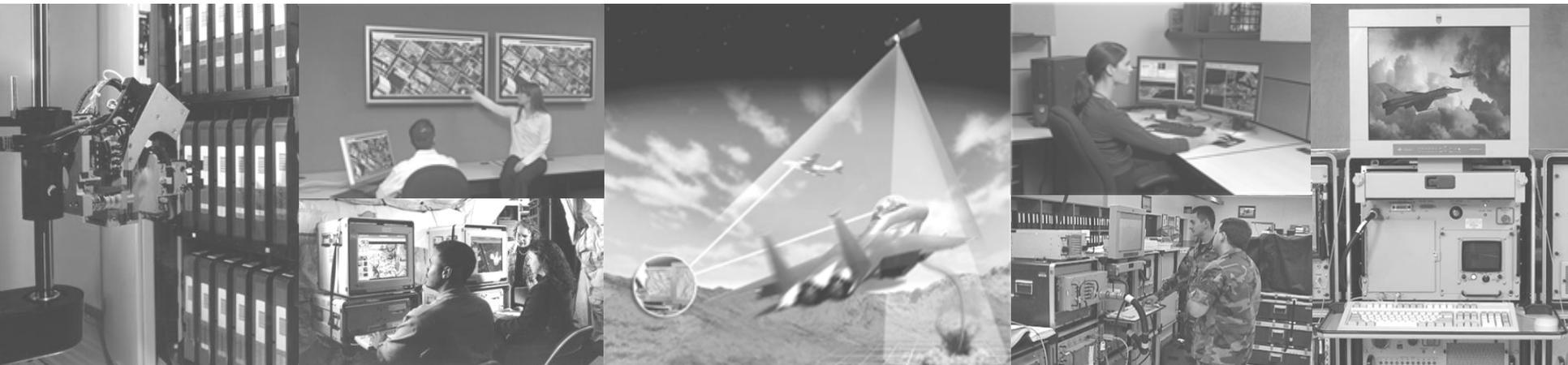


Looking Ahead To NextGen Aviation An Industry Perspective

John Osterholz
Vice President, Advanced Network Systems
BAE Systems, Inc

Approved for Release; No Export Controlled Information



BAE Systems – A Global Defense Company



BAE Systems plc

- 3rd Largest Defense Company
- 100,000 Employees
- \$80B Order Book
- \$30B Annual Sales
- Five Home Nations
- Presence in 130 Nations

BAE Systems Inc. (US)

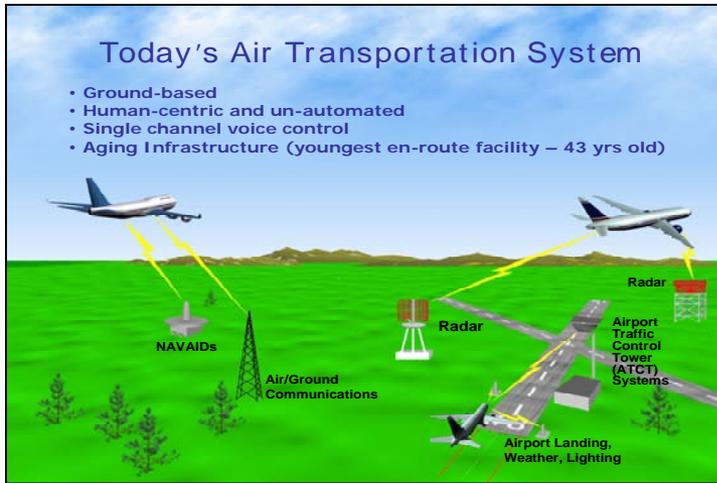
- 45,000 Employees (35,000 in the U.S.)
- \$16B Annual Sales (includes SSA work)
- 6th Largest U.S. Defense Company
- Major operations in over 30 states and in the UK, Sweden, Israel, Turkey and South Africa

