Federal Aviation Administration

National Airspace System (NAS) Cybersecurity Exercises

December 5, 2018

Presented by: Luci Holemans

NAS First

People Always

Agenda

Federal Aviation Administration

- Cyber Exercise Planning
- Cyber Exercise Conduct
- NAS Cyber Exercise Examples

NAS First
People Always

Federal Aviation Administration

Cyber Exercise Planning

NAS First
People Always

Cybersecurity Exercise Importance

Federal Aviation Administration

- Exercises improve cyber readiness by:
  1. Involving the community of aviation cybersecurity stakeholders.
  2. Providing a way to evaluate operations, processes, and capabilities.
  3. Reinforcing teamwork.
  4. Identifying both capability gaps and areas for improvement.
- Provide a mechanism to assess the preparedness of an agency's cyber response capability and its ability to withstand technology failures and cyber incidents.
- Can be used as an effective tool for identifying areas for improvement, without the operational consequences of an actual cybersecurity incident.
- Inform and enhance the agency's cybersecurity workforce, while supporting the expansion of strategic cybersecurity partnerships.

NAS First
People Always

Exercise Strategic Planning

Federal Aviation Administration

- An effective cyber exercise strategy ensures that resources are focused and outcomes drive improvements.
- Major Strategy Components:
  - Exercise Plan with Objectives
    - Define types of exercises to be conducted
  - Alignment with Agency/National Priorities & Goals
  - Resource Needs and Level of Effort
  - Organizational Engagement Plan
    - Internal
    - Whole of Agency
    - National
    - International

"Strategy without tactics is the slowest route to victory, tactics without strategy is the noise before defeat."
- Sun Tzu

NAS First
People Always

Exercise Plan

Federal Aviation Administration

- An annual comprehensive roadmap for targeting, coordinating, and conducting/participating in cybersecurity exercises.
- Defines major exercise objectives, such as:
  - Assess cyber preparedness
  - Test response processes/procedures
  - Support workforce development/training needs
  - Enhance communications and information sharing mechanisms
- Identifies key stakeholder integration requirements.
- Establishes the planned exercise schedule, to include:
  - Exercise Description
  - Major Objectives
  - Planned Dates
  - Level of Effort

NAS First
People Always

NAS Agency/National Alignment

Federal Aviation Administration

FAA Cybersecurity Strategy	NAS Cybersecurity Framework	Organizational Business Plan
Goal 2 - Objective 2.4: ▪ Improve cybersecurity risk detection through cybersecurity exercises. Goal 4 - Objective 4.2: ▪ Support cyber workforce training through exercises. Goal 5 - Objective 5.1: ▪ Expand participation in cyber exercises with external partners. Goal 5 - Objective 5.2: ▪ Improve collaboration with government, industry and private sector.	Protect Data Security (PR.DS): ▪ Metric: Conduct period Tabletop Exercise (TTX) testing of cybersecurity incident response and recovery plans for the NAS. Response Planning (RS.RP): ▪ Metric: Cybersecurity incident response SOPs are executed during and after events. Recovery Planning (RC.RP): ▪ Metric: After action reviews are conducted for TTX testing of cybersecurity incident recovery plans.	FY 19 Target 1: ▪ Participate in a partner developed incident response process exercise to validate FAA's incident response processes. **DHS Cybersecurity Strategy** ▪ Objective 5.3: Increase cooperation between incident responders to ensure efficient threat response and asset response efforts. **DOT Cybersecurity Strategy** ▪ Strategic Goal 4 (Accountability): Management Objective 2: Mission Efficiency and Support: Emergency Preparedness. **National Cyber Strategy** ▪ September 20, 2018, U.S. Government strategy to advance an open, interoperable, reliable, and secure cyberspace.

NAS First
People Always

Types of Cyber Exercises

Federal Aviation Administration

Type		Description	Example Goals & Objectives
Discussion Based	Tabletop Exercise (TTX)	Facilitated discussion that provides a forum for developing plans and procedures; typically focuses on strategic, policy-oriented issues that do not involve deployment of resources.	Goal: Enhance understanding of roles & responsibilities; develop new plans, policies, procedures, and agreements.
Operations Based	Functional Exercise (FE)	Involves players dispersed at multiple locations; conducted in simulated environment; focuses on action-oriented activities; used to validate plans, policies, procedures, clarify roles & responsibilities, identify resource gaps & improvement opportunities.	Goal: Validate & evaluate capabilities; focused on plans, policies, and procedures.
	Full Scale Exercise (FSE)	High stress multi-agency activities designed to test coordinated responses & rapid problem solving skills; most complex resource-intensive and possibly most expensive.	Goal: Coordinate between multiple agencies & organizations; demonstrate roles & responsibilities as addressed in plans and procedures.

