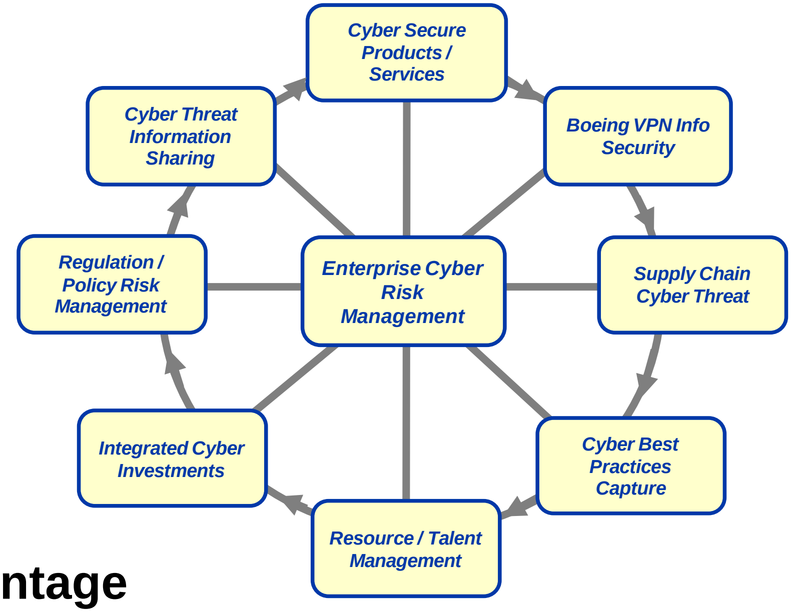
Cyber Risk Management

…..an Enterprise View

Greg Deiter

CYBERWEST – Phoenix AZ
14 May, 2014

A Robust View of the Cyber Threat


Cyber Secure Products / Services
Boeing VPN Info Security
Supply Chain Cyber Threat
Cyber Best Practices Capture
Resource / Talent Management
Integrated Cyber Investments
Regulation / Policy Risk Management
Cyber Threat Information Sharing
Enterprise Cyber Risk Management

Aligning the Enterprise to:

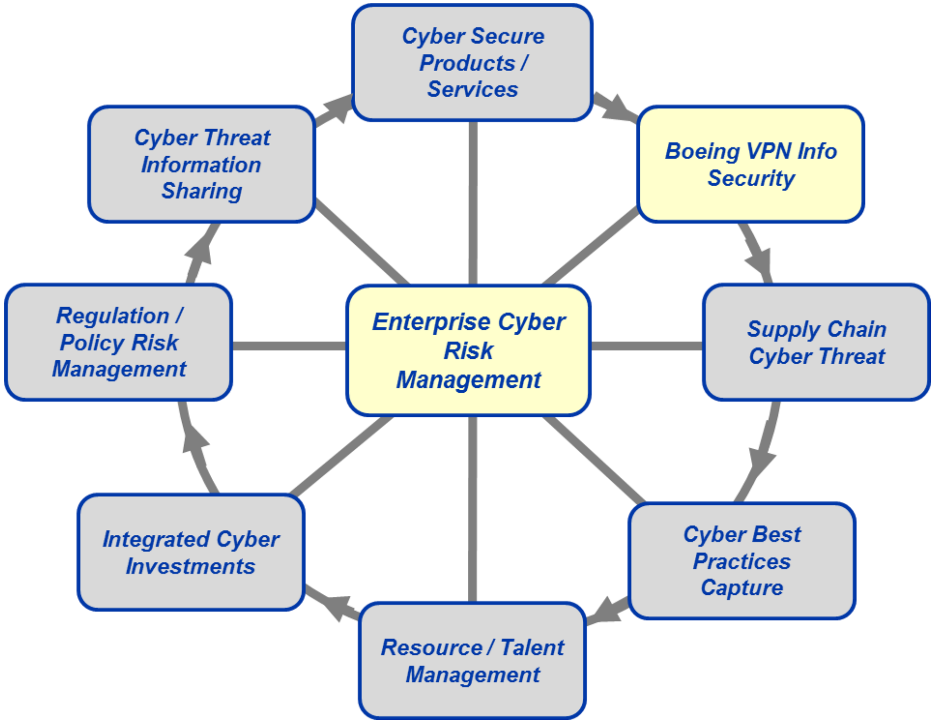
1. **Protect the company from emerging threats – our IP, Supply Chain, Production Systems, People Data**

2. **Cyber-secure our Products and Services to create a competitive advantage**

3. **Manage the regulatory environment and align industry partners**

4. **Balance Segregation/Sharing to improve One Boeing Collaboration**

Data / Info Protection Focus



Cyber Secure Products / Services

Boeing VPN Info Security

Supply Chain Cyber Threat

Cyber Best Practices Capture

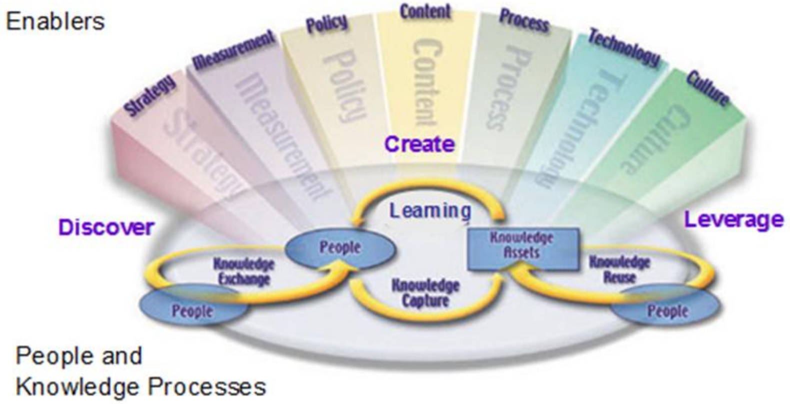
Resource / Talent Management

Integrated Cyber Investments

Regulation / Policy Risk Management

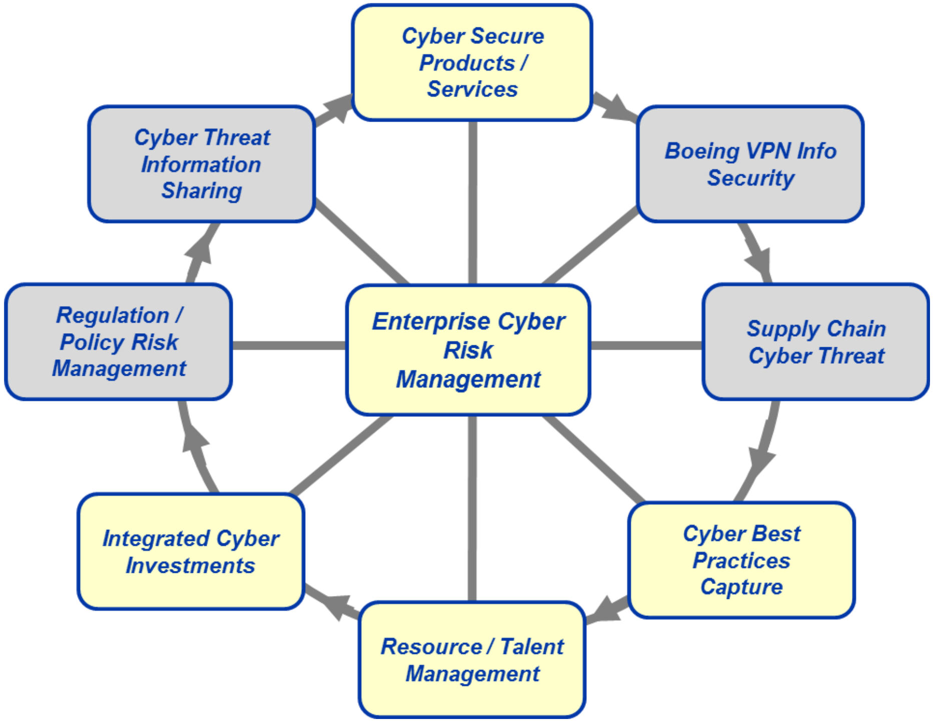
Cyber Threat Information Sharing

Enterprise Cyber Risk Management



- **Varied Challenges**
  - HUGE Target – Evolving Threats
  - Corporate Culture – ONE Boeing
  - User Transparency - dual edged sword
  - Effectiveness Measures / Metrics
- **Defense in Depth**
  - Continuously adding layers
  - Leverage Systems / People through Smart Automation
- **Government’s Role**
  - Threat Information Sharing
  - Spur Investment – People, Tools
- **Industry Partnerships**
  - DIB, ISACs
  - Industry Specific Forums – e.g., NDIA