***The U.S. accounts for nearly half of all employees,
40% of shareholders, and more than one third of revenues***

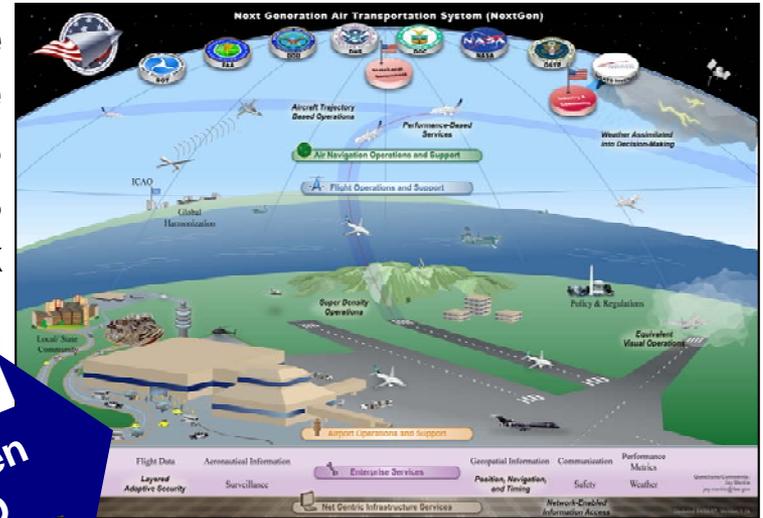
NextGen Aviation and Network Enabled Operation - The Promise Of Delivering Real Capability

Curb To Curb Scope
Net-Centric Architecture
Data And Application Access
Collaborative Flight Operations
IPv6 Enabled Network
FAA Led Interagency Collaboration

As Is



**NextGen
NEO**



Gate To Gate Scope
Point To Point Architecture
Push To Talk Voice
Controller Centric Flight Operations
Switched Circuit Network
Largely an FAA Program

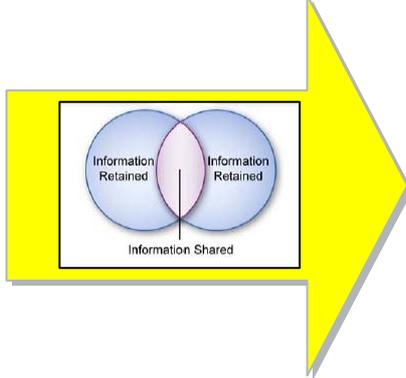
The NextGen Depends on Network Enabled Operations (NEO)

The Big NextGen Idea – Information Sharing Across Aviation Communities Of Interest

Objective - to achieve “collaborative decision making” through shared information. Accomplished through distributed information management.



From Many Ground Radars and Limited Capability A/C



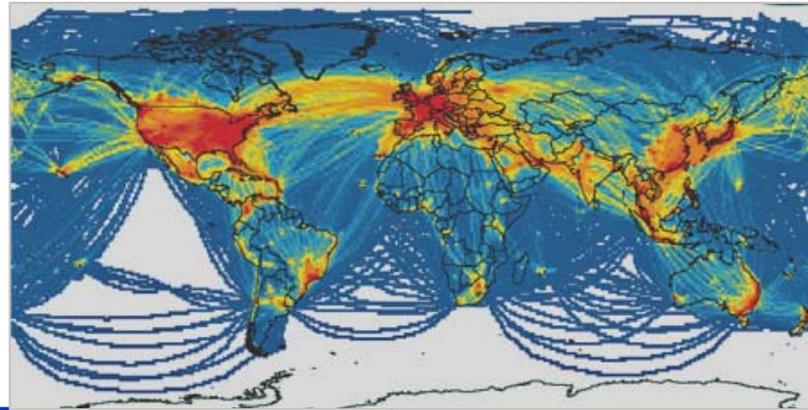
To Fewer Ground Radars and More Capable A/C



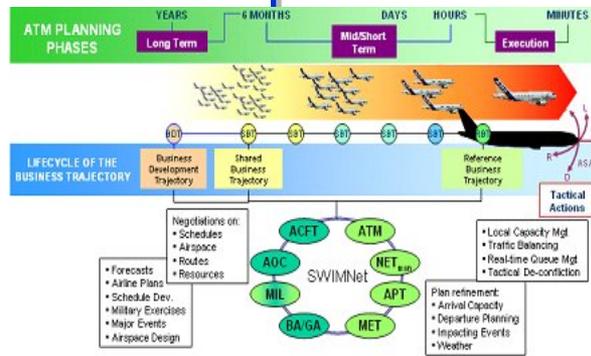
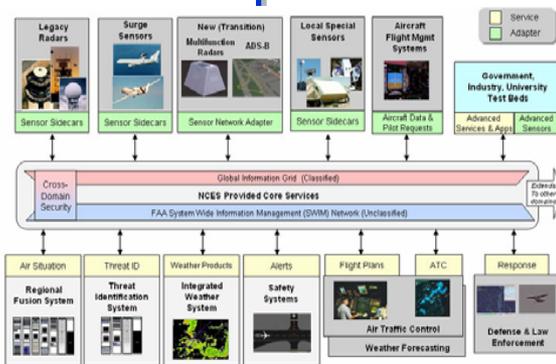
And ...

