Architecting a Secure Enterprise Data Sharing Environment to the Edge

Deborah L Farroha – DoD
Bassam S Farroha, Ph.D. EE, MBA – DoD

Presentation for the INCOSE
Symposium June 2011 Denver, CO

Introduction

- This paper investigates **securely sharing** information with the tactical user ***while protecting the data and the information systems*** from intruders and malware.
- How to best **share** information **across traditional and non-traditional domain boundaries.**
- In Federal Government, Local Government and Commercial Entities, there is ***no consistent way to discover, access, or share data, without a priori knowledge*** of where systems are, how to access them, and how to query them & having **prior authorization**.
- This situation was partially created by **funding approaches** where each organization, and mission are assigned their individual funding vehicle and asked to efficiently manage those funds to develop needed capabilities.

Introduction

- Developing a **Comprehensive Data Services Architecture** will **provide a mechanism to access multiple data sources** utilizing common approaches.
  - enable ***enterprise-wide data discovery*** and providing the end users with relevant information.
- In the new Information sharing environment, we have the responsibility to **share some information, while protecting others.**
  - **utilize** *Meta-Data* and *Digital policy* **to identify what is sharable and with whom.**

Drivers for Expanded AIS

- We are **facing an explosive growth in data types** and volume
- Along with an **exponential increase in the speed and power** of **processing capabilities**.
- We need to enable:
  - *Horizontal discovery*
  - *Secure Data tagging*
  - *Automating Access Authorized*
  - *Identification/Consumption relevant data*
- Regardless of:
  - *Physical location*
  - *Data type (ex VoIP, E-Mail,…)*
  - *Technical implementation*

Info Sharing Philosophy Shift

- **Original State** – "**Need To Know**" minimal, if any, sharing outside of "home" domain.
- **Next State** – "**Need to Share**" encourages sharing among services, agencies, coalition partners, and state/ local organizations…
- **ENTER**: Wiki-leaks…..
- **Present State** – **Balanced approach** to share as much as securely possible…based on *Authenticated Identity, Credentials, to grant access*…need to follow the letter of the law in sharing.

