A Framework for Enterprise Security Management to Enable Enhanced Information Sharing

Bassam S Farroha, Ph.D. EE, MBA – TASC
Ms. Deborah L Farroha – DoD
Ms. Melinda M Whitfield – DoD

System and Software Technology
Conference 2010
Salt Lake city, UT

bassam.s.farroha@ugov.gov or farroha@ieee.org

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Framework for Enterprise Security Management to Enable Enhanced Information Sharing	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Northrop Grumman - TASC,4805 Stonecroft Blvd,Chantilly,VA,20151**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 22nd Systems and Software Technology Conference (SSTC), 26-29 April 2010, Salt Lake City, UT.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**30**	

Defining the Enterprise

- **Enterprise:** The enterprise includes the systems, people and data that work together to support a mission.

- **Enterprise Services:** Enterprise Services are the collection of IT services that are performed in a centralized manner over the distributed enterprise resources.

- **Enterprise Security:** Securing the enterprise components including infrastructure, data and Applications between the boundaries of the Enterprise.

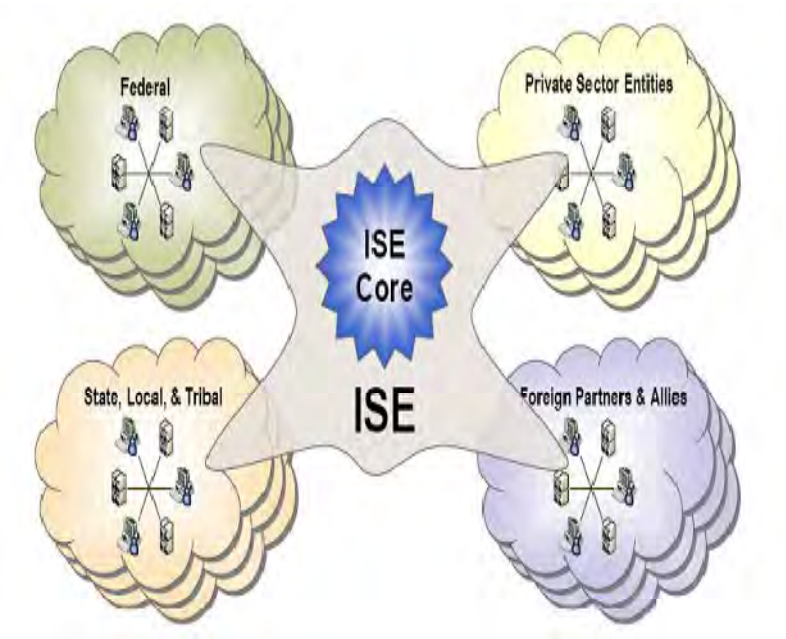
Department of Defense Global Information Grid Architectural Vision

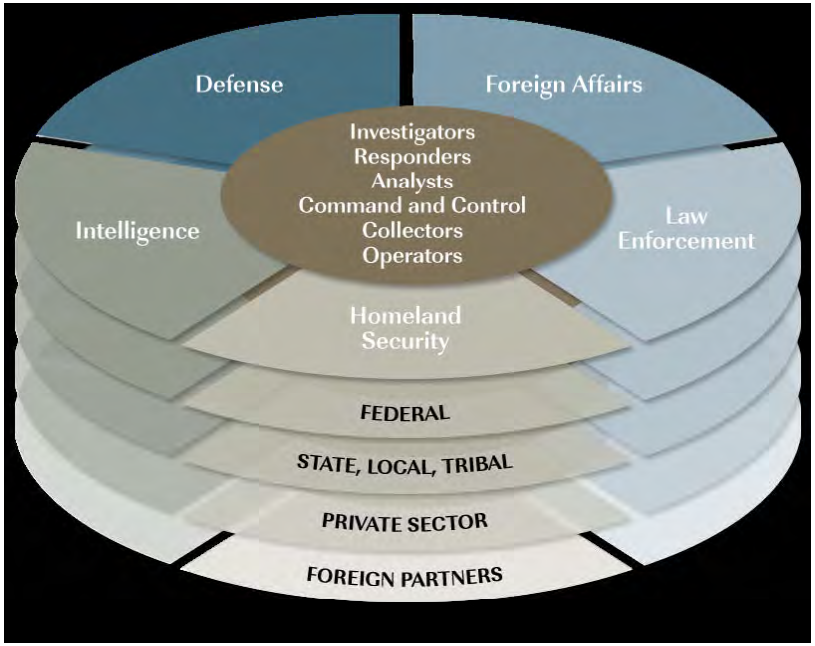
Elements of Enterprise Security Management