NAS First
People Always

Exercise Level of Effort Estimate

Federal Aviation Administration

Type of Exercise	Overall Scope of Effort	Time to Plan (Months)	Length of Execution (Days)	Staff Baseline (# of People)	Complex Objectives & Larger Footprint
Tabletop (TTX)	Limited number of players & planners.	2.0 – 3.0	0.5 – 2.0	3.0 – 4.0	3 – 6 months 4 – 8 people
Functional Exercise (FE)	More players, time, real targets for scenarios.	5.0 – 8.0	2.0 – 4.0	5.0 – 8.0	8 – 20 months 8 – 12 people
Full Scale Exercise (FSE)	Multiple orgs and cross-agency planning teams, largest number of players, fully-tested IT environment, SMEs.	9.0 – 18.0	4.0 – 10.0	10.0 – 20.0	19 – 22 months 20 – 30 people

NAS First
People Always

Federal Aviation Administration

Cyber Exercise Conduct

NAS First
People Always

Key Exercise Roles

Federal Aviation Administration

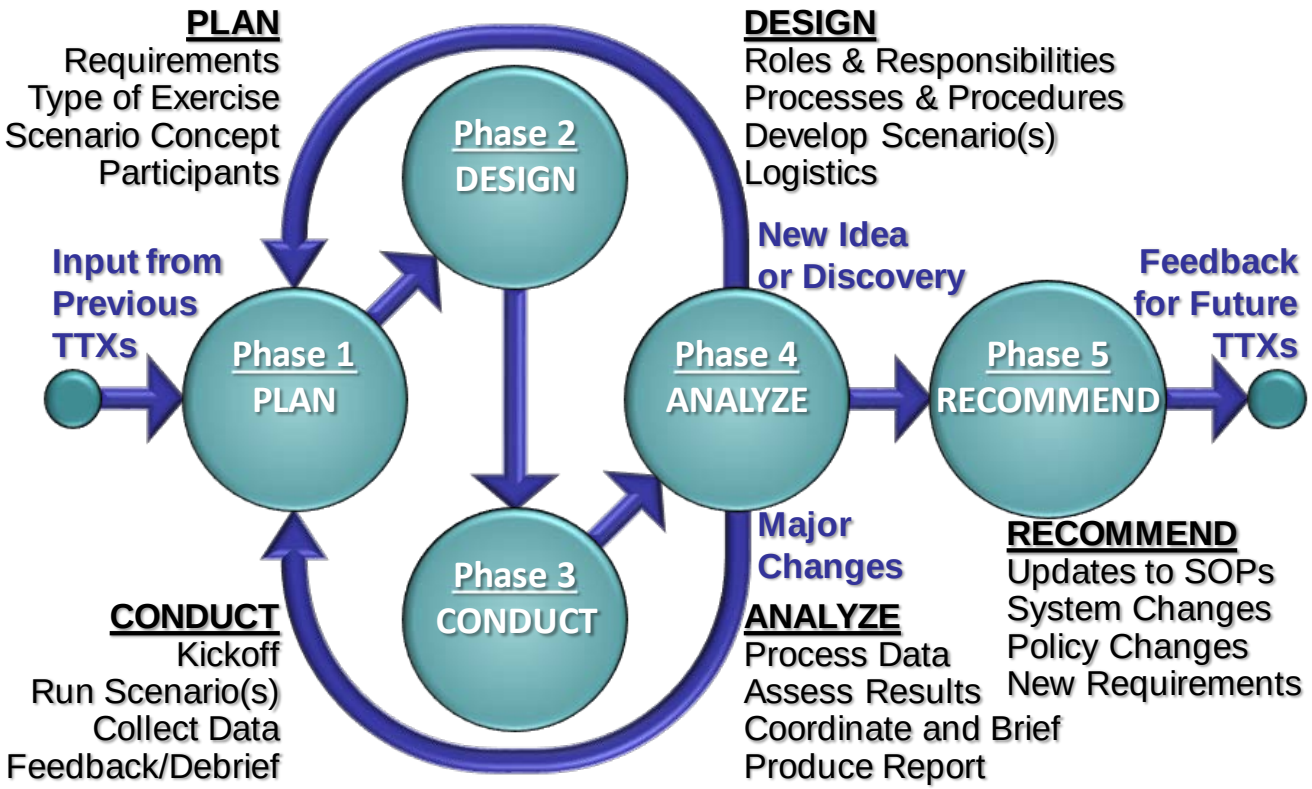
ROLE	RESPONSIBILITIES
Team Lead/ Deputy Team Lead	• Administration • Coordination • Program Management • Logistics (people, resources, schedule)
Scenario Planner	• Scenario Detailing • Infrastructure Design • Master Scenario Events List (MSEL) Development
Exercise Ops Planner	• Manning Roster • Conference Packets & Briefings • Ops & Facility Logistics
Assessments Planner	• Observation • Evaluation • Reporting Outcomes
Network/Tools Planner	• Building Network Infrastructure • Technical Integration • Subject Matter Expertise