Cyber Secure Products / Services



Cyber Secure Products / Services

Boeing VPN Info Security

Supply Chain Cyber Threat

Cyber Best Practices Capture

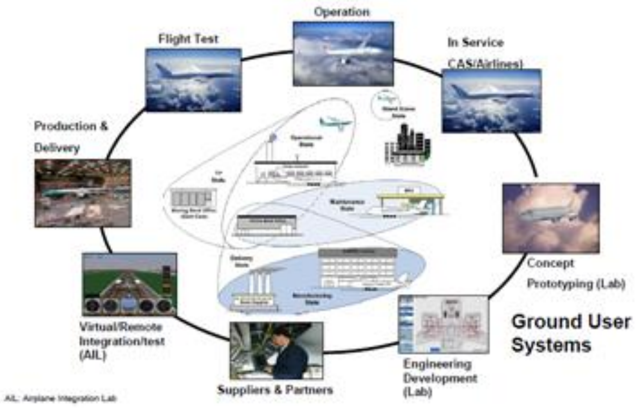
Resource / Talent Management

Integrated Cyber Investments

Regulation / Policy Risk Management

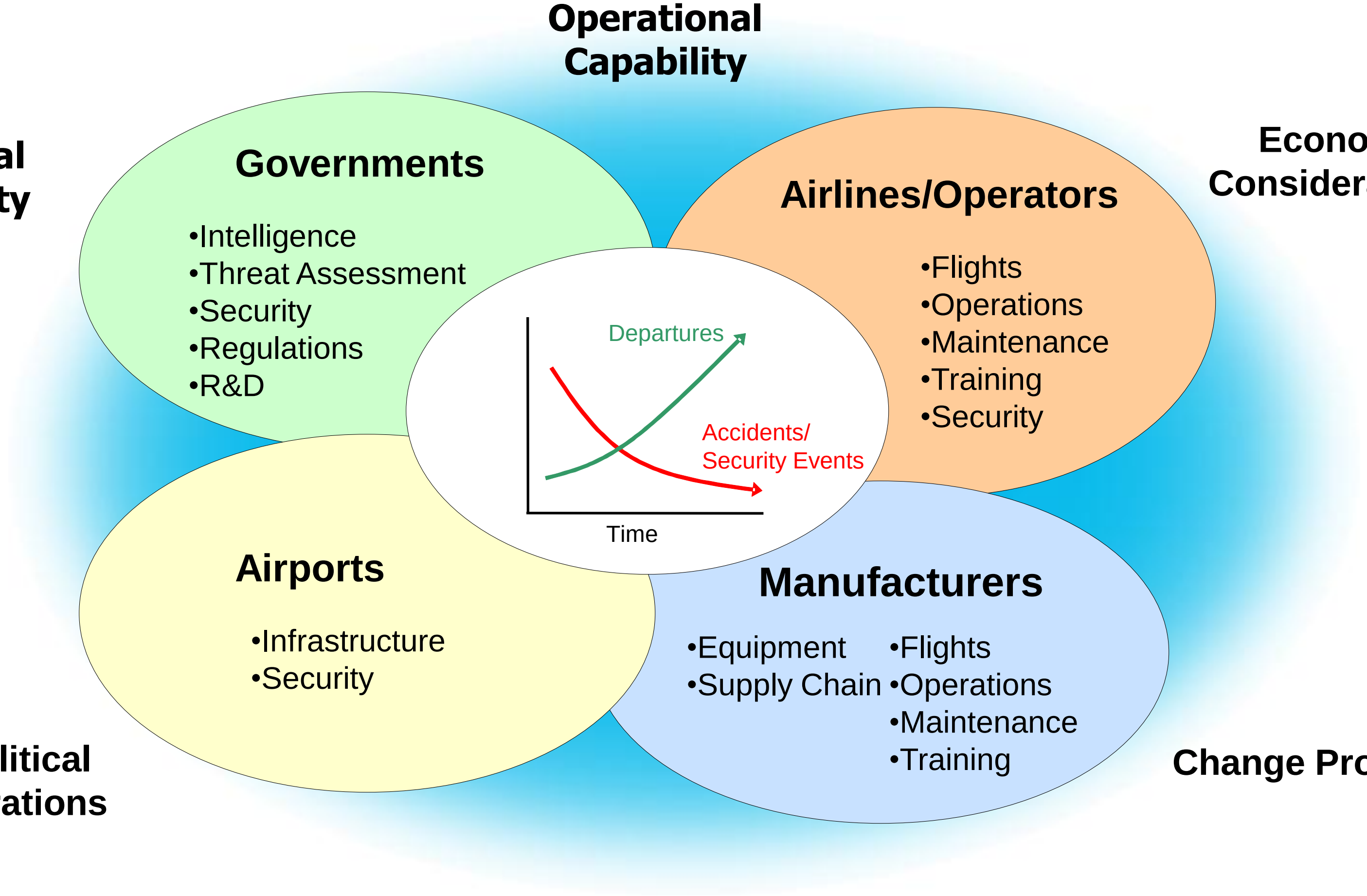
Cyber Threat Information Sharing

Enterprise Cyber Risk Management



- **E-Enabled Solutions**
  - Dreamliner Connectivity / Data Flows
  - Net-centric Defense, Space & Security
  - Info Based Service Offerings
- **Cyber Security Best Practices**
  - Protect the Core – Safety, Security
  - Secure the Ecosystem
  - Implement via Functional Excellence
- **Integrated Investments**
  - Enterprise AND Product Focus
  - Commercial and Defense synergy
  - Leveraging Partnerships
- **Cyber Talent Management**
  - Beyond IT Network Security
  - Leveraging / Sharing Talent

Safe, Secure & Efficient
Global Air Transportation System



Operational Capability

Technical Capability

Economic Considerations

Governments

- Intelligence
- Threat Assessment
- Security
- Regulations
- R&D

Airlines/Operators

- Flights
- Operations
- Maintenance
- Training
- Security

Airports

- Infrastructure
- Security

Manufacturers

- Equipment
- Supply Chain
- Flights
- Operations
- Maintenance
- Training

Geo-Political Considerations

Change Process

The biggest challenge in cyber securing any complex system is aligning the stakeholders and systems engineering the solution

The Aviation Landscape

e-Enabled Environment

Redacted –

deemed proprietary

Cyber Threats exist at ALL Layers of the Aviation Ecosystem

Commercial Aviation Cyber Security

External Drivers

- The speed at which threats continue to evolve
- Economics are driving increased connectivity in aviation
- Security must continue to improve in an increasingly complex and dynamic
- Success depends on many stakeholder

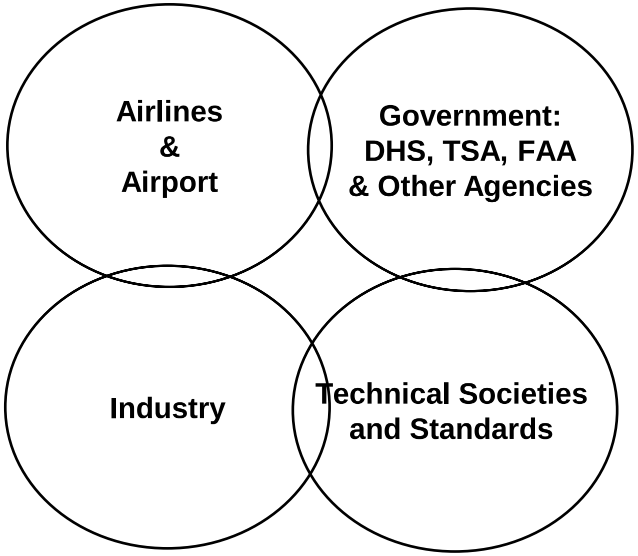
Key Challenges

- Pace of regulatory environment
- Pace of change process
- Broad spectrum of technology deployment throughout the fleet
- Silos within aviation domain
- Honeymoon period
- Engaging USG and industry senior leadership in risk management process and decision making

Targets

- A world confident in the strength, vigilance, efficiency, and resiliency of the aviation security system.
- A common roadmap for governments and industry working together to assure the security of the global air transportation system.

Today



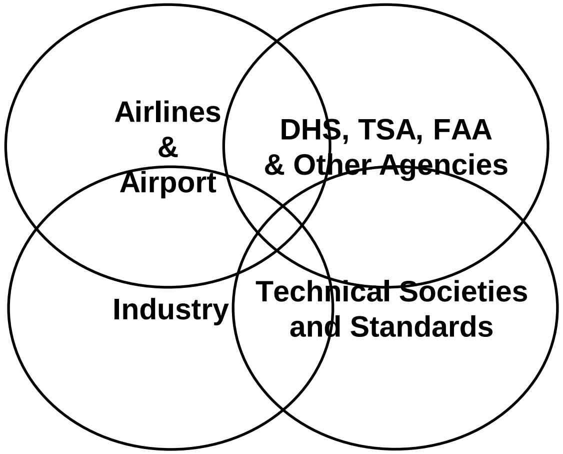
Airlines & Airport

Government: DHS, TSA, FAA & Other Agencies

Industry

Technical Societies and Standards

Future



Airlines & Airport

DHS, TSA, FAA & Other Agencies

Industry

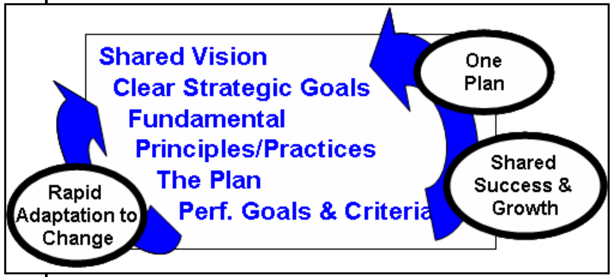
Technical Societies and Standards

Metrics & Indicators

- Common, defined strategies and plans
- No safety related cyber events
- No disruption of operations
- Implementable architecture, system and support structure
- Design, test & certification cycle time
- Solutions transcending aviation