The main Elements of Enterprise Security Management are:

- Identity Management
- Attribute Management
- Credential Management
- Privilege Management
- IA Meta Data Management
- Digital Policy Management
- IA Configuration Management
- IA Audit Management
- Cryptographic Key Management

ISE for Multi Agency Collaboration



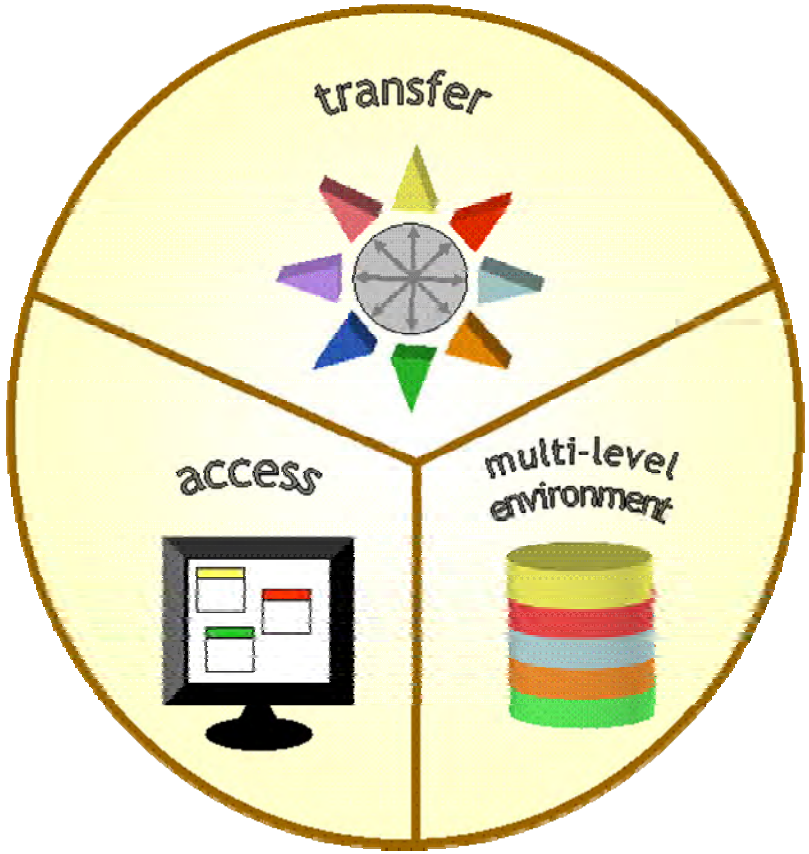


Information Sharing Environment
Enterprise Architecture Framework

CDS Vision

- Cross Domain Enterprise Services Vision Statement….. ***Secure and seamless cross domain services available when and where the customer's mission requires***

Types Of CDS



- **Transfer:** Facilitate the transfer of information between different security domains
- **Access:** User access (to apps & data) to multiple domains from a single keyboard/video/mouse
- **Multi Level:** Label-aware management of data labeled at various security levels

