

## 5th DoD PK Enabling Technical Forum

November 20, 2003

# Secure Collaborative Environment

Previously Called US-UK Generic DMZ Architecture  
Officially Called Transatlantic Secure Collaboration Environment

### *Requisites for Collaboration*

- *Strong Identity Management*
- *Data Segregation Management*

Paul D. Grant, Information Assurance Executive

Office of the DoD Chief Information Officer

Paul.Grant@OSD.Mil



Power to the Edge 

# Importance

## **The Giants of Defense Industry are Putting Their Money on Solving “Net Centric” for Themselves**

- **Same Solution Space that DoD is Pursuing / Funding**
- **Names/Motivations may be different, but Results = Same**
- **All Concerned Accept Need to Interoperate**
  - **Internationally**
  - **Between Competitors and Sub-Contractors**
  - **With their Defense Customers,**
    - **DOD, MOD, Other Primes, Other Government Organizations**
- **These Companies Deploy With Us**

**For the Finish Line, We now have opportunity to Help:**

- **Build to Interoperability (on the first try)**
- **Use Their Synergy and**
- **Pool Results of Our Combined Investments**



*Power to the Edge* 

# “A Framework for Secure Collaboration Across US/UK Defense”

- **Published, March 5, 2003**
- **Sponsored and Paid By:**
  - **Rolls-Royce**
  - **BAE Systems**
  - **General Dynamics**
  - **Lockheed Martin Corporation**
  - **Raytheon Company**
- **Advised By:**
  - **US DoD**
  - **UK MoD**
- **In cooperation with UK Council for eBusiness**
- **Prepared by Booz, Allen, Hamilton**

**Report is Available at:**  
**<http://www.afei.org/news/framework.cfm>**



# SCE Framework

- **Purpose:** Provide principles and guidelines that any US/UK-based defense contractor can use to provide a SCE
  - Identify requirements and policy issues to develop an architecture that enables geographically dispersed business partners to securely collaborate
  - Develop a common framework and a flexible, secure, collaborative environment design
- **Open Document:** Designed for guidance of any defense industry company or government organization that needs to work in a collaborative environment



# Intermediate Products That Fed the Framework

- **Catalogue of Design Requirements** (Nov 21, 2002 )
- **Analysis of the Collaborative Policy Environment** (Nov 21, 2002)
- **Following identified for Elaboration in Framework**
  - Info Security
  - Export
  - Risk Models
  - Identity Management
  - Marking and Handling
  - Data Purging
  - Certification and Accreditation
  - Computer Network Defense
  - Enterprise Configuration Management
  - Encryption
  - Verification
  - Privacy
  - Personal Security
  - Physical Security



**Prepared by BAH for participating companies**

*Power to the Edge* 

# The collaboration model is changing to adapt to the new industry trends . . . the security solution must be equally adaptable and flexible

A Net-Centric DoD  
NII/CIO

STRATEGIC DRIVERS

BUSINESS DRIVERS

SECURITY DRIVERS

## Previous Collaboration Model

## Emerging Collaboration Model

1

Industry Structure

- National – Collaboration strategy based on national model of primes, subs, and suppliers

- International – Collaboration strategy based on international model of primes, subs, and suppliers

2

Business Model

- Product-Centric – Collaboration oriented around a particular product line and development phase

- Service-Centric – Collaboration spans entire lifecycle and multiple product lines

3

Organization

- Business Unit – Developed to support a particular line-of-business

- Extended Enterprise – Collaborations stretches across business units, company boundaries and international borders

4

Collaboration Model

- Static – Developed in accordance with policies and regulations of particular product line; little change or flexibility

- Dynamic – Rapidly adapts to changing business model and introduction of new partners

5

Focus

- Function – Collaboration systems developed to support one particular function (e.g., exchanges, R&D, supply-chain)

- Value Chain/Life-cycle – Collaboration spans the entire lifecycle with reusable data

6

Security Drivers

- Government – DoD/MoD security regulations and export control policies

- Commercial – Corporate policies designed to protect intellectual capital or competitive intelligence

7

Security Model

- Network-Centric – Security designed around the network (e.g., DMZ, firewalls)