NextGen Aviation Has Become A Global Speculation

**Mission Critical
Information Intensive**



**Multiple Access Points
Security & Resilience**



Transition

Today	2010 Beyond
Ground Based Navigation	Satellite Based Navigation
Sensor-based Navigation	Performance-based Navigation
Voice Communication	DL/Voice Communication
Ground Radar Surveillance	Integrated ADS-B/MDS/Radar Surveillance
Separate ATM Automation Systems	Networking ATM Automation System
Flight Plan Management	Air Traffic Flow Management
ATM Internal Information Exchange System	Integrated Information Exchange for ATM, AOC and Airports etc.

**China
India**



NextGen/NEO

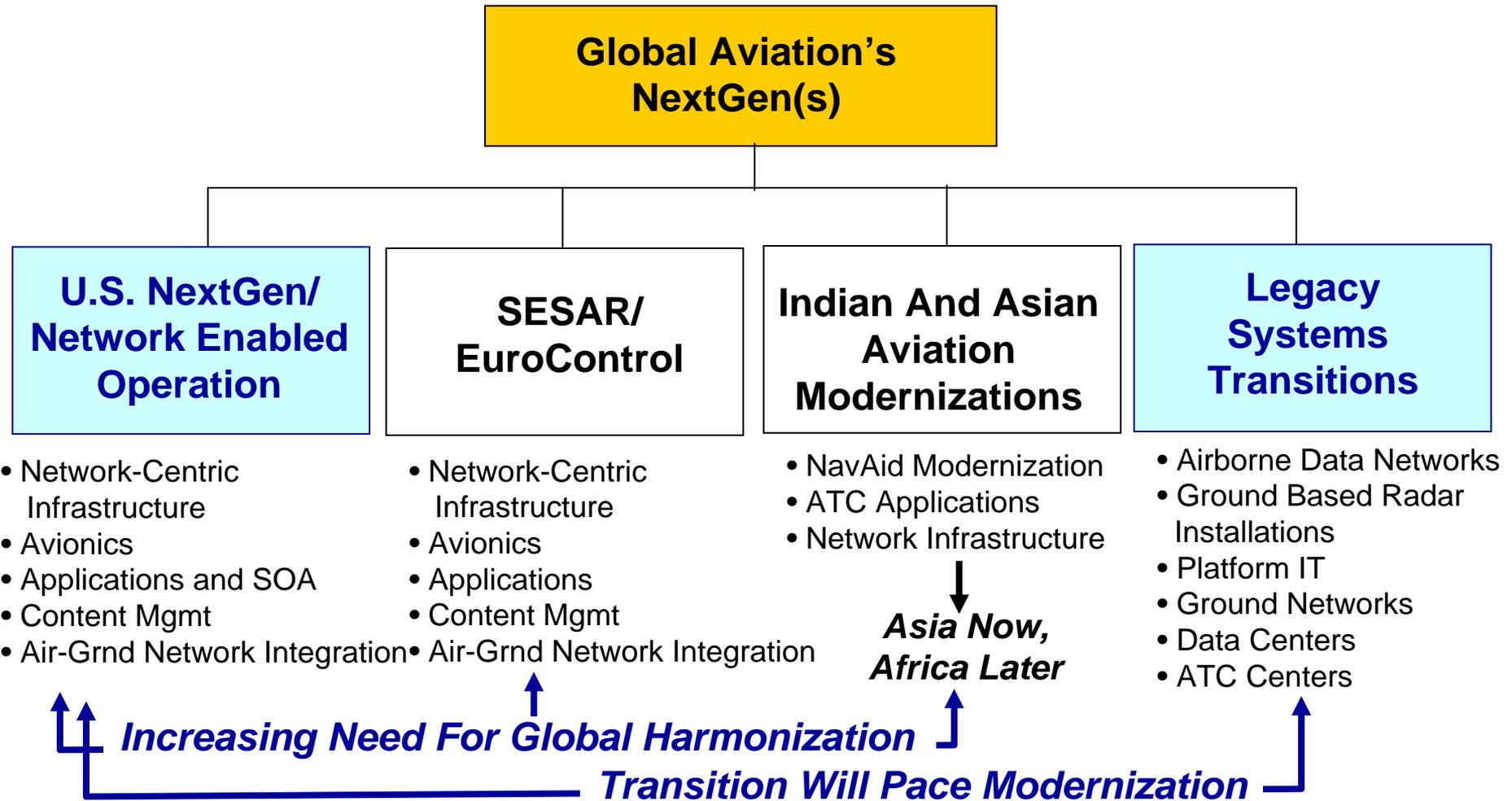
SESAR/Eurocontrol

The Global Nature of "Cyberspace" enabled Aviation necessitates an international approach to Interoperability & Security

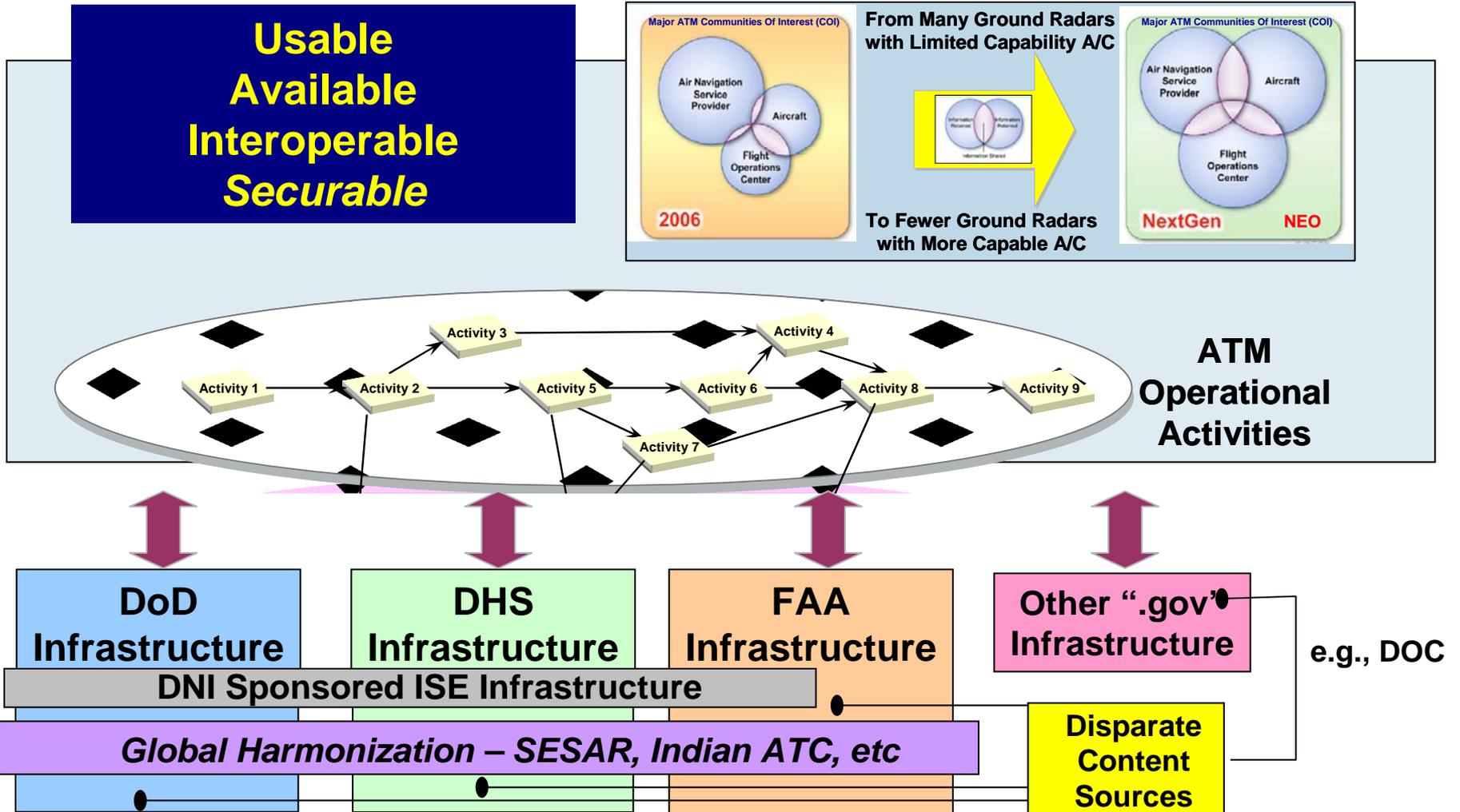
Implications For Advancing Aviation's NextGen Within A Networked World