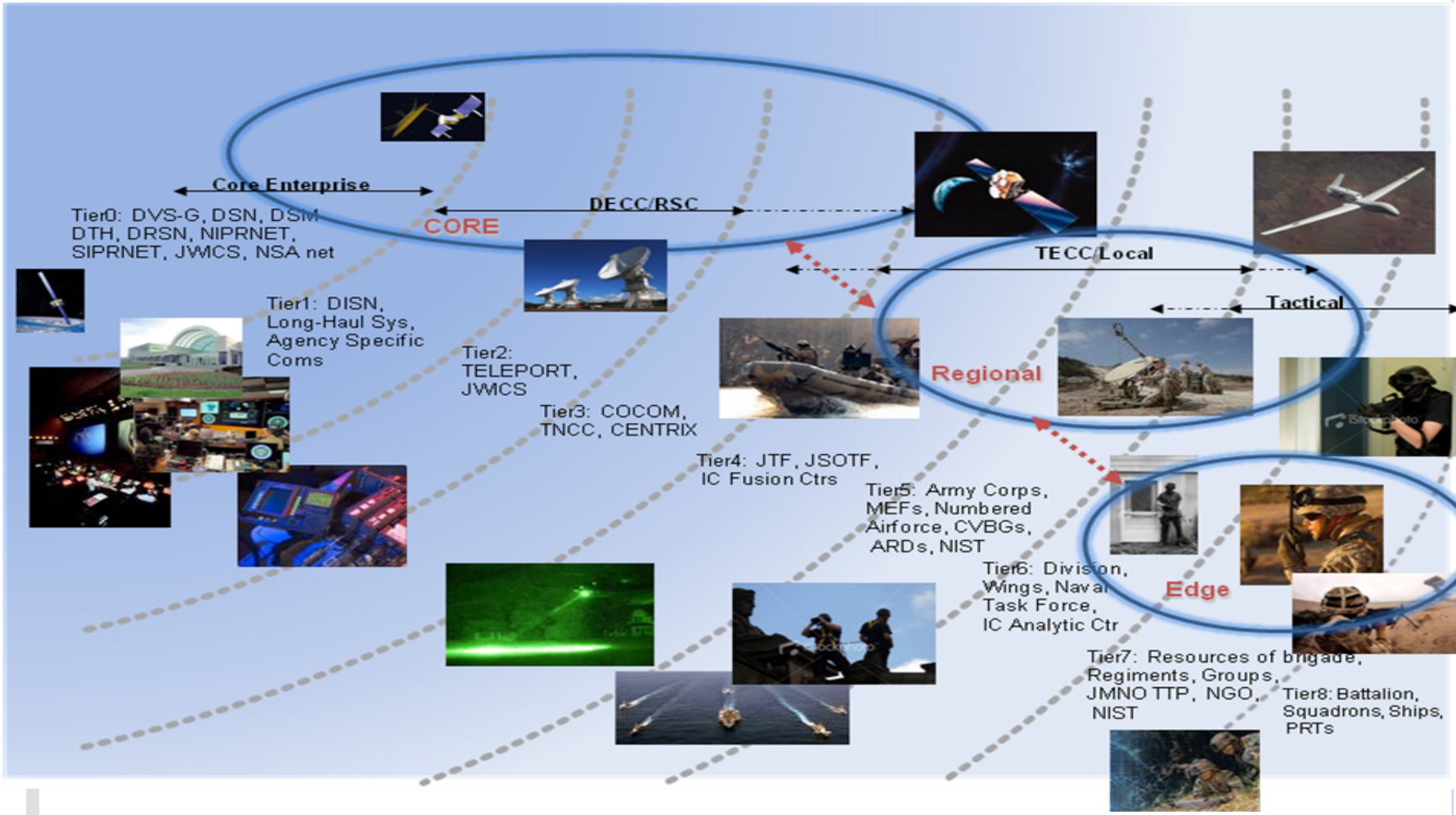
All the way to the Tactical Edge

Where is the Tactical Edge?

- Some of the characteristics that traditionally identified a tactical system:
  - Edge with respect to type of Communications systems
  - Mobile Units
  - Wireless Connections
  - Quality of Service over the connection
  - Throughput and Data Rates
  - Reliability of links
  - Error Rates
  - Limited Size, Weight, and Power
  - Distance from the perceived Core
  - Level of physical or logical threat on the link
  - Multi-Hop before reaching destination
- Continuously evolving as technology changes

What is the “Tactical Edge”?

Everything forward of a deployed tactical network’s main servers



Information Sharing

- **Historic** Roadblocks to Information Sharing
  - ***No consistent way to discover, access, or share data***
  - *Need* ***Prior knowledge*** of location, access and query methods
- Long Term Goals to Improve Information Sharing
  - ***Improve architecture*** and design of IT systems
  - ***Provide Common interfaces*** and ***interoperable meta-data***