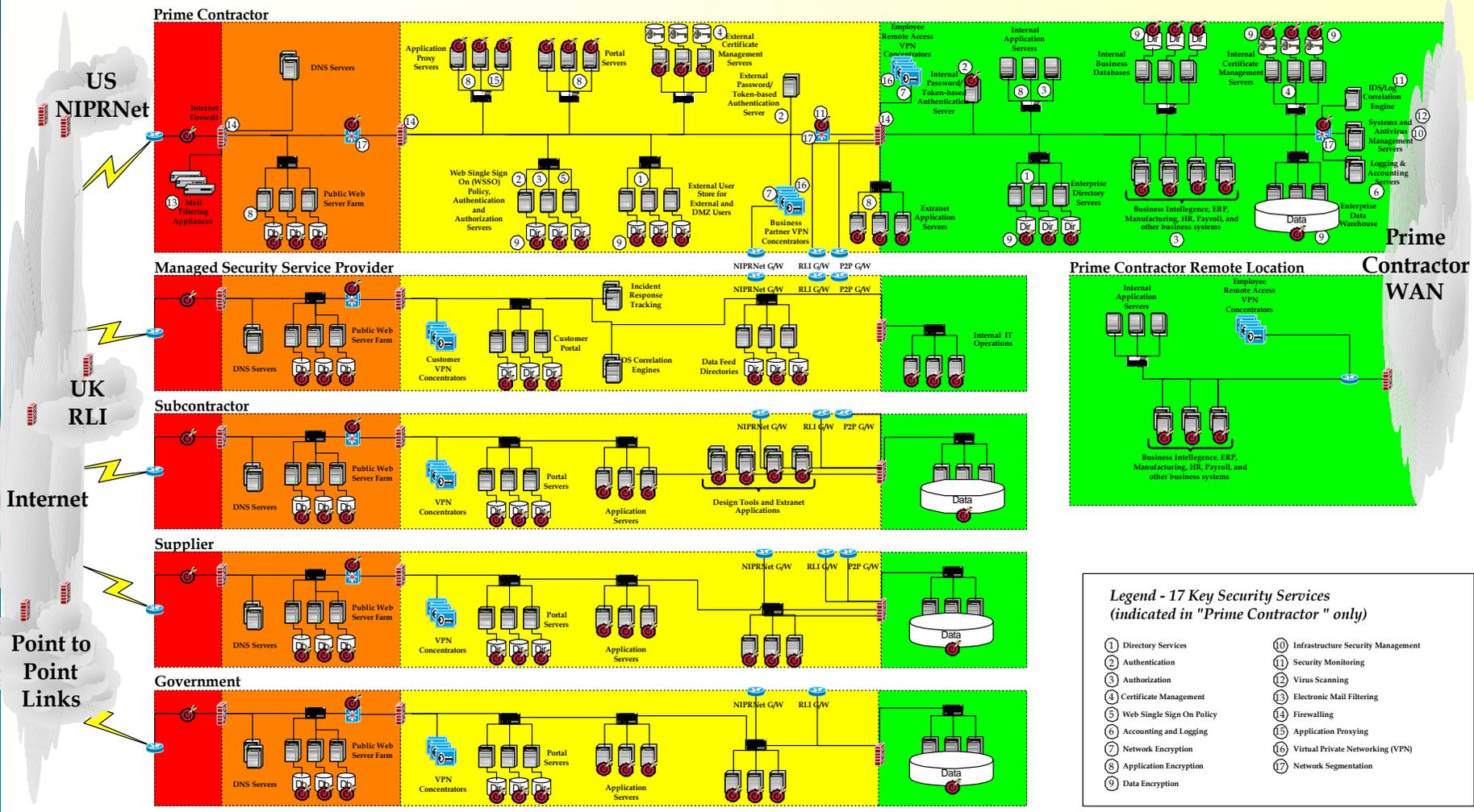
- Data-Centric – Security built into the data (e.g., data tags/XML)



*Power to the Edge*



# Conceptual architecture is structured around four "trust" zones with the yellow "trust" zone hosting the secure collaborative environment



**Legend - 17 Key Security Services (indicated in "Prime Contractor" only)**

|                             |                                      |
|-----------------------------|--------------------------------------|
| ① Directory Services        | ⑩ Infrastructure Security Management |
| ② Authentication            | ⑪ Security Monitoring                |
| ③ Authorization             | ⑫ Virus Scanning                     |
| ④ Certificate Management    | ⑬ Electronic Mail Filtering          |
| ⑤ Web Single Sign On Policy | ⑭ Firewalling                        |
| ⑥ Accounting and Logging    | ⑮ Application Proxying               |
| ⑦ Network Encryption        | ⑯ Virtual Private Networking (VPN)   |
| ⑧ Application Encryption    | ⑰ Network Segmentation               |
| ⑨ Data Encryption           |                                      |

**Legend - Components**

|                             |                                       |                       |
|-----------------------------|---------------------------------------|-----------------------|
| Router                      | Network IDS Sensor                    | Certificate Directory |
| Network Segmentation Device | Server with Host-based IDS Sensor     | Directory (LDAP/X500) |
| Load Balancer               | High-speed Data Line (T1, E1, DSL...) | Database              |
| VPN Concentrator/Gateway    | WAN/Internet/P2P Networks             | Server                |
| Firewall Cluster            |                                       |                       |