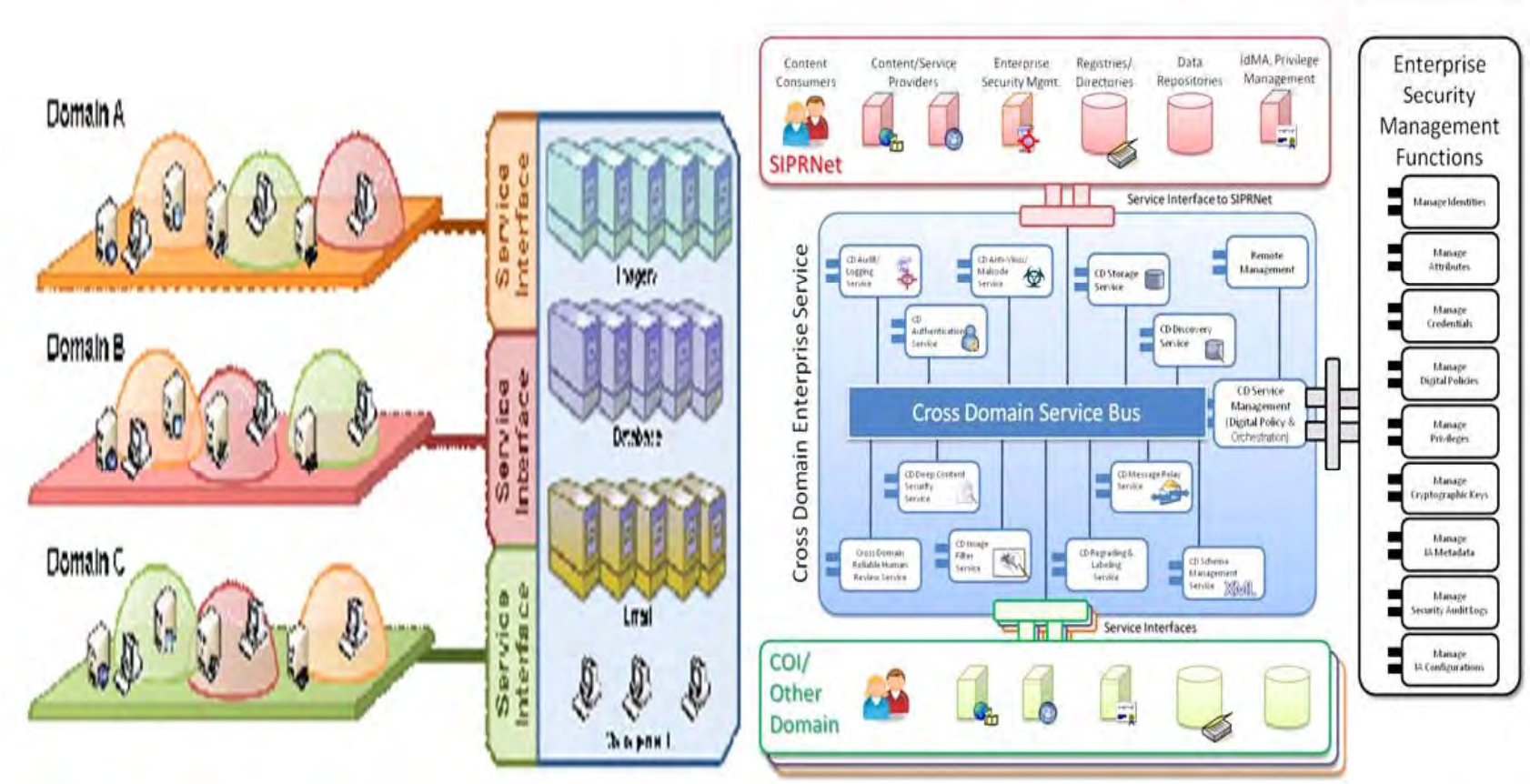
Common CD Functions

- Hidden Data detection & exposure
- Search for encrypted messages
- Reliable Human Review (RHR)
- Specialized content filtering
- Anti-Virus and Malicious Code Detection
- Data blocking like firewalls
- Cryptographic devices
- Downgrading - change classification without changing data content