Share SECURELY

Threats to The Tactical Edge
Coalition Environment

- Includes all the typical security and operational challenges

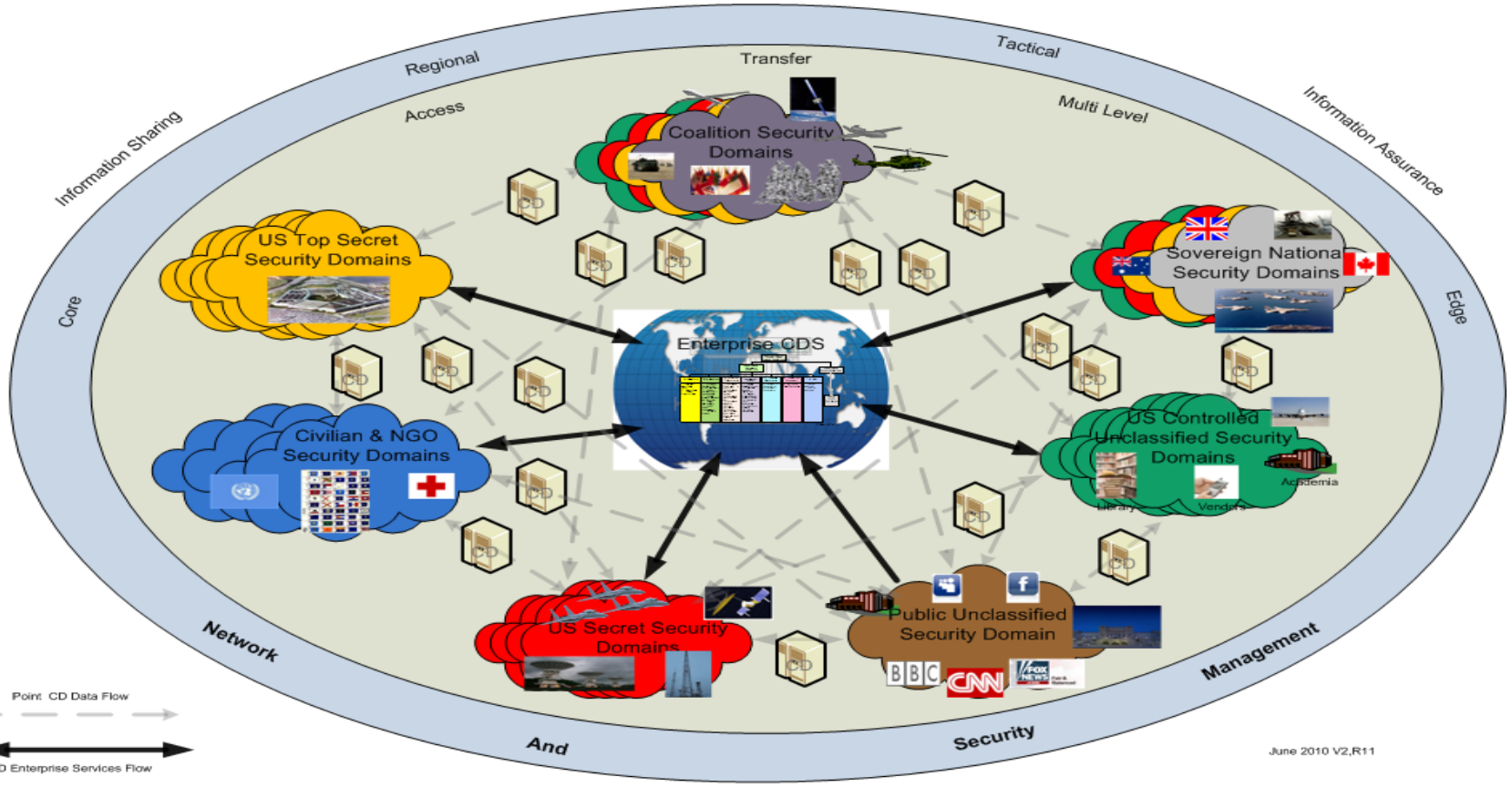
PLUS

- **Physical control over datalink** is *limited*
- Information being shared ***between*** **government**, defense, non-government, and **foreign partners**
- Various **dissimilar classification** methods and labels among partner nations
- Dissimilar **infrastructures**
- Foreign Partnerships of highly dynamic nature with **intricate political sensitivities** among members
- **High Probability of Information Compromise**
  - *Equipment Capture* or *Transmission Intercept*

Security Domains

- Each organization's *protected information systems*, data and processes constitute a ***security domain***.
  - We *need to defend against internal, external, and natural threats*
- Multiple organizations have protected domains including Health Care, Banking, Securities Exchange, etc
- Dept of Justice, Dept of State, Dept of Defense ….
  - Unclassified, Confidential, Secret, Top Secret
- **Tactical & Edge** are usually considered a **separate domains** due to added threat level