**Legend - Trust, Data Storage, and User Sessions Zones**

|  |  |
|--|--|
| <b>No Trust - Internet Network</b><br>Data - No data stored<br>User - Unauthenticated user sessions permitted  | <b>Collaboration Trust - DMZ</b><br>Data - Only external user data and portal policy data stored<br>User - All user sessions must be authenticated. All user sessions are encrypted via VPN and application level encryption                           |
| <b>Public Trust - Public Network</b><br>Data - Minimum public web-application data stored<br>User - Unauthenticated user sessions permitted from all zones | <b>Trusted - Corporate LAN</b><br>Data - All application data and internal user data stored. The majority of all data stored in this zone.<br>User - No user session permitted from YELLOW Zone. Only employee user sessions permitted via VPN or LAN. |



Power to the Edge

# Next Block of Work Funded and Underway

- **Opened Invitation for Others to Join and Help**
  - Participation increased and added:
    - Northrop Grumman, Westland Helicopters, Boeing
    - Now at 10 With Others expressing Interest
    - Canadians are in (DND and CAE) (Dutch expressing interest)
- **Pilot the Framework in Current Programs**
- **Export Data Segregation**
  - Data Tagging & Rule-based Content Management,
  - Data Management, Protection
- **CIDM**
  - Strong Access Control based upon Identity and Roles
  - Requires Trust between Partners



# From First Body of Work Companies Agreed to Pilot Framework

- **Lockheed**
  - JSF, C130J
- **General Dynamics**
  - Bowman, Astute, Electric Boat
- **BAE SYSTEMS**
  - Sub on JSF, Astute, CVF
- **Rolls-Royce**
  - Sub on JSF, EJ200 (Eurofighter), internal and other programs
- **Raytheon**
  - Javelin/Astor



# The Players Today



**BAE SYSTEMS**



**Raytheon**



**WESTLAND**



**smiths**

## Related - Affiliates

- UKCeB
- Booz, Allen, Hamilton
  - Contractor
- Exostar
- AFEI
- AIA

- **US Government**
  - Department of Defense
  - Department of State
  - NIST
- **UK Government**
  - Ministry of Defense
  - DTI
- **Canadian DND**



*Power to the Edge* 

# The Players

## US Government

- **Department of Defense**
- **USD Policy**
  - DTSA
  - USXPorts Program
- **USD AT&L**
  - DSCA
- **USD P&R**
  - DMDC (ACO)
- **DoD CIO**
  - DISA & DTIC
  - PKI PMO
- **USD I**
  - DSS
- **JSF JPO**
- **FCS PMO**
- **Department of State**
- **Department of Commerce**
  - NIST
- **Department of Homeland Security**
- **INTELINK Mgmt Office**
- **Federal Id & Credentialing Committee**



## Next Steps

# Export Data Segregation

Statement of Requirements and Statement of Work

To establish guidance on the minimum set of security mechanisms that could enable a company to have confidence that it would not commit an export violation. The core of this work will be around data tagging and content management.

**By any other name, this is data management for use in secure collaboration in a net-centric environment.**



*Power to the Edge* 

# Next Steps

## Collaborative Identity Management (CIDM)

### Statement of Requirements and Statement of Work

To establish a Framework for CIDM so that organisations' identity management regimes can interoperate. The Framework will need to take account of major, existing CIDM initiatives e.g. US DOD CAC PKI, Federal Bridge, MOD/DECS Chambersign etc as well as other coordinating bodies e.g. PKIX, OASIS, ISO.

**By any other name, this is identity proofing for use in secure collaboration in a net-centric environment. For DoD, it is our CAC Program and the Federal Bridge Certification Authority.**



# Recommendations to Move to Secure Collaborative Environment

- **Engage with the Others working “net centricity”**
  - Large Defense Contractors (for their enterprise)
  - Other Ministries / Departments of Defense
  - Must be interoperable
- **Apply the Framework to Your Efforts**
  - Both Internal and External,
  - Expect it from Primes and their subs, e.g. JSF, FCS
- **Assist the Interoperable Convergence to Secure Collaborative Environment (SCE)**
- **Emphasis on:**
  - Collaborative Identity Management
  - Sharing Data that is Segregation Managed



# BACK UP Slides Follow



*Power to the Edge* 

# References

- **DoDD 8500.1, Information Assurance, Oct 24, 2002**
- **DoDI 8500.2, Information Assurance (IA) Implementation, Feb 6, 2003**
- **DoDD 8190.03, Smart Card Technology, August 31, 2002**
- **Deputy Secretary of Defense Memorandum (DEPSECDEF), “Department of Defense (DoD) Public Key Infrastructure (PKI)”, Aug 12, 2000 \***
- **DEPSECDEF Memorandum, “ Public Key Infrastructure (PKI) Policy Update”, May 2002 \***
- **DEPSECDEF Memorandum, “Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)”, May 17, 2001 \***