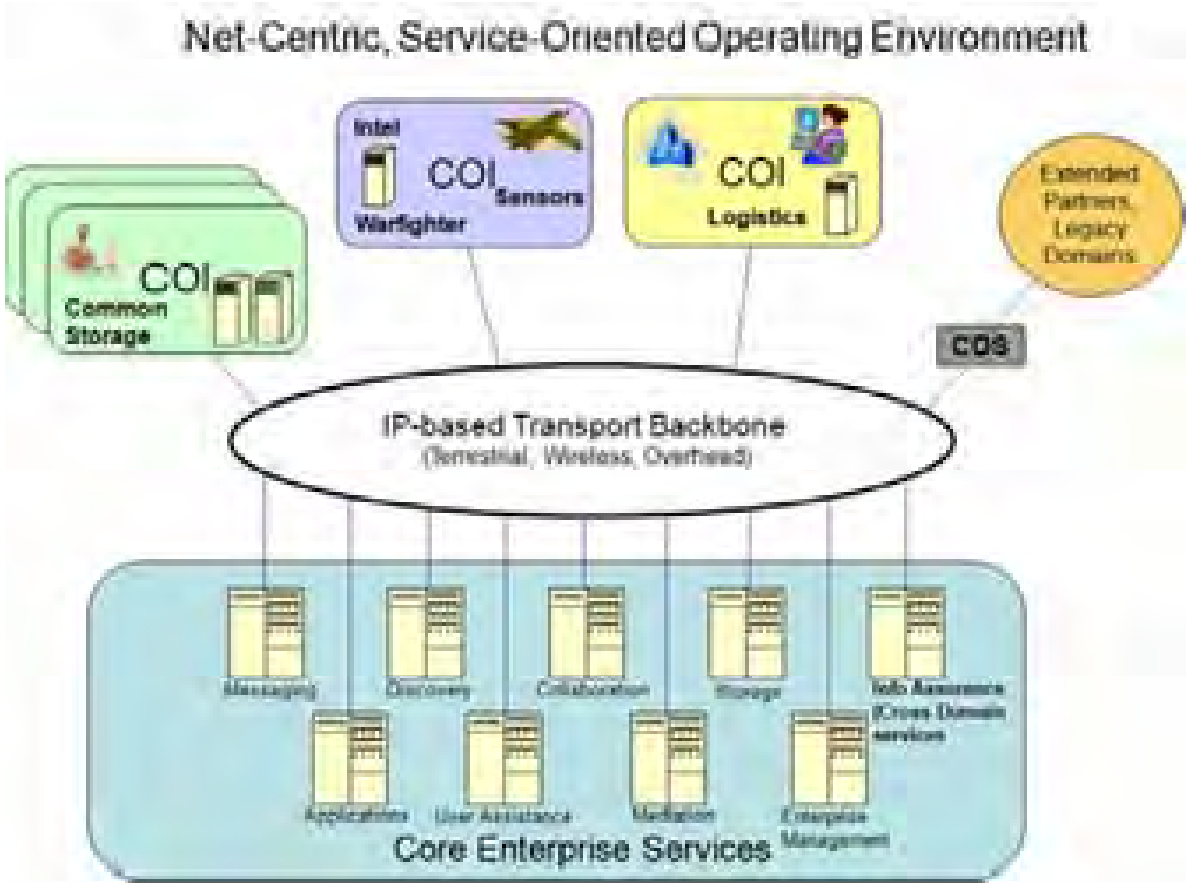
Common CD Functions (Cont)

- Prevent leakage of data from the high side to the low side
- Defend against attacks (DoS, Malicious contents,…)
- Filtering - eliminate data based on pre-defined criteria (i.e., Specific data type, classification)
- Keyword Search - search for “dirty words check”
- Integrity Checks - verify that data has not been modified
- Sanitization - remove or edit portions of text that are sensitive so that resulting data is less sensitive.

Centralized to Integrated



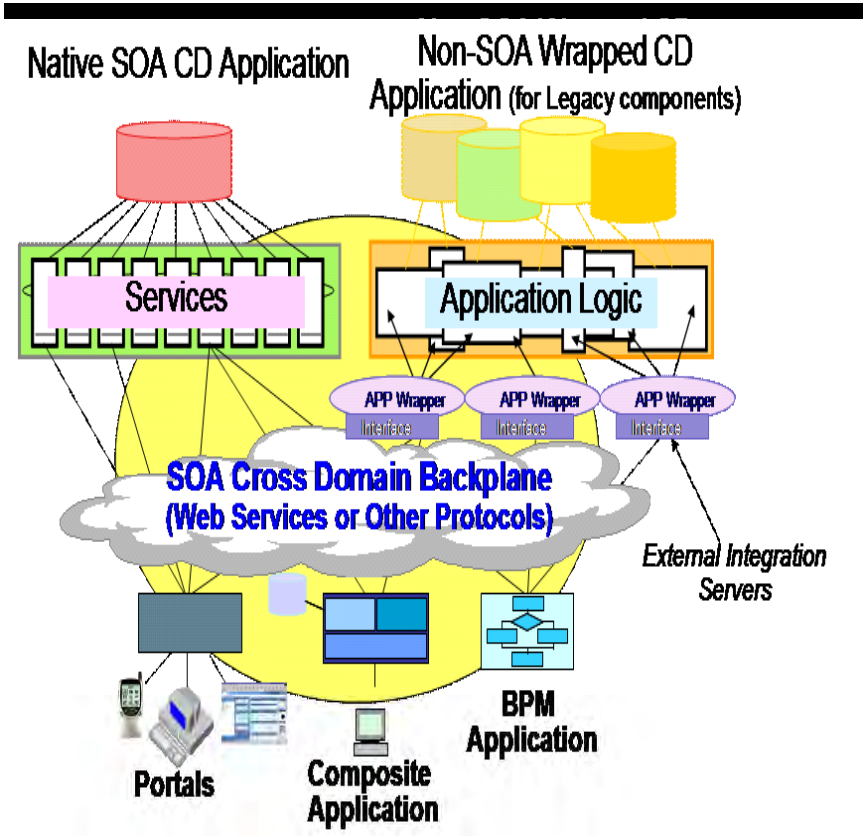
Core Services over the Enterprise Services Bus