High Level Representation of CDES



Community Cross Domain Enterprise OV-1

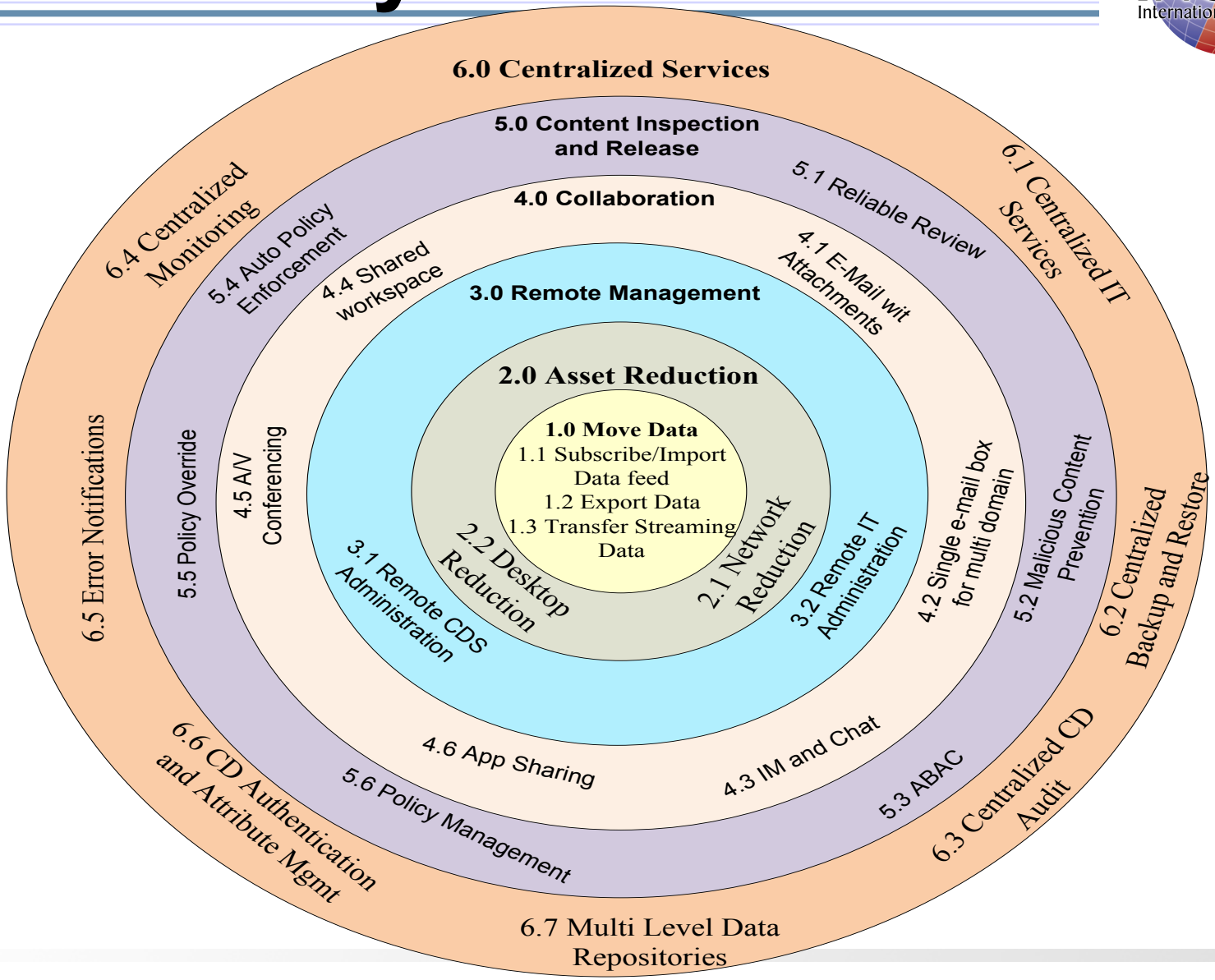
CD Functions & Protection Criteria

- Types of CDS (Guard) - Functions
  - Transfer, Access, Multi-level
- Basic operations of most common CDS types
  - Low-to-High Transfer; malicious code inspection
  - High-to-Low Transfer; Dirty-Word/Reliable Human Review
  - High-to-Low Access with Anonymizer
  - Low-to-High Access - **Not Allowed**
- Data services
  - Audit Trail of entities accessing sensitive data
  - Meta-data tagging and Crypto-binding