NAS First
People Always

NAS Cyber Exercise Process

Federal Aviation Administration

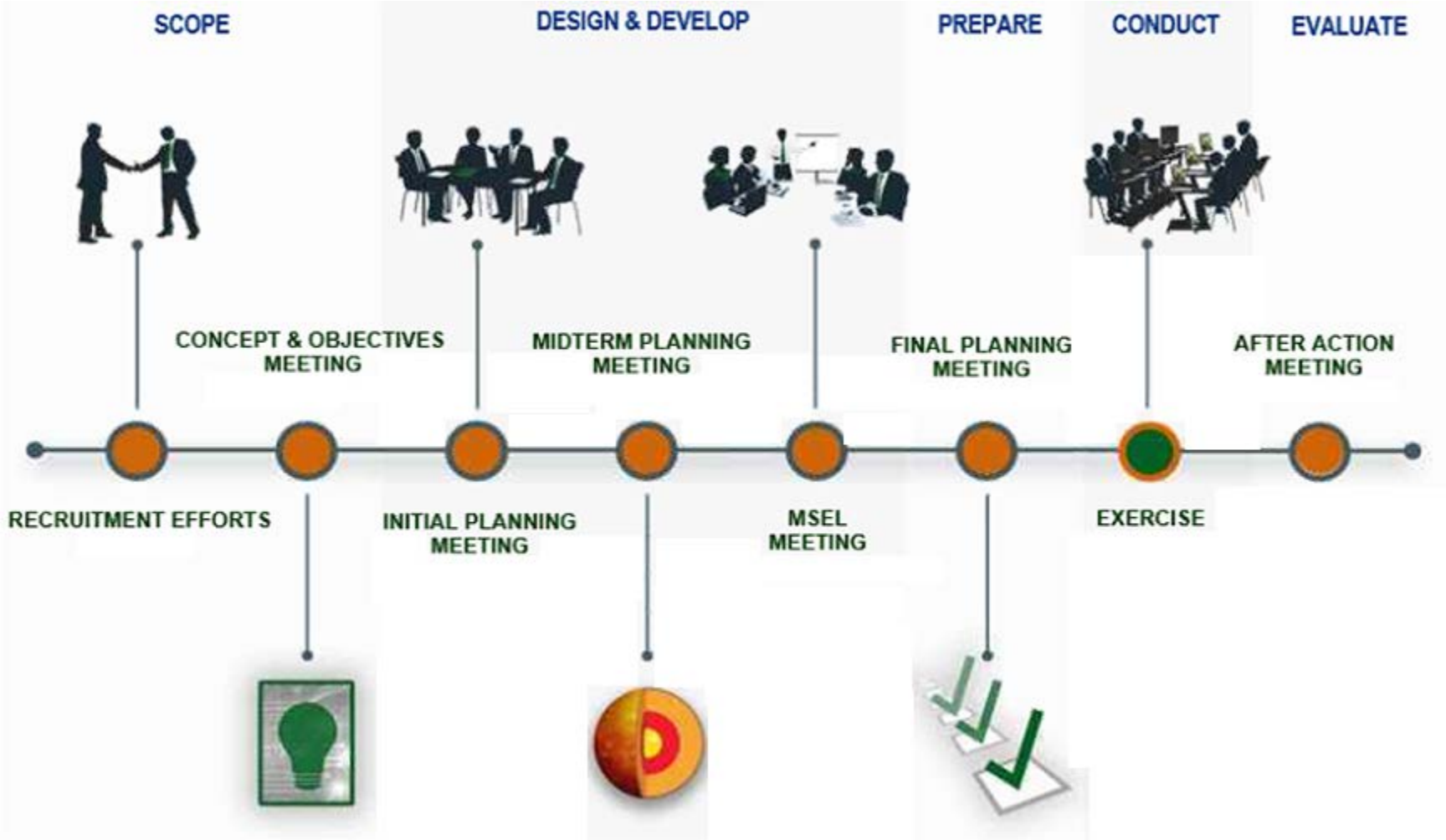
- NAS leverages the FEMA *Homeland Security Exercise and Evaluation Program* (HSEEP) approach to exercise program management.