Issues in Building a Common CD Enterprise

- Lack of acceptable cost model
- Dealing with variations of data Types and Priorities
- Developing common infrastructure capabilities
- Dealing with application versions including VoIP, IP version.
- Maintaining the required QoS for application to efficiently function
- Finding an equivalent model for the commercial SLA
- Developing an acceptable model for Enterprise Management

Objective of Resulting Architecture



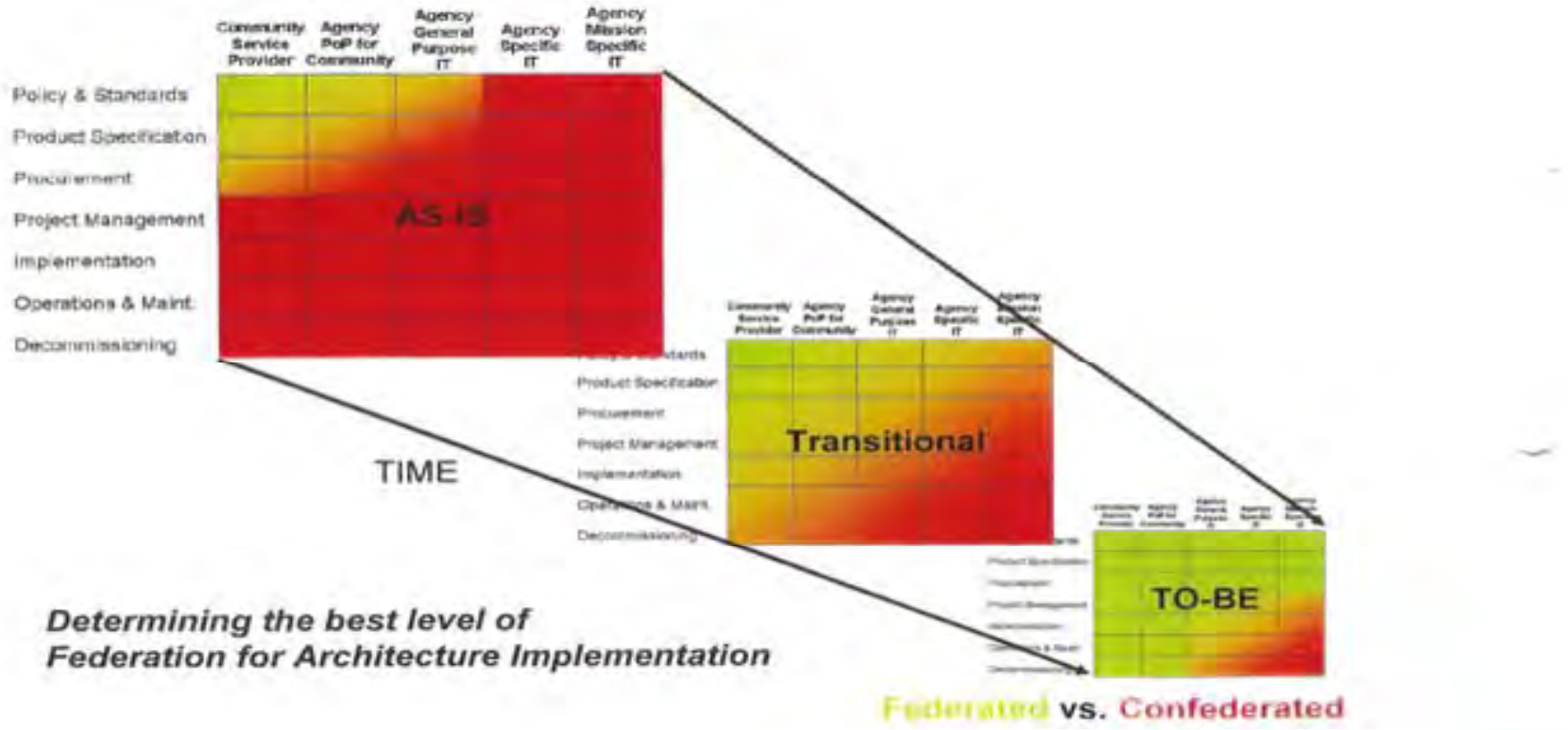
The CD Enterprise includes new and legacy Systems