Protection Methods for Data Sharing & Data Security

- Guards
  - Generally implemented on trusted platform (often B1 or higher)
  - Connects domains at different levels
  - Opens doors that are normally closed
  - Prevents data leakage
  - Filters data at application level
  - Few services allowed through (e.g., E-mail, messages, file transfer)
  - Often no IP forwarding
  - Performs downgrading
- Firewalls
  - Not generally implemented on trusted platform
  - Connects domains at same level
  - Closes doors that are normally open
  - Controls network services
  - Filters packets at protocol level; may proxy packets at application level
  - More services allowed through (e.g., file transfer, E-mail, TELNET, HTTP)
  - Some types offer IP forwarding
  - No downgrading required

Taxonomy of CD Services



Sharing Information means:

- Across Traditional Boundaries
- Allied and Coalition Considerations
- Other Agencies and commercial
- The common **challenges**:
  - **Technology** – dissimilar platform architecture, undiscoverable, non-interchangeable hardware
  - **Budget** – development of systems based on local needs creates higher costs in the long term…need cost avoidance strategy
  - **Policy** – still for the most part reflects the "Need To Know" paradigm
  - **Process** – mainly based on P2P systems and source code with little external dependency tracking

Better Information Sharing Through:

- **Standards**-based and **scalable** architecture
- **Ability to pass data between domains including:**
  - **Management and control** data
  - **Situational awareness** data
  - **Information Assurance status** data
- Ability to support **remote policy administration and remote CM**
- Capability to support **discovery and retrieval** of information ***across the multiple security domains***
- Capability to **support tactical** and austere environment applications

How Do We Get There?

- SOA GIG with NetOps Management & Oversight
- "*Crawl, Walk, Run*" Data Discovery Approach:
  - Minimally Automated: builds trust
  - Enhanced Automation: introduction of **prioritized** list of returns on more automated searches
  - Automated Discovery and Subscription: ***simultaneous searches in and across multiple domains***

Quality of Service Precedence & Preemption

- For the Enterprise and Edge, we need to consider the following for proper application execution and end user services……
  - Latency, availability, reliability, security, safety, network speed, buffering and storage capacity, Error rates…
  - Routine, priority, Immediate Flash, Flash Override

Class of Service	Manual	P2P	Automated	Low level Service	Full Enterprise Services
A	X	X	X	X	X
B	X	X	X	X	
C	X	X	X		
D	X	X			
E	X				

Classes of Service

A: Class A Service will require high bandwidth and high reliability with high QoS.

B: This link will have moderate bandwidth and moderate QoS.

