NextGen Net-centric Operations CyberSecurity Issues Net-Centric Working Group Meeting

October 1, 2009

Michael Little
Joint Planning and Development Office

NextGen Net-centric Operations Organizations

- JPDO Mission

  Ensure that the transformation of the US air transportation systems is realized by identifying, facilitating, and integrating the activities, commitments, and contributions of government partners, industry, and other key stakeholders to achieve the goals and benefits of the Next Generation Air Transportation System (NextGen)

- Role of JPDO NCOD
  - NCO = Applying Network methods and technologies to improve or transform an operation or process
  - Net-centric Infrastructure Services
    - Framework for sharing information among Organizations
  - Net-centric Information Exchange Services
    - Direct the information to the users who need it
- Role of NCWG
  - Provide Agency and Industry input into plans
  - Review and comment NCOD Products

JPDO NCOD CyberSecurity Issues

- Inter-organization Issues Require Collaboration
  - Federal Agencies comply with NIST 800-53
  - Agency CIO's responsible for ensuring compliance
  - Non-Government Organizations are less constrained
- Information Exchange Services
  - Establish access control restrictions on information
  - Define re-publication restrictions
  - Define common categories of access restrictions and roles
- Infrastructure Services – Basis for Mutual Trust
  - Certification and Authorization of Systems
  - ID Management for Personnel and Systems
  - Connectivity/Interoperability for Authorized Use
  - Ongoing monitoring and near-real time risk mitigation

CyberSecurity Is Critical to NextGen Success

- Significant Transformations require Inter-Organizational Trust
  - Ground Network Services
  - Air-Ground Network Services
  - ANSP Facilities and Infrastructure Services
  - Infrastructure Management Services/QoS
  - Mission Support Services
- All of which require Cybersecurity to be viewed in the broadest possible context
  - Operational Federal Agency Partners
  - Airports
  - Airlines
  - Passengers