NAS First
People Always

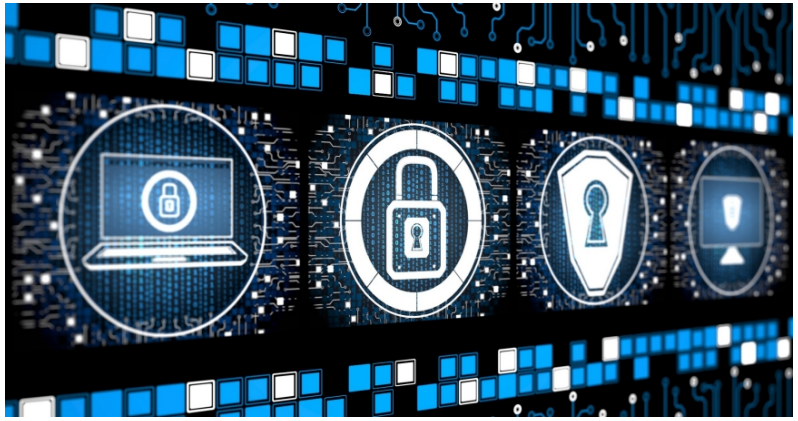
NAS Exercises Timeline

Federal Aviation Administration



NAS First
People Always

Federal Aviation Administration



NAS Cyber Exercise Examples

NAS First
People Always

Agency: FAA IRP

Federal Aviation Administration

Conducted: June 19 – 21, 2018

- Objectives
  - Examine cyber event decision making, coordination & communication within agency organizations while exercising the FAA Incident Response Plan (IRP);
  - Validate NAS Cyber Operations (NCO) incident response (IR) capabilities through the NAS Cyber Incident Response Team (NCIRT) process; and
  - Evaluate exercise player actions against the current FAA IRP and recommend updates to the plan.
- Lessons Learned Areas
  - Stakeholder Collaboration
  - Exercise Technology (ex: QoS / VM Environment capacity)
  - System Level Incident Response Plan
  - Business Impact
  - NAS-system level incident response capabilities and contingency plans.

NAS First
People Always

National: Cyber Storm VI

Conducted: April 10 – 13, 2018

Federal Aviation Administration

- Objectives
  - Examine coordination, communication flows, & information sharing within the FAA, with federal agencies (DHS, DOT), and coordinating entities (A-ISAC);
  - Validate NAS Cyber Operations (NCO) incident response (IR) capabilities through the NAS Cyber Incident Response Team (NCIRT) process; and
  - Assess agency reporting, escalation, and decision-making functions during a major cyber incident.
- Lessons Learned Areas
  - Information Sharing & Communication
  - Incident Response
  - Impact Assessment
  - Informing CS VI and Future Exercises
  - Department Level Education

NAS First
People Always

International: Caribbean1 TTX

Conducted: July 17 – 19, 2018

- Objectives
  - Develop and promote common understanding of cyber threats, vulnerabilities, and resultant risk across the Aviation Ecosystem
  - Identify gaps in state policies and operations
  - Identify and promote regional partnerships and mechanisms for information sharing on emerging threats and incident response
- Lessons Learned Areas
  - Policies should include considerations for cybersecurity
  - Stakeholders and responsibilities
  - ICAO guidance and mechanisms on cybersecurity
  - Communication resources and collaborative tools
  - Regional coordination websites
  - Existing information technology and cybersecurity frameworks

International: TSA/Israel TTX

Federal Aviation Administration

Planned: February 12-13, 2019

- Background/Overview
  - TSA hosting a Joint US/Israel Aviation cyber defense exercise in order to identify bilateral opportunities for increased cyber communication and coordination.
- Objectives
  - Familiarize participants with respective organizational structures, authorities, and capabilities associated with handling a significant cyber incident.
  - Understand respective policies and procedures, as well as roles and responsibilities, for responding to a significant cyber incident within respective countries.
  - Identify communication channels and potential gaps in information sharing.
  - Enhance general awareness of cyber threats, risks, and vulnerabilities within the aviation sector when responding to a transnational cyber incident(s).
- Participants will include
  - Department of Homeland Security (DHS)
  - Federal Aviation Administration (FAA)
  - Department of Transportation (DOT)
  - Transportation Security Administration (TSA)
  - MS-ISAC & A-ISAC
  - Israel National Cyber Directorate (INCD)
  - Israel Airport Authority (IAA)
  - Civil Aviation Authority (CAA)

NAS First
People Always