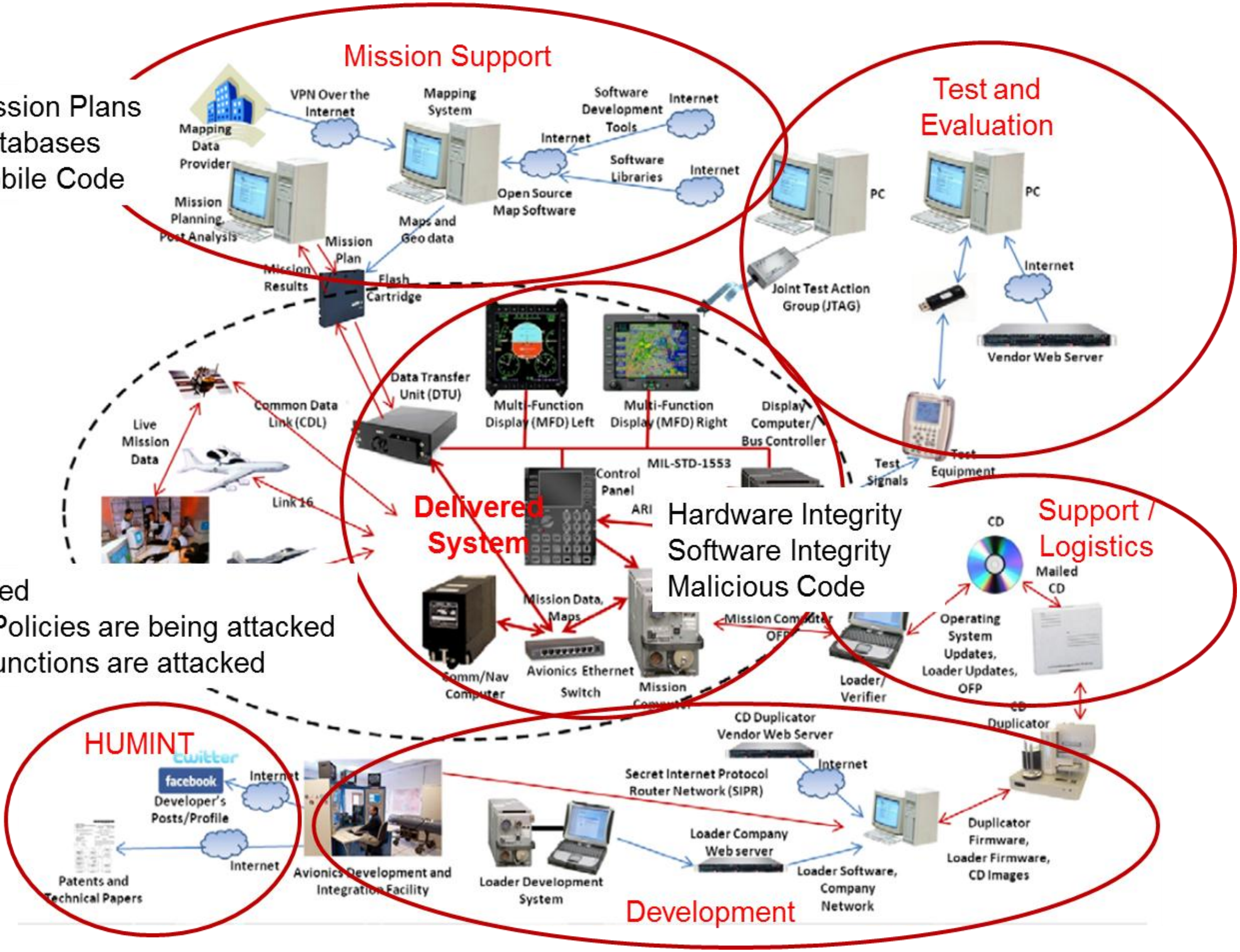
Aviation Core Competencies

- Disciplined
- Anti-fragile
- Capable, knowledgeable workforce



Shared Vision
Clear Strategic Goals
Fundamental Principles/Practices
The Plan
Perf. Goals & Criteria

Typical Defense / Space / Security Cyber Security Domains



Mission Plans
Databases
Mobile Code

Hardware Integrity
Software Integrity
Malicious Code

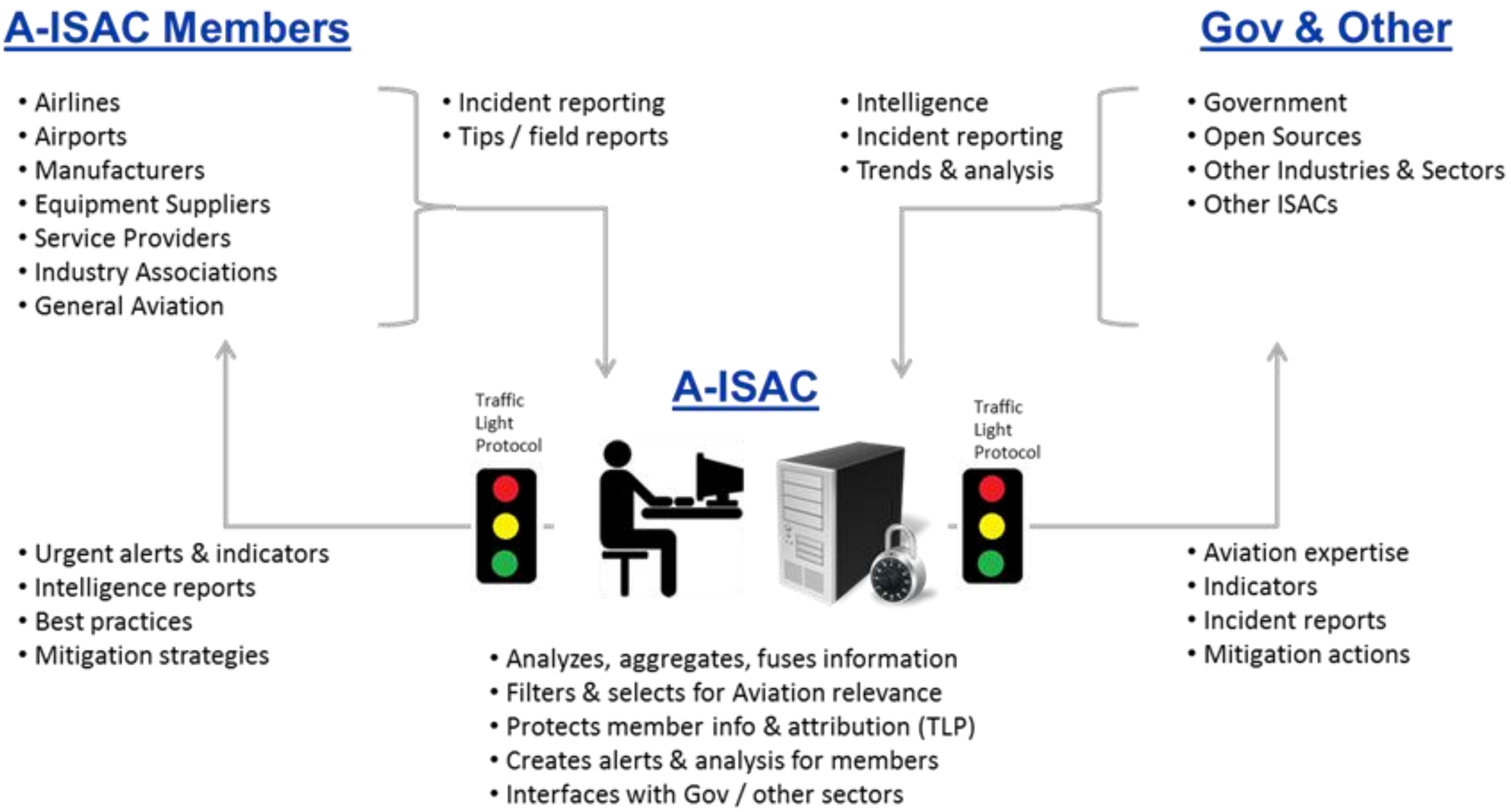
C2 attacked
Security Policies are being attacked
Critical Functions are attacked

R&D Focus / Cyber Investment Aligned

Redacted –

deemed proprietary

Leveraging the DHS ISAC Process



A-ISAC Members

- Airlines
- Airports
- Manufacturers
- Equipment Suppliers
- Service Providers
- Industry Associations
- General Aviation

- Incident reporting
- Tips / field reports

Gov & Other

- Government
- Open Sources
- Other Industries & Sectors
- Other ISACs

- Intelligence
- Incident reporting
- Trends & analysis

A-ISAC

- Urgent alerts & indicators
- Intelligence reports
- Best practices
- Mitigation strategies

- Analyzes, aggregates, fuses information
- Filters & selects for Aviation relevance
- Protects member info & attribution (TLP)
- Creates alerts & analysis for members
- Interfaces with Gov / other sectors