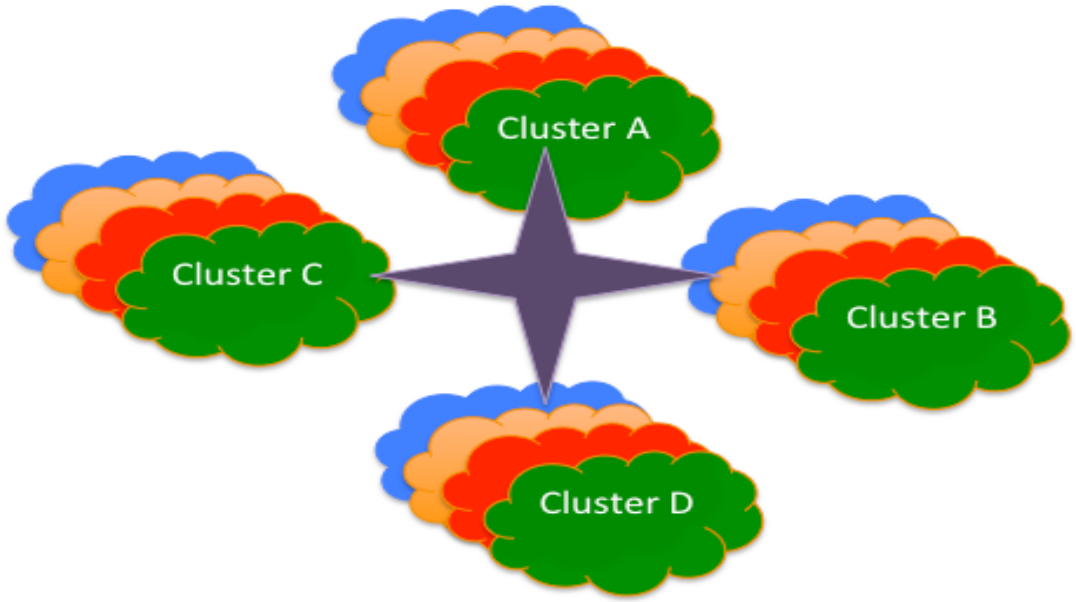
C: This class of capability is assigned for automated systems that have multi point connectivity through a portal or similar access points.

D: This type of link is a Point to Point attachment which acts as a pipe and filter to relay data between two distinct systems.

E: This service is needed when we have no datalink connections.

Technology Alternative

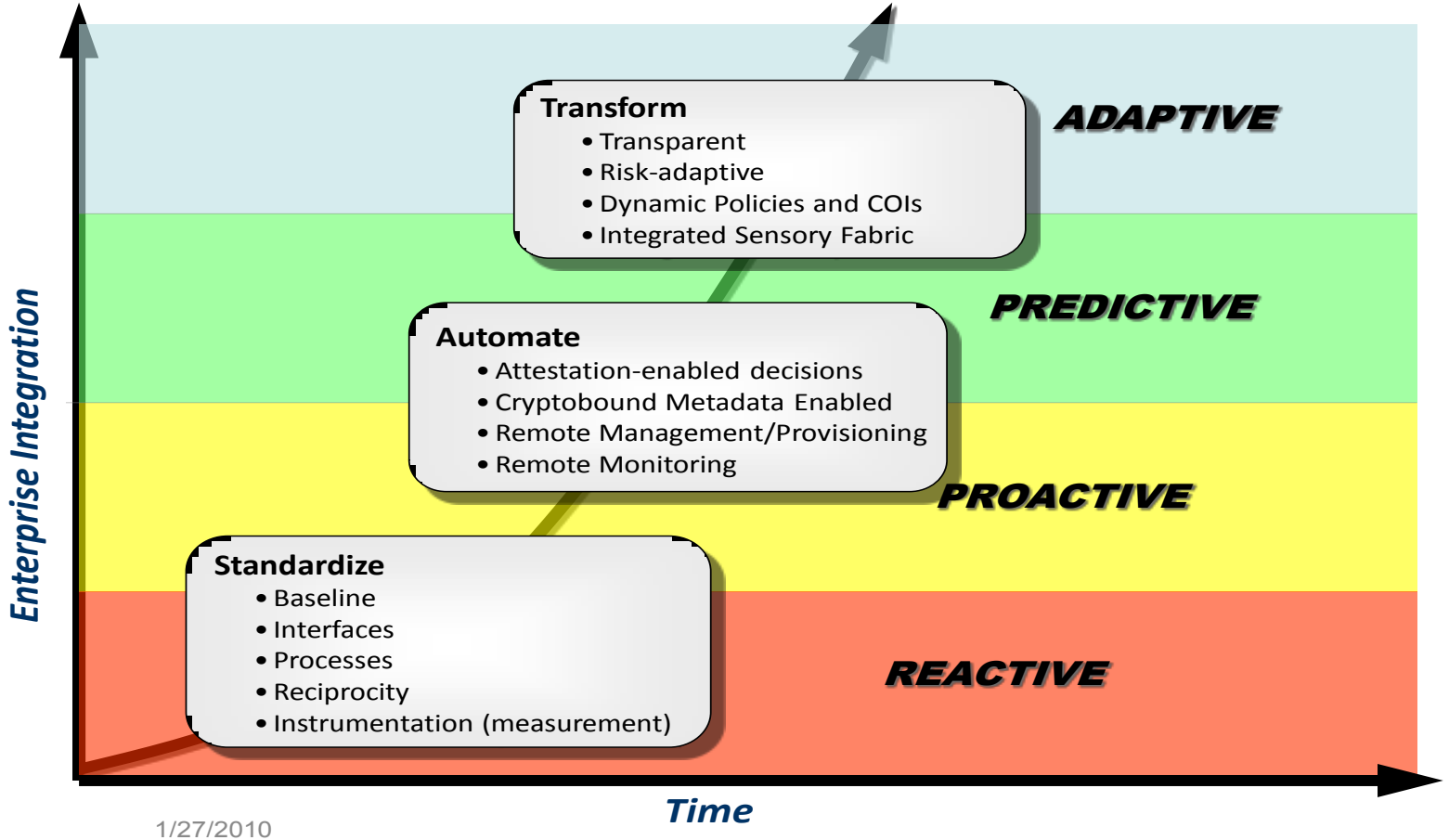
- Point to Point
- Enterprise Services…accessible by the edge
- Virtualization – reduced SWaP footprint
- Cloud – shared resources working together for faster results without huge investment for specialized hardware
- Multi-Domain in the Cloud
- Secure Mobility