- Validating and sequencing implementation and global harmonization of modernization programs – *Interoperable standards, patterns and processes*
- Enterprise service oriented architecture interoperability and assurance – *Run time responsive Services Oriented Architectures*
- Cybersecurity in a heterogeneous network enabled mission critical environment – *Achieving situational awareness and “Cyber Setback”*
- Integrating cooperative and non cooperative surveillance – *Operational management of trust*
- The challenge of UAS operations – *Autonomic meets autonomous*
- Federating air surveillance and maritime domain awareness – *Interoperability, security and governance at the data level*

Coordination of Next Generation Implementations Will Require New Forms Of Governance



NextGen Interoperability Needs Are Unprecedented



The Implications of Cybersecurity For NextGen Aviation Are Significant

- Conducting business in Cyberspace represents an irreversible component of modern business and society
- Military and civilian network exploitations by a variety of actors are increasing in scale and frequency
- National authorities and alliances are undertaking significant policy, programmatic and operational actions
- The security of Cyberspace has taken on international urgency as critical infrastructures continue to be successfully attacked



“Our information infrastructure — including the internet, **telecommunications networks, computer systems, and embedded processors and controllers in critical industries** — increasingly **is being targeted for exploitation and potentially for disruption or destruction**, by a growing array of state and non-state adversaries.”

SENATE SELECT COMMITTEE ON INTELLIGENCE
FEBRUARY 2008 –
DNI ANNUAL THREAT ASSESSMENT
Feb 5, 2008

Cybersecurity Is Now A Run Time Proposition

Enter The Network Centric Operations Industry Consortium

Meet The NCOIC –

NCOIC brings a global perspective to facilitate NCO adoption

NCOIC brings an industry neutral perspective to facilitate NCO adoption

FAA - NCOIC CRADA

NCOIC Response to FAA Cyber Security Strategy Draft

October 31, 2007

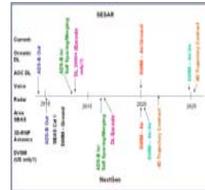
BAE Systems
The Boeing Company
Harris Corporation
HP
IBM
Lockheed Martin Company
Raytheon Company
Rockwell Collins
Thales

This document is a summary of comments from individual NCOIC member companies and represents the viewpoints of those member companies plus that of the review group in general. This document has not been voted upon by the Consortium membership and does not represent an official position of the NCOIC.

Cybersecurity Strategy Review

Aviation Deliverables in Review

- "Vision for A Netcentric Aviation Ecosystem" White Paper concluded formal review this week – Will come to EC for ratification
 - Benefits described for users in the areas of
 - Capacity
 - Safety
 - Efficiency
 - Security
 - Agility
 - Sustainability
 - Business Benefit Interdependencies
- "SESAR and NextGen Comparison" White Paper enters formal review this week
 - Summarizes, compares and contrasts Network Centric attributes for the two overarching Program concept documents that will enable the transformation of the European and United States Air Traffic Management Systems from today's legacy paradigm into a more robust, highly automated and integrated digital environment.
 - Emphasis placed on NextGen NetCentric Infrastructure Services and Shared Situational Awareness Services and SESAR NetCentric Infrastructure Services.



Aviation as an Ecosystem

NATO – NCOIC LOI

Cyber Defense An Industry Perspective

Industry Perspective on "Challenges In Providing Cooperative Cyber Defence Capabilities To NATO Forces"

- Operational Challenges**
 - Dynamic Situational Awareness
 - Degraded Operations
 - Cyber Defense Information Sharing
- Industry Perspective**
 - Key Areas Where Industry Is Innovating
 - The Value Of The NCOIC And Its Members
 - Speed And Delivery Of Value
- Concrete Steps**
 - Validating The Benefits Of NATO – Industry Collaboration
 - Building Trust – A Bilateral Framework For Progress
 - Potential Venues Leading To Early Success