- Aviation expertise
- Indicators
- Incident reports
- Mitigation actions

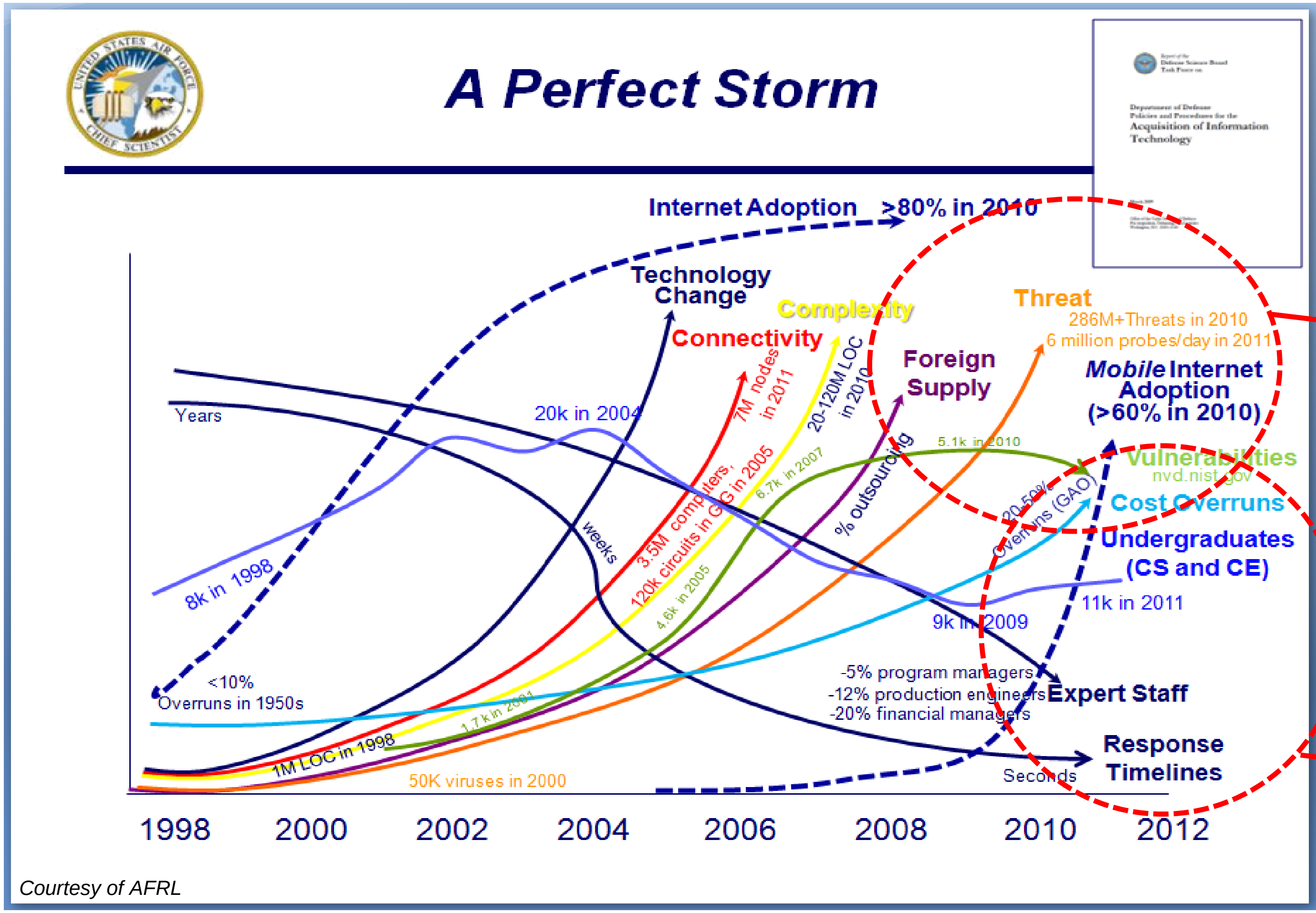
Utilize ISAC to Demonstrate an Industry who doesn't need Mandatory Controls

Aviation ISWG / ISAC Benefits

- **Shared Situational Awareness**
  - Trusted information sharing with aviation peers
  - Access to U.S. Government & CI partners
  - Access knowledgeable minds in cybersecurity
  - Knowledge, information, resources, analysis
- **Shared Learning & Risk Mitigation**
  - Threats, vulnerabilities, trends & technologies
  - Get help & details about a specific attack
  - Build mitigation strategies
  - Understand what the USG / others are doing
  - Protect and secure the business
  - Build resiliency

Shared Awareness Across Commercial Aviation

Cyber Talent Management – can we recover?



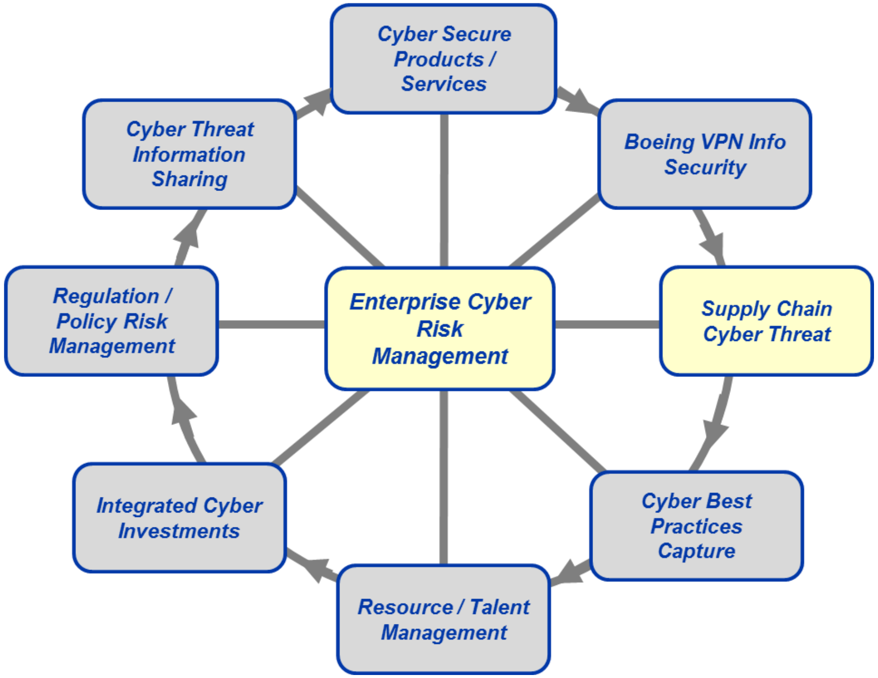
Courtesy of AFRL

Network Security & Product Security Demand Increasing

Existing Expertise demand nearing overload - symptoms appearing

Increasing Need for Enterprise Cyber Expertise – Industry and USG

Supply Chain Cyber Risk Management



Cyber Secure Products / Services

Boeing VPN Info Security

Supply Chain Cyber Threat

Cyber Best Practices Capture

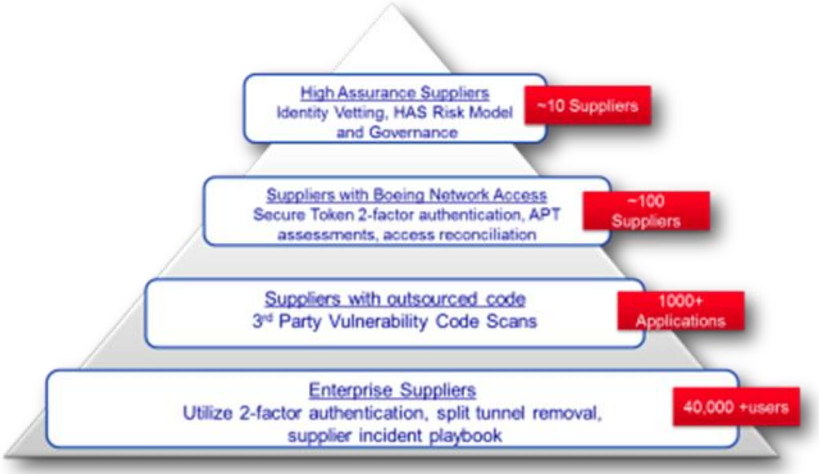
Resource / Talent Management

Integrated Cyber Investments

Regulation / Policy Risk Management

Cyber Threat Information Sharing

Enterprise Cyber Risk Management



High Assurance Suppliers
Identity Vetting, HAS Risk Model and Governance

~10 Suppliers

Suppliers with Boeing Network Access
Secure Token 2-factor authentication, APT assessments, access reconciliation

~100 Suppliers

Suppliers with outsourced code
3rd Party Vulnerability Code Scans

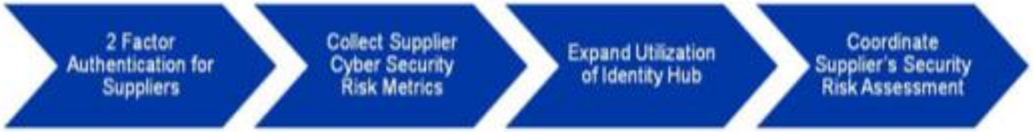
1000+ Applications

Enterprise Suppliers
Utilize 2-factor authentication, split tunnel removal, supplier incident playbook

40,000 +users

- **Identity Mgt. / Access Controls**
  - 2-factor authentication, secure portals
  - Dedicated /controlled links, one-time tokens
- **Contractual Requirements**
  - "Doing Business with Boeing" expectations
  - T&Cs, Quality Specs, Cyber Scorecards
- **Virtual Collaboration Standards**
- **SC Continuity / Risk / Resilience**
  - Enterprise CONOPS, Recovery Use Cases
- **Customer / Partner IP Protection**
  - DOD UTCI DFARs
  - High Assurance Enclaves, Net Segmentation
- **Regulatory Alignment**
  - Industry Working Groups, NIST Framework Alignment, SCRM Policy Discussions