- Translating the identified cross domain enterprise services (CDES) Capability Objectives into High-Level CD Requirements
- Developing an evolving Architecture for the CDES
- Developing a comprehensive maintenance and upgrade plan for the enterprise
- Understanding the evolving Constituent Systems and Relationships
- Increasing the extent to which CDES Performance Meets Capability Objectives over Time
- Monitoring and assessing potential environmental effects and impacts of changes on CDES performance
- Addressing evolving needs and solution options

ISE Enterprise Architecture Options

- **Confederated**
  - No common program oversight
  - No binding interoperability specifications
  - Changes in requirements and interfaces are not reported and no other program approval is requested.
  - Geographically dispersed Systems
  - Uncommon Data formats and standards
  - No common certification method
- **Federated**
  - Independent programs communicating to deliver a service
  - Usually have a synchronized Procurement Processes
  - largely defined by and “held together” by standards
  - Coordination at different stages of implementation
  - Synchronized Requirements/development changes
  - Reciprocity in Certification and Accreditation
- **Unified**
  - Programs are ccentrally managed for a specific purpose
  - Budgets are centrally controlled
  - systems maintain some measure of independence
  - Each program normal operational mode is in a subordinate relationship to the central purpose
  - Requirement allocation between systems and programs are under centralized authority
  - Centralized certification and Accreditation

Levels of Federation



Virtualization

- Virtualization is a technique used to provide a certain kind of software implementation of a machine that executes programs giving the impression of physical machine environment
  - Full Virtualization provides complete simulation of the underlying service layers where any software capable of execution on the intended hardware can be run in the virtual machine
  - Other Virtualization methods allow only certain or modified software to run within a virtual machine.
- Cloud Computing utilizes the concept of virtualization to provide remote services to the customers over general computing infrastructure while appearing to have customized services to each user.

Virtualization of CD Assets

- Cross Domain as a Service
- SLA need to be established
- Discover, Publish and Subscribe
- Advantages
  - Enablers for Enterprise Architecture
  - Better load balancing
- Issues:
  - Susceptibility to DoS
  - Network Loading
  - Increased latency when network loads are high
  - Need queuing, priority and QoS Algorithms
  - Certifications and accreditation

Approaches to Virtualization: Managed Co-location

- Managed collocation is often referred to as dedicated server farms.
- When using this form of service, the provider has a dedicated server that is preconfigured to certain specifications with selected software applications on it that the customer can use within limits.
- In addition to this, the provider generally takes the responsibility of providing any software upgrades to the provided applications on the system and general maintenance such as reboots, hardware issues and any backups they may include.

The typical cloud implementation utilizes managed co-location approaches.

Approaches to Virtualization: Unmanaged Co-location

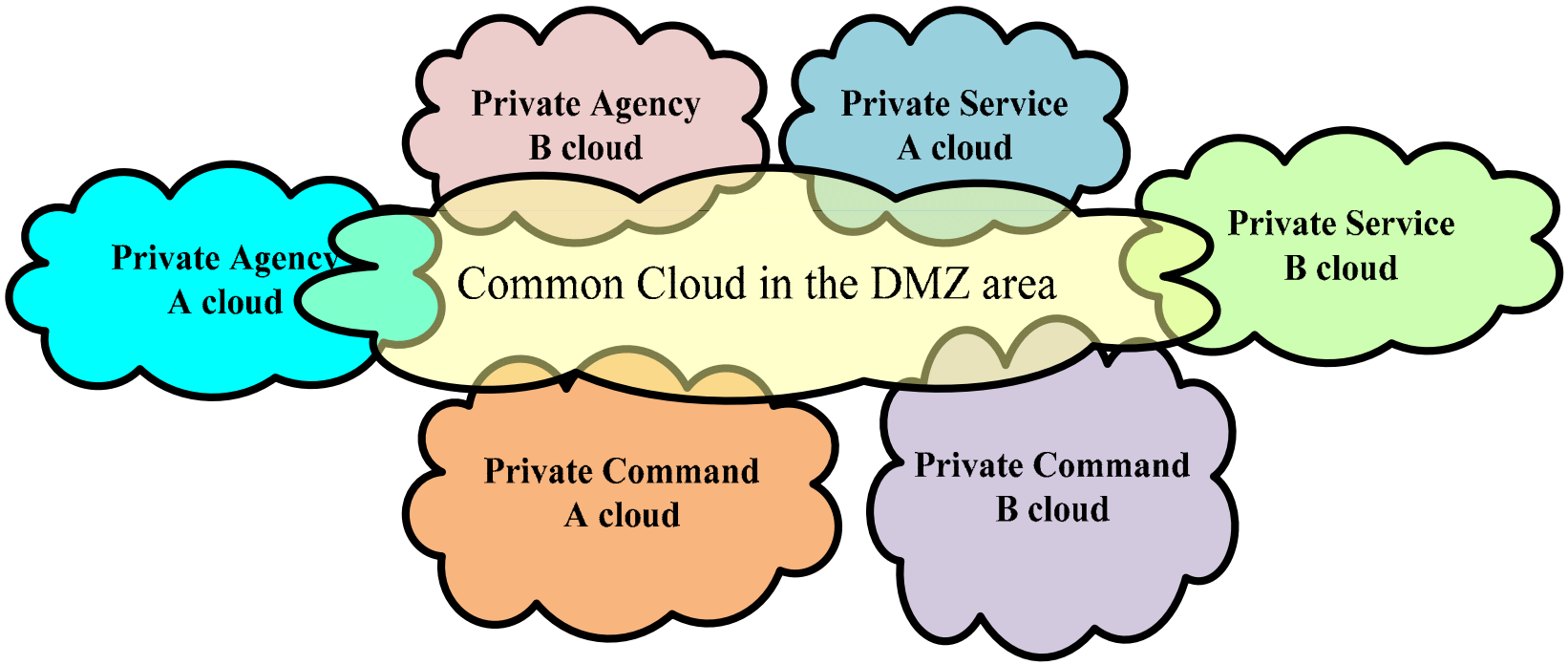
- Customers are required to provide their own hardware and manage all of the hardware and software on their own.
  - This allows for much greater flexibility in what can be done but has the drawback of more work by the customer.
- Of course, as a customer you are still bound to the service agreements of the provider.
  - Most collocation providers will have clauses that disallow certain things from being hosted on the server. These items typically include services which generate a large amount of network traffic and can cause severe problems for the provider.