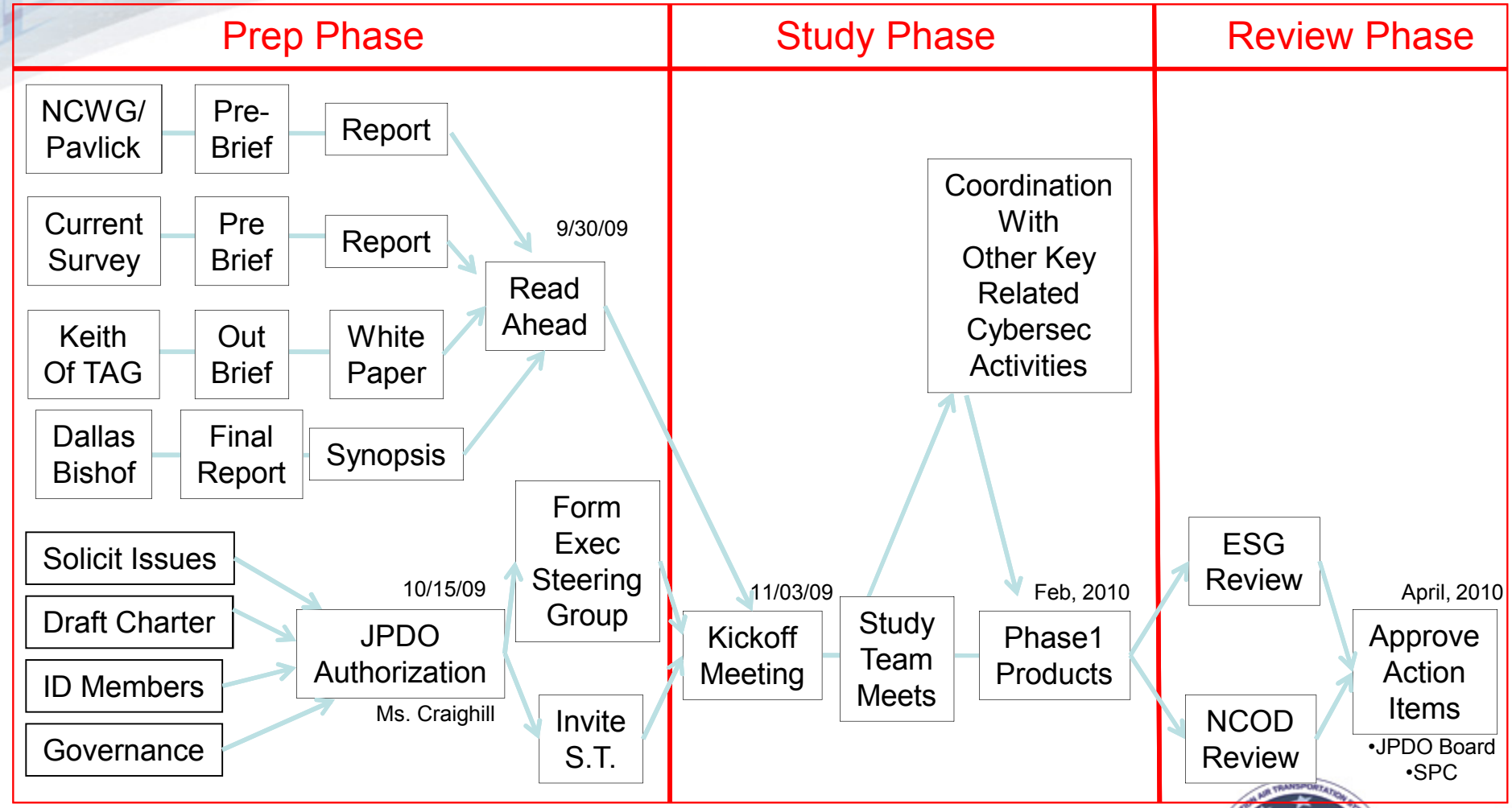
Key Features of Strategy

- Four Phase Approach
  - Preparation Phase: NCOD and contributors
  - Study Phase: Study Team
  - Review Phase:
    - Exec Steering Group and NCOD
    - SPC approval
  - Implementation Phase: Approved by SPC
    - Joint Actions using COI
    - Agency Actions added to JPE as approved SPC
- Follow JPDO and NCOD Governance Models
- Strategy must include participation from both Government and Industry
- Strategy must provide coordination with EU efforts
- Create an Executive Steering Group
  - With Cybersecurity Authority within Agencies (generally CIO offices)
  - Reports to SPC
- Study Team represents Subject Matter Experts on policy and practice
  - Include technical experts from industry, but avoid driving specific solutions

Notional Study Group Outputs

- Executive Steering Group to define deliverables
- Sample deliverables
  - Initial Policy and Governance Framework
    - e.g., Federated ID Management implementation
  - Initial Trust Model at Aviation Ecosystem Level
  - Identify key barriers for information sharing
  - First Draft of an experimentation plan for use with inter-organizational test bed

3-Phase Study Team



NCWG Topics

- Review and Comment the Overall Approach
- Have we captured all the issues for inter-organizational consideration?
- Who should be on the Study Group?
- Who else should Study Group talk to?
  - Health, finance, IRS?

Backup

Cybersecurity Strategy Issues

- What authority does DHS have over all this?
  - Should they be the chair of the Study Team and the ESG?
- Do JPDO Board Members have authority to deal with these issues?
  - Sometimes not in a position to speak for Agency on these matters (NASA and I think FAA)
- How do we appropriately include industry
  - Airlines, airports, (anyone else)
  - Who can speak for them? (trade associations?)

NextGen NCO CyberSecurity Actions

- Confidentiality
  - Inform users of requirements to protect Proprietary and SBU Data from compromise at destination
  - Authorized use among Organizations
- Integrity of Data
  - Service provider credentialing of information exchange
  - Standards for verification of data integrity and authenticity upon receipt
- Availability of Service
  - Adequately sized and protected from overload
  - Permit real-time discovery and unanticipated use