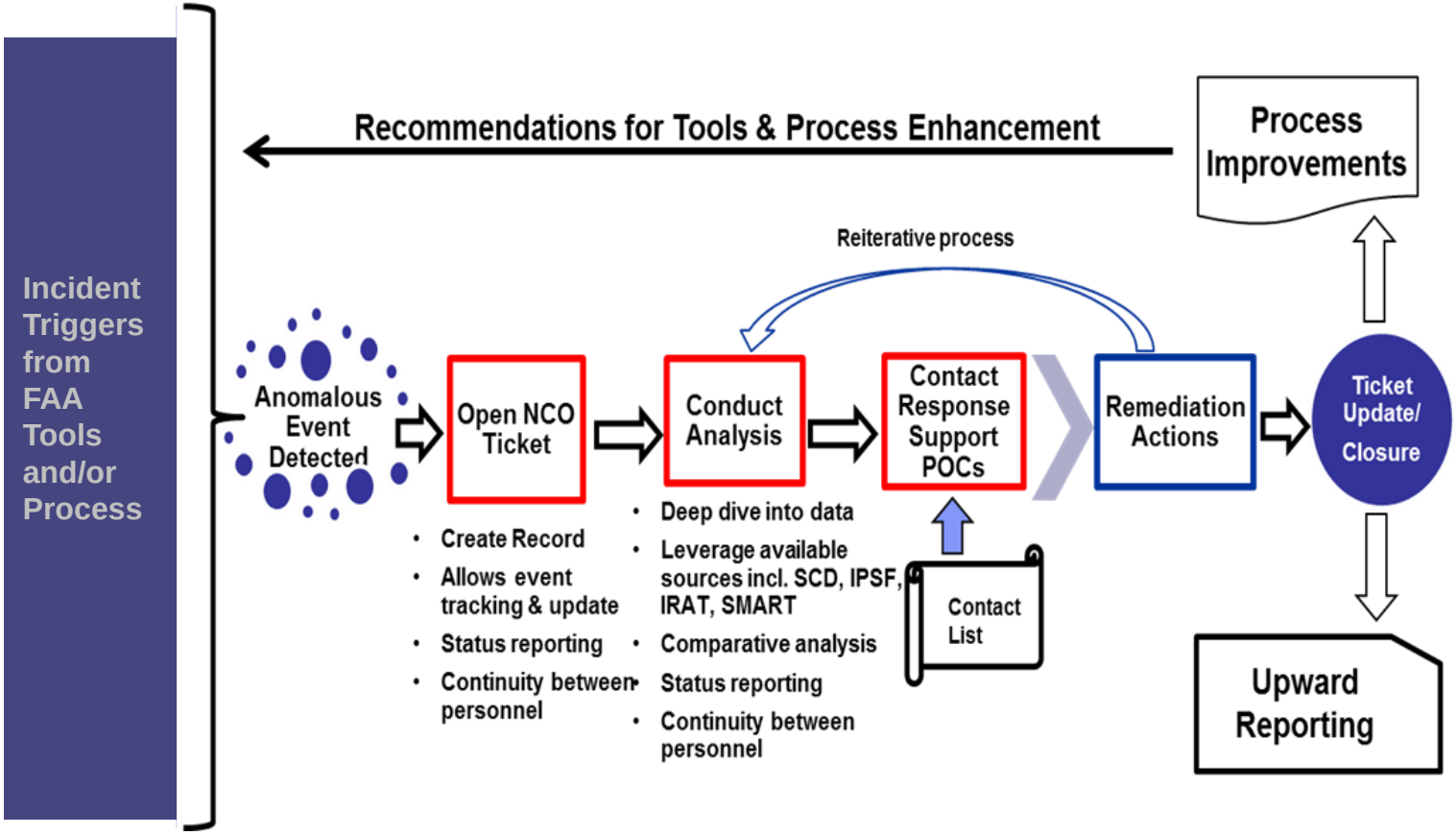
NAS Cyber Security Monitoring

- The NAS is an Industrial Control System (ICS) with the following network environment characteristics:
  - Static in nature
  - Limited number of applications
  - Specialized user base
- Monitoring the NAS environment differs greatly from monitoring a standard IT networking environment and focuses on:
  - Minimizing impact to operations (as passive as possible)
  - Baseline modeling
  - Detecting baseline changes
  - “Whitelisting” and “Fingerprinting”

NCO Event Analysis/Response

- NCO performs NAS centralized cyber event monitoring and response functions, including:
  - Analyzing system cyber event information to identify events that require response actions
  - Performing cyber event trend analysis
  - Assessing all cyber events/alerts/incidents generated from monitoring sources
  - Coordinating/tracking NAS cyber event response/remediation activities
  - Supporting upward and outward situational awareness across FAA organizations and external agencies

Incident Response Process



Coordination

- **Enterprise Control Centers**
  - SECC, VECC, and NECC will notify NCO of any cyber concerns or anomalies in the scope of responsibility
- **NOCC**
  - experts in the NAS that provide NAS impact analysis
- **ASH (Security and Hazardous Materials Safety)**
  - Provides cyber threat info to various organizations

NCO Cyber Incident Response Team (NCIRT)

- The NCO establishes the NCIRT, as needed, for events/incidents with potential impact to the NAS
- Security/operations experts from the following organizations:
  - **NAS Cyber Operations (FAA NCO)**
  - **DOT/FAA Security Operations Center (FAA SOC)**
  - **FAA Security and Hazardous Material (FAA ASH)**
  - **FAA Telecommunications Infrastructure Security Operations Control Center (FTI SOCC)**
  - **FAA National Operation Control Center (NOCC)**
  - **NAS Authorizing Official Designated Representative (AODR) & National Operations Group (NOG) Manager**
  - **System Stakeholders**
  - FTI Primary Network Operations Control Center (PNOCC)
  - Network Enterprise Management Center (NEMC)
  - Enterprise Data Services (EDS)
  - FAA Enterprise Control Center (FAA ECC)
- NCIRT membership is dynamic and may change over the cyber security lifecycle based on the nature of the event and affected entities.