Supply Chain – *Industry Collaboration /Partnerships*



2 Factor Authentication for Suppliers

Collect Supplier Cyber Security Risk Metrics

Expand Utilization of Identity Hub

Coordinate Supplier's Security Risk Assessment

Implemented 2-factor Authentication

- Actions Taken
  - Update
  - Upgrad
  - Increas
  - Standa
  - Streng
  - Implem
- Lesson
  - Execut
  - Multiple
  - Dedica
  - Focuse
  - Clear u

Expand Utilization of Exostar Identity Hub

- Actions Taken
  - Establis
  - Proces
- Lessons
  - Takes lo
  - Coordin

Supplier Security Assessment

- Actions Taken

a standardized process

y suppliers in the Boeing Supply Chain (VPN

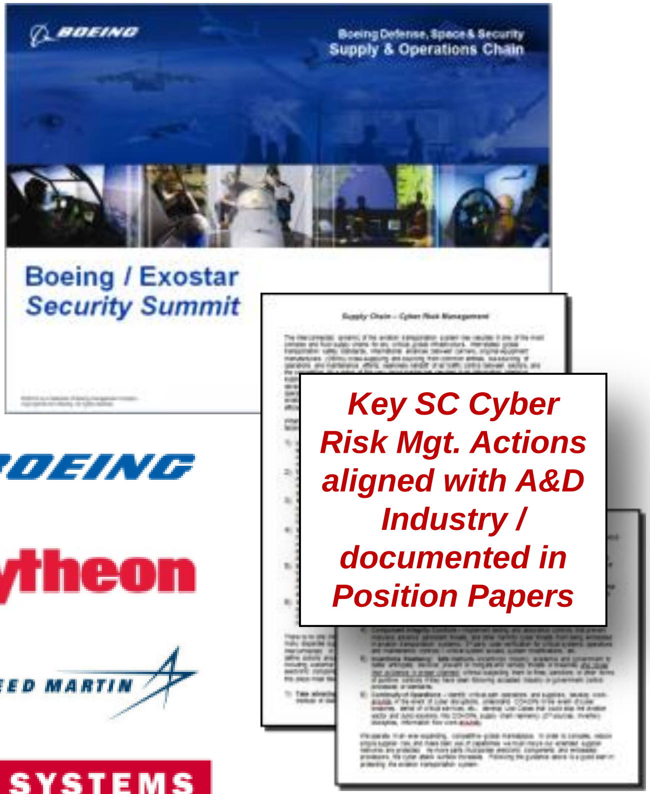
across Governing Investors / Industry

Governing Investors to develop consistent process that enable information sharing

chain is critical to mitigate risks and protect intellectual property

Unique Identifier	Function	Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
PR	Protec		
DE	Detec		
RS	Respond	AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Supply Chain Cyber Risk Management aligned with NIST Framework



Boeing Defense, Space & Security
Supply & Operations Chain

Boeing / Exostar *Security Summit*

Supply Chain – Cyber Risk Management

Key SC Cyber Risk Mgt. Actions aligned with A&D Industry / documented in Position Papers

BOEING

Raytheon

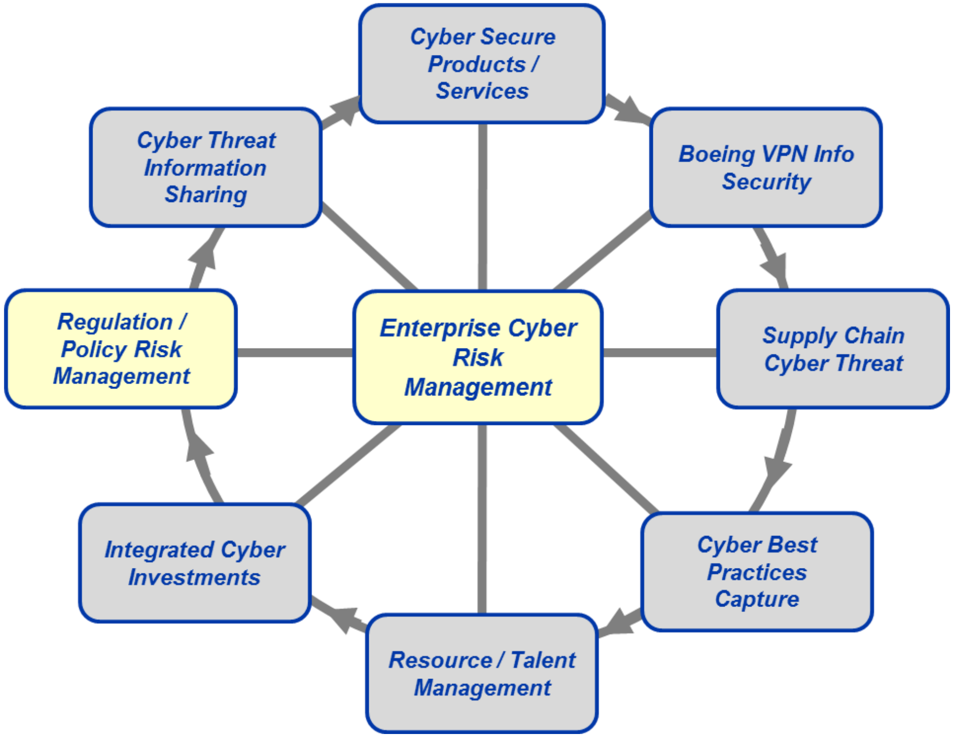
LOCKHEED MARTIN

BAE SYSTEMS

Rolls-Royce

Industry, USG Alliances to minimize impact to A&D Suppliers, Network

Cyber Policy / Regulations



Cyber Secure Products / Services

Boeing VPN Info Security

Supply Chain Cyber Threat

Cyber Best Practices Capture

Resource / Talent Management

Integrated Cyber Investments

Regulation / Policy Risk Management

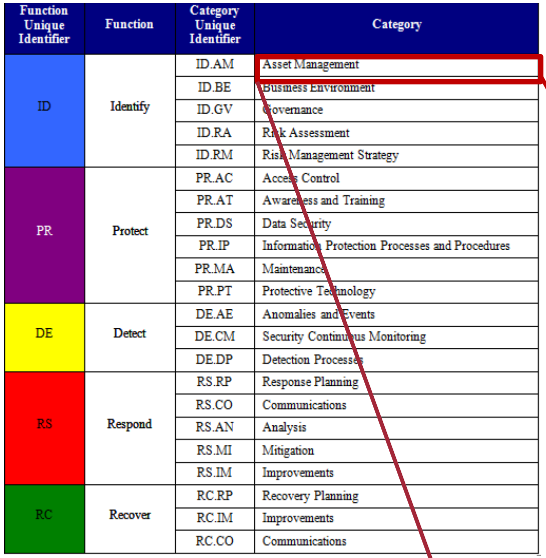
Cyber Threat Information Sharing

Enterprise Cyber Risk Management

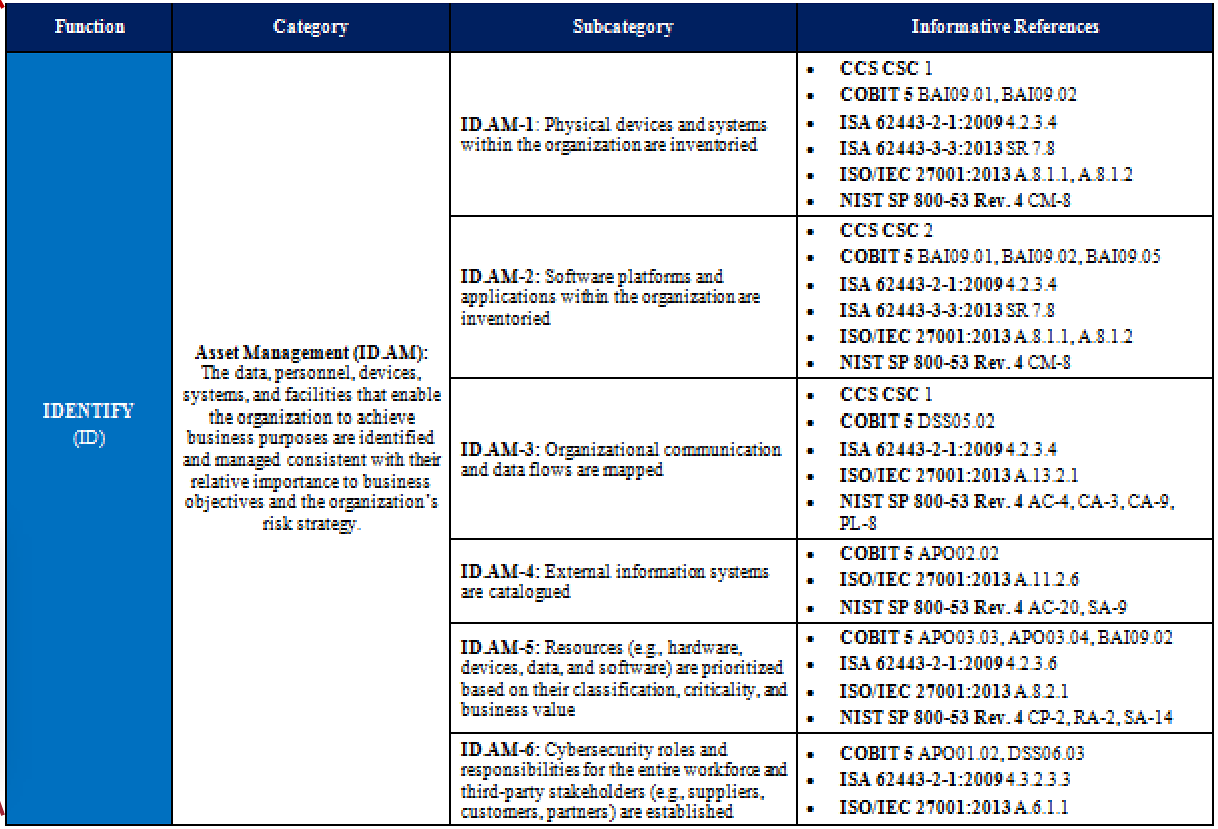
- **Can Policy / Regulation keep pace with Evolving Threats?**
  - Compliance-based approach will focus on last year's (or beyond) threat
  - Industry <u>and</u> USG needs flexibility
- **Government's Role**
  - Threat Information Sharing and Indemnification for those who do
  - Spur Investment – People, Tools
- **NIST Cyber Security Framework**
  - Great foundation – facilitates inter-operability
  - Industry motivated to adopt…incentives or support for some critical infrastructure (e.g., utilities)
- **Industry Partnerships**
  - DIB, ISACs
  - Industry Specific Forums – e.g., NDIA