When the technical requirements of running the server require applications that are not supported by the provider or you want to have more control over the configuration and use of the server, unmanaged collocation is typically the best choice.

Cloud Definition

- Cloud computing is utilizing resources as a service over an Intra-net or inter-net to provide a dynamically scalable computing or storage services.
- Cloud computing services often provide common applications that are accessed from a remote location, where the software stored on the servers and Data is sent to the servers from the user location.
- Users need not have detailed knowledge of or control over the technology infrastructure in the "cloud" that supports them.

Conceptual Cloud Model for Multi-Domain Environment



Conceptual Cloud Computing model for Inter-Domain Data Sharing

Virtualization and Clouds

- Due to the continuous increase in demand for processing and storage, system designers are always looking for architectures and algorithms to process data quicker than currently possible with available resources.
- The cloud approach attempts to assemble very large, powerful systems consisting of many small, inexpensive commodity components
  - Pro: Component systems tend to be much less costly than a single, faster machine with comparable capabilities.
  - Pro: Resources are available and underutilized
  - Con: The component resources are already consuming power, Space and producing heat
  - Con: Increased data exposure over datalink
  - Con: Prioritization of tasks over resources presents a challenge
  - Con: Software challenges are prevalent in this environment because writing software that can take full advantage of the aggregate computing power of many machines is far more difficult than adopting software for a single faster machine

The Framework

- Information Sharing between services and agencies is done utilizing Point-to-Point systems
- The Information Sharing mandate requires all information that can be shared to be made available to the agencies
- There is a need to share with coalition members
- Need to develop
  - A publish and subscribe architecture
  - Automated discovery services
  - A risk identification and mitigation plan to include cost of information exposure
  - A high level gap analysis identifying weaknesses in current architecture, auditing and authentication.
  - Order of Magnitude Cost and timeline of fulfilling the needs

Analysis Objectives

- Candidate Systems identified and potential threats classified
- Security priorities assessed
- Gap analysis between current system and desired state
  - Are the basic technologies available to develop needed capabilities?
  - Is the data protected at every point from which it can be accessed?
  - Has it adequately protected the network against previous attacks?
- Identify the Enterprise Boundaries
  - How many security domains are within the Enterprise?
  - Does the Enterprise allow low-to-high and High-to-low Transfers?
  - Does the Enterprise allow High to Low Access?
  - What other accesses does the Enterprise allow?
  - Does the Enterprise connect to international destinations?
  - Do the laws in the international destination differ about protecting data?
- Does the current security system meet or exceed industry and government requirements
- Attain a cost estimates requirements as a baseline for design phase