Technology/Product Gaps for Assured Information Sharing

- Secure Remote Management
- Secure Cloud Environment
- Secure Streaming Media
- Crypto-Binding of Meta Data
- Accredited Virtualization Services and Multi-Level Security including above Secret level
- Secure Real-Time Collaboration
- Enhanced Identity and Access Management
- Secure Commercial Mobile Technology

Information Protection Maturation Chart



Conclusions

- We defined new Core enterprise CD services to the Edge
- We investigated the threat levels within the tactical environments
- Ultimately, the overall approach will:
  - *eliminate the stovepipe* architectures
  - *Enable data sharing*
  - *Convert P2P architecture to an integrated* enterprise with edge connections
  - opens the doors to ***discover & share*** *information across traditional and non-traditional domain boundaries.*

Conclusions

- **Strategy** must **encompass core, edge** and all in-between
- Build **flexible architectures** to enable the protection of newer infrastructure models like clouds
- ***Ensure*** **accreditation is possible**, and reciprocity is being established by all stakeholders
- **Secure data tagging** is essential for moving forward in sharing evolution
- CD Enterprise Services are a vital element in strategy for affordability, flexibility and management of assured information sharing
- Progress being made but we must **direct newer investments** to developing **common services** and information sharing.

Contact Information

Ms. Deborah L. Farroha
Technical Director
Enterprise Systems Engineering and Architecture
Department of Defense
Deborah.l.farroha@ugov.gov

Dr. Bassam Farroha
Technical Director
Enterprise Security Management
Department of Defense
bassam.s.farroha@ugov.gov

Challenges at the Tactical Edge

- Requirements are Growing – we have many thousands of edge units
- Configuring, provisioning, and auditing critical but very difficult
- Environment is Disconnected/Intermittent, Limited Bandwidth (DIL)
- Remote management needed but not securely implemented
- Small form factor (SFF) Size, Weight, and Power (SWAP) and environmental constraints
- Current governance processes are limited
- Strategies needed for integrating and interoperating from the Core to the Edge and vice versa

Security for QoS and P&P

- Controls needed for shared system resources using QoS and P&P services model:
  - User authentication
  - Precedence level access
  - Network survivability
  - Header Encryption
  - Network Robustness
  - Network Forensics