Aligned with NIST Framework (CSF)

Executive Order 13636



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

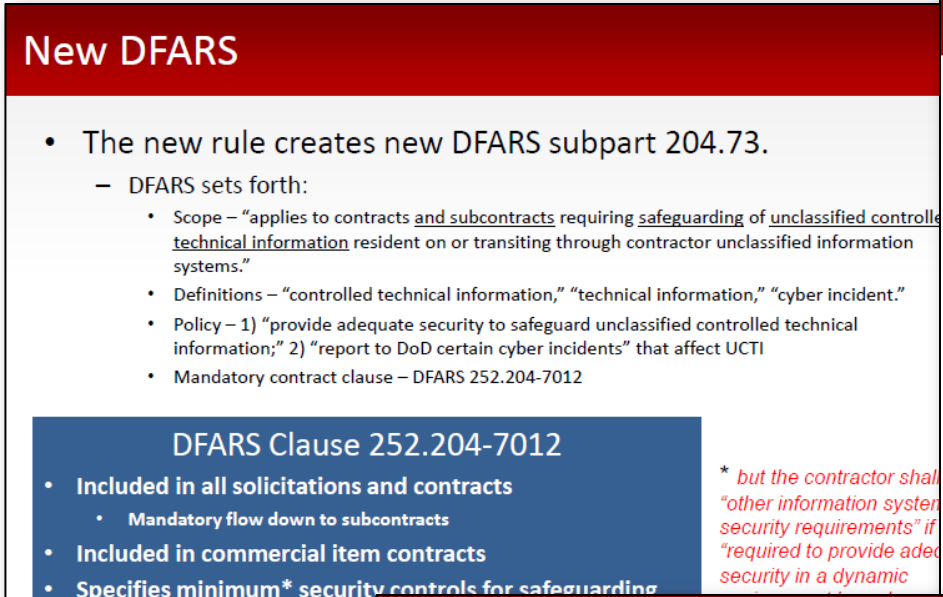


Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1

Documenting Meets or Exceeds Mapping of Internal Cyber Controls to NIST Framework

Framework essential tool in aligning Partners, Suppliers, Customers

DOD / GSA / Other Exec Branch Moving Out



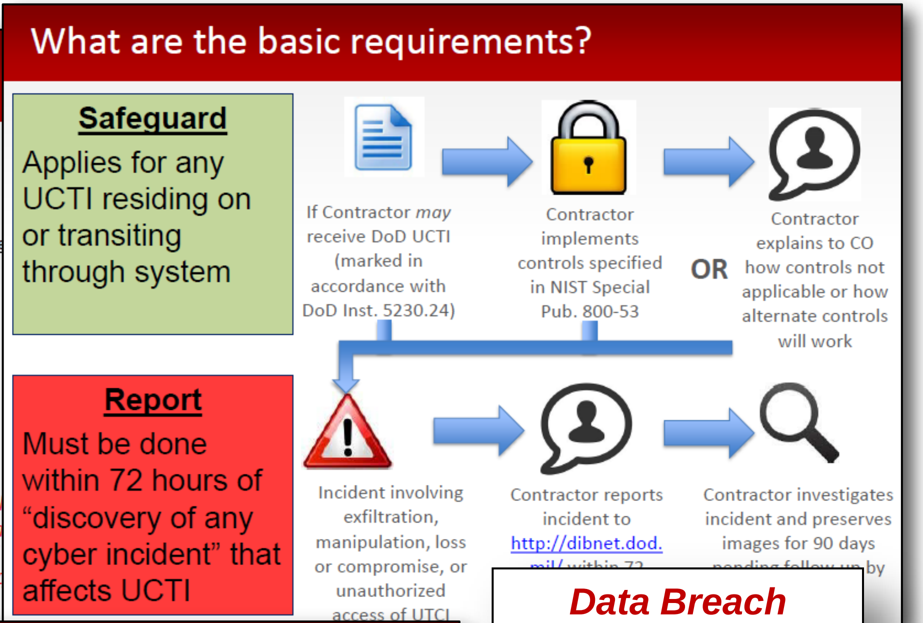
New DFARS

- The new rule creates new DFARS subpart 204.73.
  - DFARS sets forth:
    - Scope – "applies to contracts <u>and subcontracts</u> requiring <u>safeguarding</u> of <u>unclassified controlle</u> <u>technical information</u> resident on or transiting through contractor unclassified information systems."
    - Definitions – "controlled technical information," "technical information," "cyber incident."
    - Policy – 1) "provide adequate security to safeguard unclassified controlled technical information;" 2) "report to DoD certain cyber incidents" that affect UCTI
    - Mandatory contract clause – DFARS 252.204-7012

DFARS Clause 252.204-7012

- **Included in all solicitations and contracts**
  - **Mandatory flow down to subcontracts**
- **Included in commercial item contracts**
- **Specifies minimum* security controls for safeguarding**
- **Clarifies reporting requirem**

* *but the contractor shall "other information system security requirements" if "required to provide adeq security in a dynamic*



What are the basic requirements?

<u>Safeguard</u>

Applies for any UCTI residing on or transiting through system

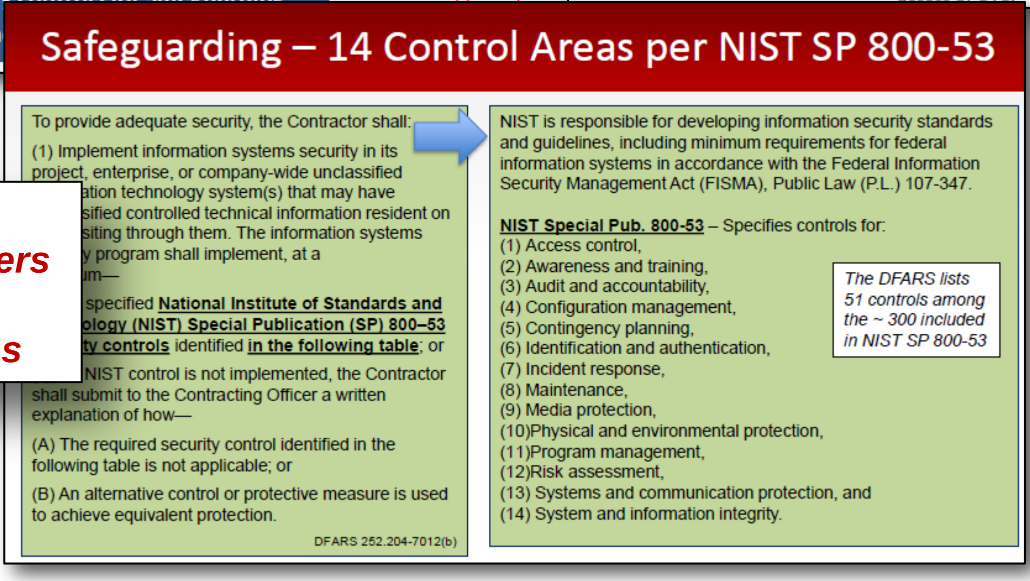
If Contractor *may* receive DoD UCTI (marked in accordance with DoD Inst. 5230.24)
Contractor implements controls specified in NIST Special Pub. 800-53
OR
Contractor explains to CO how controls not applicable or how alternate controls will work

<u>Report</u>

Must be done within 72 hours of "discovery of any cyber incident" that affects UCTI

Incident involving exfiltration, manipulation, loss or compromise, or unauthorized access of UTCI
Contractor reports incident to http://dibnet.dod.mil/ within 72
Contractor investigates incident and preserves images for 90 days pending follow up by

Data Breach Reporting should Focus on Future Prevention vs. Punishment



Safeguarding – 14 Control Areas per NIST SP 800-53

To provide adequate security, the Contractor shall:

(1) Implement information systems security in its project, enterprise, or company-wide unclassified ation technology system(s) that may have sified controlled technical information resident on siting through them. The information systems y program shall implement, at a um—

specified **<u>National Institute of Standards and</u>** **<u>ology (NIST) Special Publication (SP) 800–53</u>** **<u>ty controls</u>** identified **<u>in the following table</u>**; or

NIST control is not implemented, the Contractor shall submit to the Contracting Officer a written explanation of how—

(A) The required security control identified in the following table is not applicable; or

(B) An alternative control or protective measure is used to achieve equivalent protection.