Design Objectives

- Work with stakeholders to finalize prioritized Enterprise security requirements
- Develop Operational Build Plan to Satisfy Requirements using agile design methods
- Assess the attack points where potential threats are possible
  - Penetration tests that simulate attacks on the Enterprise can help locate vulnerabilities
  - Don't forget the Insider threat
- Develop and socialize physical threat policies
- Identify any Virtualization Architectures that are appropriate
- *Architect a Multi-level secure system that covers all pillars of an ISE to include Intrusion detection/ prevention*
  - Ensure that IDS monitors all possible points of entry and also all sensitive points inside the network
  - Ensure that you devise systems that cover users that try to access data above their cleared level
  - When a suspicious pattern is observed ensure that the systems shuts down all data flows to the suspect part of the storage network and alerts the security managers of possible exposure
  - Tag all data
- Identify the authentication and auditing software
  - Ensure Authentication and auditing software are interoperable with coalition
- Ensure the availability of secure backup and remote data recovery measures are appropriate
- Develop the training, certification and reporting procedures
  - These procedures must be observed by all personnel accessing the secure data
- Testing/certification procedures for incremental builds and connection to external enterprises are developed

Deployment Objectives

- Ensure Physical Security in deployment location is adequate
- Ensure all personnel are only allowed access to their required clearance/access level
- Ensure that fused data gets evaluated prior to placing it on the network
- Ensure that appropriate auditing, authentication, physical security and encryption strategies as specified in design phase are implemented appropriately
- Testing completed
  - Check of compliance with test scripts recommended in design phase
  - Perform integrity tests
  - Verify system behaves as expected
- Ensure that Training is completed prior to activation
  - Develop training materials
  - Develop rules, regulations and clear penalties for violations
  - All users and managers must be trained, certified and informed of any changes in policies
- Ensure that the management processes and procedures are in compliant with the overall enterprise security requirements
  - Remember….The Enterprise is as secure as its weakest link
- Continuous testing requirements
  - Ensure that metadata is being utilized correctly, and restrictions are non-bypassable
  - Periodically Audit data to detect any unauthorized modification or destruction of information and ensure the integrity of the network
  - Regularly scan, test and audit Enterprise activities
  - Record all user activities and review on a regular basis to determine any inconsistencies
- Ensure that Security rules and procedures are updated to meet the current threat

Enterprise Security Management Trends

ESM Today	Proposed ESM
Rigid where assets are managed based on prior policy	Flexible where reconfiguration is possible to support the evolving mission
Static where planning is done prior to mission and the operational criteria is set	Dynamic where the enterprise adapts to mission and tempo
Stovepipe with interface adapters/translators and encapsulated messages	Federated where components are independent but support interoperability
Secure where security needs are set and the evolving mission might require changes or suffer	Assured where risk and access are balanced
Manpower Intensive where management is physically distributed and manually performed	Transparent where speed of reconfiguration enables the changing mission

What Does the Community Need to Investigate

- What type of virtualized architecture is most appropriate for the CD systems (local clouds, global clouds, Unmanaged Co-location, Managed co-location, ..)
- How do we deal with an enterprise that has virtualized components that span across a cloud (i.e cloud resources on more than one domain, or user and clouds on different domains, or..)
- How do we deal with the classification level when the data fusion or processed data within the cloud delivers higher classification than the input
- Can we get the certification authorities to update their standards and methods to accommodate this new technology in time
- Can we develop a cost model that follows commercial service providers where the provider assume all costs of the operations, gets paid for the services, and be accountable to delivering QoS according to an SLA.
- Identity and Privilege management across the clouds
- Crypto Binding Advantages and Issues with propagation

Contact Information:

Dr. Bassam S Farroha
Chief Systems Engineer/Chief Architect
Northrop Grumman - TASC
Supporting the DNI/CIO at the UCDMO
farroha@ieee.org
bassam.s.farroha@ugov.gov
Office 240-373-2547 Mobile 443-676-9420

Ms. Deborah L. Farroha
D/Chief Enterprise Systems Engineering
Department of Defense
Deborah.l.farroha@ugov.gov

Ms. Melinda M Whitfield
Chief Strategist
Department of Defense
UCDMO
Melinda.m.Whitfield@ugov.gov
Office 240-373-0796

Acronyms

- APP = abbreviation for application
- BPM = business process management
- CD = cross domain
- COI = community of interest
- DoS = denial of service
- IP = internet protocol
- ISE = information sharing environment
- QoS = quality of service
- SLA = service level agreement
- SOA = service-oriented architecture
- VOIP = voice over internet protocol