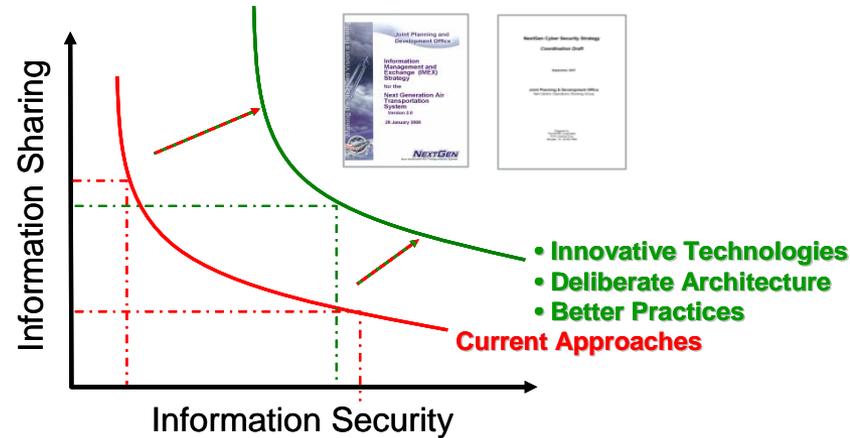
Cyber Defense Technology Assessment

Balancing Cooperative & Non Cooperative Surveillance - Operational Trust Management

Sustaining An Effective Balance Requires Information Sharing

- Cooperative Surveillance
- Non-cooperative Surveillance
- Surveillance and Intelligence

- Incentivize A Basis For Sharing
 - Respect supply AND demand
 - Provide clean access audits on line
 - Trusted broker – long term archive
- Facilitate Run Time Security
 - Eliminate unneeded functionality – e.g., thin client
 - Role based security combined with digital rights mgmt
 - Focus on insider threat – rebalance toward physical security
- Strategically Insert Diversity
 - Geographical and Functional Adaptability
 - Integrate a multiplicity of suppliers in enterprise solution
 - Control key architecture components even if commodity purchased



Operational Insight - Federating Air Surveillance & Maritime Awareness

Efforts undertaken in this plan will be designed to the maximum extent practical to be ***consistent with surveillance and intelligence sharing efforts already in effect or planned for the maritime and land domains***. Over time, the goal is an integrated domain awareness architecture.

Air Domain Surveillance and Intelligence Integration Plan
Department of Homeland Security 26 March 2007

Part of the (Canadian) Air Force's plan is that it "will explore new relationships with the Navy so ***aerospace control and maritime surveillance and control are executed jointly within Canada***

DND, Director General Air Force Development, *Strategic Vectors: The Air Force Transformation Vision*, 1 September 2004, p. 45.

We will not win the Global War on Terrorism if we cannot tell the bad guys from the good guys. We have to develop the capability to do that. ***A maritime NORAD is essential.***

Admiral Vern Clark, Chief of Naval Operations
Signal Magazine December 2004

The ***asymmetric domination of the littoral is indeed the greatest challenge to the globalized state that depends on the sea and air*** for its lanes of communication, transport, trade and movement of people.

W. Lawrence S. Prabhakar
Securing India's Littorals in the Twenty-first Century: Issues and Challenges August 2006

We've Surrounded The Problem And Are Admiring It ...

Surveillance Summit Wrap-Up

Way-Ahead for Air Domain
Awareness

RADM Kelly
Col. John Anderson
Mr. Tim Wallace

Interagency Air Maritime Surveillance Summit June 5-6, 2008

General Consensus

- We need to find a way to better enable/manage Air Domain Awareness
 - Air Surveillance Capabilities
 - Information Integration (net-centric)
 - Interagency Automation (common tools)
- We need to be compatible/integrated with Maritime efforts – and those of other domains

ADSII-103 Recommendations

- The Network-Centric/Enabled Operations air surveillance system must be a federated interagency system
 - Common automation system and common data distribution network
 - Multi-level security authentication
 - Role-based access
 - Enable a User Defined Operational Picture
 - Establish a fully coordinated information environment across all stakeholders to support their working effectively as a cohesive unit
- Establish a lead agency or department
 - Fund, resource and charter to enable operations based on cross agency net-centric best practices and requirements guidelines

21

Final Thoughts – “The only thing we have to fear is fear itself.”