DFARS 252.204-7012(b)

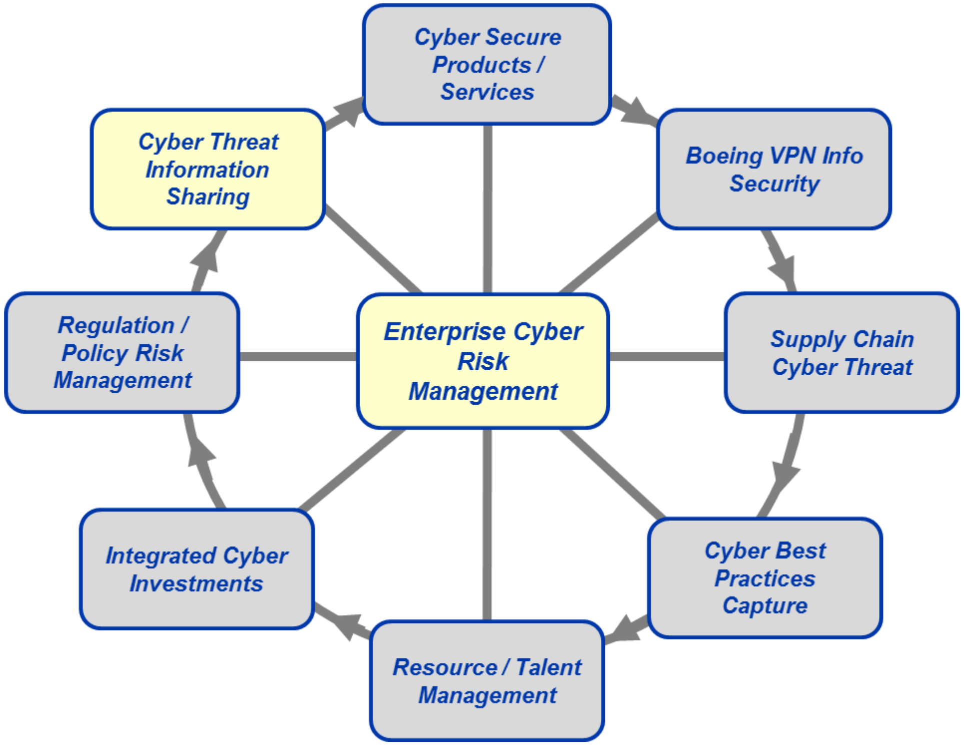
NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems in accordance with the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347.

<u>NIST Special Pub. 800-53</u> – Specifies controls for:
(1) Access control,
(2) Awareness and training,
(3) Audit and accountability,
(4) Configuration management,
(5) Contingency planning,
(6) Identification and authentication,
(7) Incident response,
(8) Maintenance,
(9) Media protection,
(10)Physical and environmental protection,
(11)Program management,
(12)Risk assessment,
(13) Systems and communication protection, and
(14) System and information integrity.

The DFARS lists 51 controls among the ~ 300 included in NIST SP 800-53

Working with Specific Customers on Program Protection plans

Cyber Threat Info Sharing

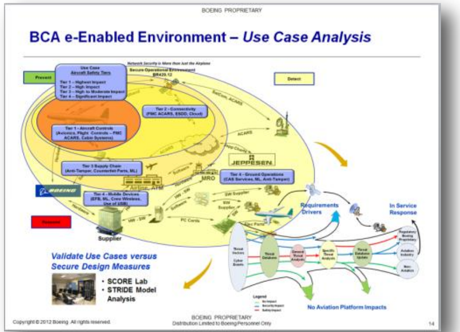


Cyber Secure Products / Services
Boeing VPN Info Security
Supply Chain Cyber Threat
Cyber Best Practices Capture
Resource / Talent Management
Integrated Cyber Investments
Regulation / Policy Risk Management
Cyber Threat Information Sharing
Enterprise Cyber Risk Management

- **Within and Across Industries**
  - Industry Forums – e.g., NDIA
  - A&D Partnerships – e.g., Exostar
  - Academia, think Tank Engagement
- **Between USG and Industry**
  - DIB and ESF Forums
  - DHS ISACs and Cross-ISAC WGs
  - FACE Working Groups
- **Within our Enterprise**
  - Weekly, Monthly Forums
  - Dedicated Focals with clear RAA
- **With Policy Makers**
  - Position Papers, Hill and Agency Visits
  - Industry Forum Working Groups

Aligning and Advancing the Enterprise

bi-directional collaboration, resources sharing



BOEING PROPRIETARY

BCA e-Enabled Environment – *Use Case Analysis*

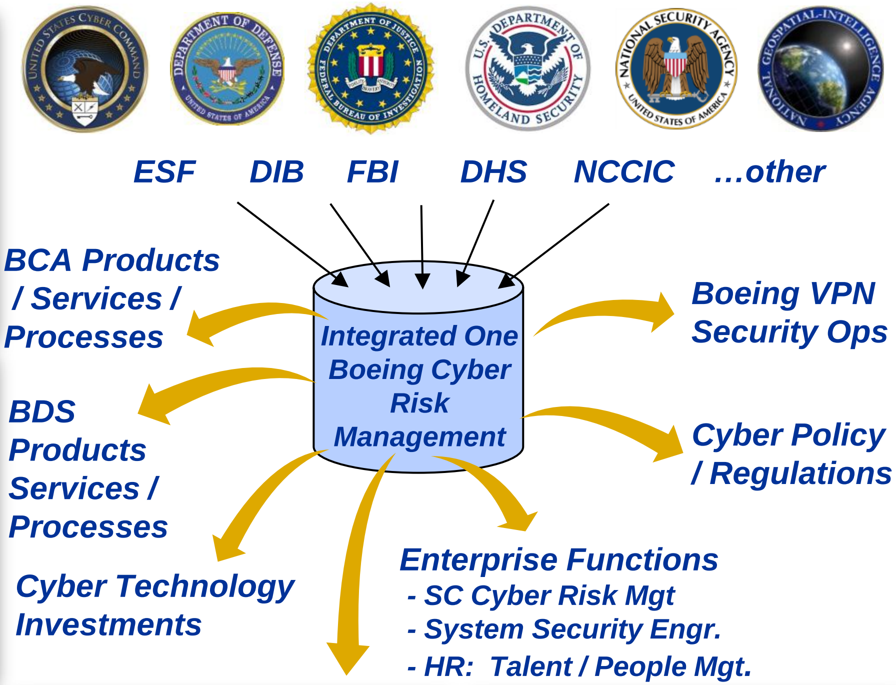
Network Security is More than Just the Airplane
Secure Operational Environment
BR429.12
Use Case
Aircraft Safety Tiers
Tier 1 – Highest Impact
Tier 2 – High Impact
Tier 3 – High to Moderate Impact
Tier 4 – Significant Impact
Prevent
Detect
Respond
Tier 2 - Connectivity (FMC ACARS, ESDD, Cloud)
Tier 1 - Aircraft Controls (Avionics, Flight Controls – FMC ACARS, Cabin Systems)
Tier 3 Supply Chain (Anti-Tamper, Counterfeit Parts, ML)
Tier 4 - Ground Operations (CAS Services, ML, Anti-Tamper)
Tier 4 - Mobile Devices (EFB, ML, Crew Wireless, Use of USB)
SatCom, ACARS
ACARS
JEPPESEN
MRO
Airline, ATM
Supplier
HW - SW
PC Cards
SW Supplier
Requirements Drivers
In Service Response
Legend
No Aviation Platform Impacts

Validate Use Cases versus Secure Design Measures

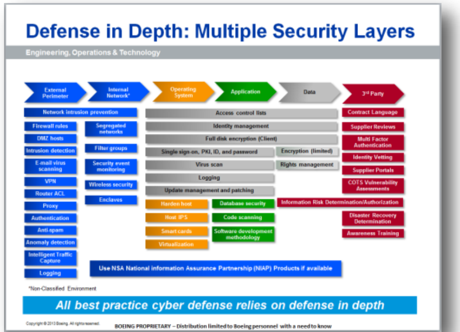
- SCORE Lab
- STRIDE Model Analysis

BOEING PROPRIETARY
Distribution Limited to Boeing Personnel Only

14



ESF
DIB
FBI
DHS
NCCIC
…other
Integrated One Boeing Cyber Risk Management
BCA Products / Services / Processes
BDS Products Services / Processes
Cyber Technology Investments
Enterprise Functions
- SC Cyber Risk Mgt
- System Security Engr.
- HR: Talent / People Mgt.
Boeing VPN Security Ops
Cyber Policy / Regulations



Defense in Depth: Multiple Security Layers

Engineering, Operations & Technology

External Perimeter → Internal Network* → Operating System → Application → Data → 3rd Party

External Perimeter / Internal Network:
- Network intrusion prevention
- Firewall rules
- DMZ hosts
- Intrusion detection
- E-mail virus scanning
- VPN
- Router ACL
- Proxy
- Authentication
- Anti-spam
- Anomaly detection
- Intelligent Traffic Capture
- Logging
- Segregated networks
- Filter groups
- Security event monitoring
- Wireless security
- Enclaves