**\* = Will Become DoDI 8520.bb, PKI and PKE, with associated Policy Memorandum**



## Booz Allen was tasked with capturing requirements, analyzing policies, and developing a design to enable secure collaboration for defense contractors

- Background
  - **UK MOD, US DoD, and industry exchanges need a secure collaborative environment that meets the collaborative business goals without compromising the competitive or regulatory environment**
- Requirement
  - Provide a document **that a company can present to their IT Department or Information Systems service providers to guide in the form of framework of architectural, procedural, technical, and security measures the implementation of a solution that meets the business needs**
- Approach
  - **Capture the requirements, assess the gaps, and identify where policy needs to evolve, and advise MOD and DoD and corporate management on how this can be achieved**
  - **Design a framework of principles and guidelines**
  - **Identify technical, procedural and management characteristics that must be present**
- Success Criteria
  - Participating companies **have endorsed and accepted the requirements, design, and framework**

**The US DoD and UK MOD regulatory authorities have accepted the framework**



*Power to the Edge* 

# History of Identity Management in the Dept of Defense

- **1988: DoD documented requirement for hardware PKI tokens for all employees**
- **1998: DoD PKI project initiated as technology became available and price became affordable**
- **2002: Version 3 of PKI deployed**
- **May 2003:**
  - **2 million people have Common Access Cards**
    - **60% of Target**
  - **2.6 million Common Access Cards Issued**
    - **Includes replaced – reissued cards**
  - **11,000 issued each day**
  - **Target 3.4 Million by end of year**



# Identity Management

- **Separate Identity from Attributes**
- **Strong Identity Management**
  - **Everyone needs strong credentials**
  - **Only one world-wide infrastructure**



*Power to the Edge* 

# DoD's PKI Program

- **Security Services**
  - Authentication → **Digital Signature using identity keys**
  - Integrity → **Digital Signature using identity keys**
  - Non-Repudiation → **Digital Signature using identity keys**
  - Privacy / Confidentiality → **Encryption using encryption keys**
- **Face to Face Identity Binding**
- **Hardware token**
  - Difference & Rationale
- **Robust Infrastructure Configuration Management and Operations**



# External Trusted Mechanisms

## External interfaces

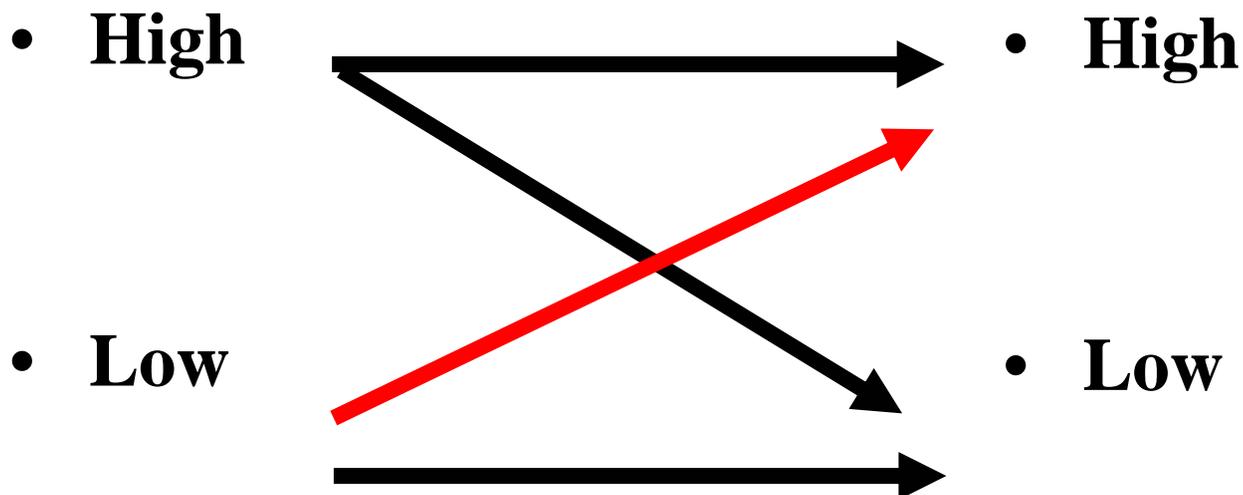
- **Need trusted, external identity management**
  - **Other US Government Organizations**
    - Federal, State, Local
  - **Coalition Partners**
  - **Sustaining Base (Private Sector)**
- **Federal Bridge Certification Authority**
- **Privilege (Role) Management Must be Dynamic**



# Identity Proofing for Data Access or Privileged Access

## Id Proof Strength

## Data or Privilege Value



*Power to the Edge*