Operating System / Application / Data:
- Access control lists
- Identity management
- Full disk encryption (Client)
- Single sign-on, PKI, ID, and password
- Encryption (limited)
- Virus scan
- Rights management
- Logging
- Update management and patching
- Harden host
- Host IPS
- Smart cards
- Virtualization
- Database security
- Code scanning
- Software development methodology

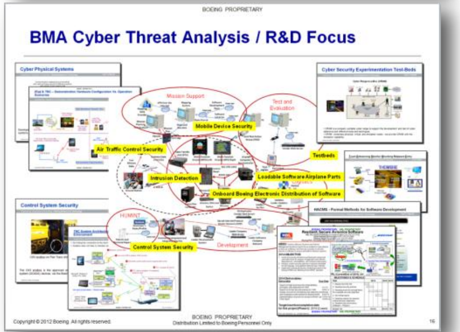
3rd Party:
- Contract Language
- Supplier Reviews
- Multi Factor Authentication
- Identity Vetting
- Supplier Portals
- COTS Vulnerability Assessments
- Information Risk Determination/Authorization
- Disaster Recovery Determination
- Awareness Training

Use NSA National information Assurance Partnership (NIAP) Products if available

*Non-Classified Environment

All best practice cyber defense relies on defense in depth

BOEING PROPRIETARY – Distribution limited to Boeing personnel with a need to know



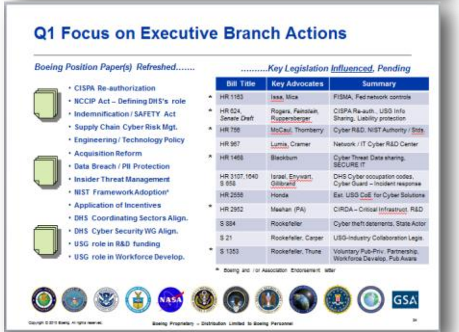
BOEING PROPRIETARY

BMA Cyber Threat Analysis / R&D Focus

Cyber Physical Systems
Cyber Security Experimentation Test-Beds
Mission Support
Test and Evaluation
Mobile Device Security
Air Traffic Control Security
Testbeds
Intrusion Detection
Loadable Software Airplane Parts
Onboard Boeing Electronic Distribution of Software
THEMBIE
Control System Security
HUMINT
Development
HACMS - Formal Methods for Software Development
Resilient, Secure Avionics Software

BOEING PROPRIETARY
Distribution Limited to Boeing Personnel Only

16



Q1 Focus on Executive Branch Actions

Boeing Position Paper(s) Refreshed.......

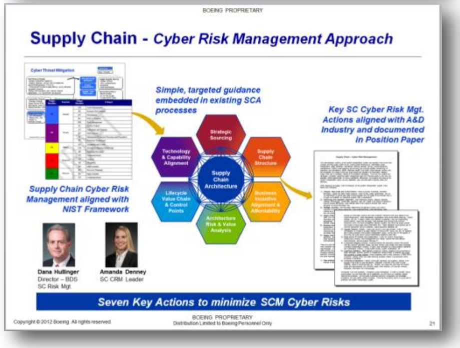
- CISPA Re-authorization
- NCCIP Act – Defining DHS's role
- Indemnification / SAFETY Act
- Supply Chain Cyber Risk Mgt.
- Engineering / Technology Policy
- Acquisition Reform
- Data Breach / PII Protection
- Insider Threat Management
- NIST Framework Adoption*
- Application of Incentives
- DHS Coordinating Sectors Align.
- DHS Cyber Security WG Align.
- USG role in R&D funding
- USG role in Workforce Develop.

..........Key Legislation Influenced, Pending

	Bill Title	Key Advocates	Summary
*	HR 1163	Issa, Mica	FISMA, Fed network controls
*	HR 624, *Senate Draft*	Rogers, Feinstein, Ruppersberger	CISPA Re-auth., USG Info Sharing, Liability protection
*	HR 756	McCaul, Thornberry	Cyber R&D, NIST Authority / Stds
	HR 967	Lumis, Cramer	Network / IT Cyber R&D Center
*	HR 1468	Blackburn	Cyber Threat Data sharing, SECURE IT
	HR 3107, 1640 S 658	Israel, Enyvart, Gillibrand	DHS Cyber occupation codes, Cyber Guard – Incident response
	HR 2556	Honda	Est. USG CoE for Cyber Solutions
*	HR 2952	Meehan (PA)	CIRDA – Critical Infrastruct. R&D
	S 884	Rockefeller	Cyber theft deterrents, State Actor
	S 21	Rockefeller, Carper	USG-Industry Collaboration Legis.
*	S 1353	Rockefeller, Thune	Voluntary Pub-Priv. Partnership, Workforce Develop, Pub Aware

* Boeing and / or Association Endorsement letter

Boeing Proprietary – Distribution Limited to Boeing Personnel



BOEING PROPRIETARY

Supply Chain - *Cyber Risk Management Approach*

Cyber Threat Mitigation
Strategic Sourcing
Supply Chain Structure
Business Incentive Alignment & Affordability
Architecture Risk & Value Analysis
Lifecycle Value Chain & Control Points
Technology & Capability Alignment
Supply Chain Architecture
Supply Chain – Cyber Risk Management

Simple, targeted guidance embedded in existing SCA processes

Key SC Cyber Risk Mgt. Actions aligned with A&D Industry and documented in Position Paper

Supply Chain Cyber Risk Management aligned with NIST Framework

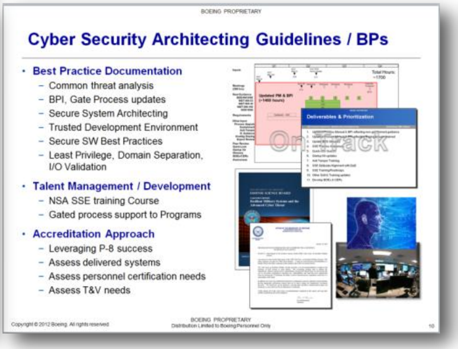
Dana Hullinger
Director – BDS
SC Risk Mgt

Amanda Denney
SC CRM Leader

Seven Key Actions to minimize SCM Cyber Risks

BOEING PROPRIETARY
Distribution Limited to Boeing Personnel Only

21



BOEING PROPRIETARY

Cyber Security Architecting Guidelines / BPs

- **Best Practice Documentation**
  - Common threat analysis
  - BPI, Gate Process updates
  - Secure System Architecting
  - Trusted Development Environment
  - Secure SW Best Practices
  - Least Privilege, Domain Separation, I/O Validation
- **Talent Management / Development**
  - NSA SSE training Course
  - Gated process support to Programs
- **Accreditation Approach**
  - Leveraging P-8 success
  - Assess delivered systems
  - Assess personnel certification needs
  - Assess T&V needs

BOEING PROPRIETARY
Distribution Limited to Boeing Personnel Only

10

BOEING PROPRIETARY

Enterprise Leadership – *positive, sustainable momentum*

Rich Massey
BMA TF
Cyber Chief Engr

Mike Garrett
Director - BCA
Aviation Security

Jimmy Farricker
Senior Chief Engr
Networks & Comms

John Toomer
Director – WDC Ops
National Security, DOD, Intelligence

Jim Shaw
Domain Leader
Networked Syst.

Scott Wickett
Director - IT
Cyber Controls & Threat Mgt

Nancy Anderson
BMA Chief Engr
Avionics, Digital Ecosystem Dev

John Craig
Manager - BCA
Program Engrg
Cyber BDE

Bonnie Triezenberg
STF – Secure SW Dev

Fred Schwien
Director – WDC Ops
DHS, TSA, FAA

Bala Chidambaram
Manager – BR&T
Cyber Security & Network Technology

Mark Ackerman
Manager - IT
Cyber Threat Mgt

Leslie Unruh
ATF – Security Systems Engineering – ACS2

Steve Whitlock
TF – IT Security
Cyber Strategy
NIST Focal

BOEING PROPRIETARY
Distribution Limited to Boeing Personnel Only

18

Leveraging KM to Align / Advance the Enterprise

Cross-Functional Excellence Evolving

- One Boeing Security Systems Engineering BPs
- Common Threat Assessment Methodology
- Engineering / IT / Supply Chain / Ops Working Together

Growing Information Security Expertise

- Over 423 Enterprise BDEs (up from 59 in April 2013)
- Multi-site representation – 180+ in WA, 70+ each in MO, CA
- Over 8,800 InSite discussions on Info Security topics
- Boeing Knowledge Management: SSE and IA COPs

Engaging Key USG Stakeholders

- NSA 2-day Course delivered to 230+ across 16 sites
- NIST engaged in DHS Coordinating Sector discussions

Knowledge Management Network / KM Team facilitating One Boeing Sharing

Boeing Proprietary – Distribution Limited to Boeing Personnel

Achieving Sustainable Enterprise Ownership of Cyber Threat

Summary

- TOP Priority remains protecting our Network/IP/People Data
- Seeing Sustainable Enterprise Ownership of Cyber Security
  - Cyber Security Leadership emerging across Enterprise
  - Cyber resources (people, processes) improving, increasing in number
  - Need to accelerate developing Cyber Talent beyond IT
- Regulatory Threat increasing *(Executive Branch moving quick)*
- Corporate Risk Profile improved – but threat evolving