

Joint Cross Domain eXchange (JCDX): Integrating Multilevel Command and Control into a Service Oriented Architecture to Provide Cross Domain Capability

An Accredited Approach
to Cross Domain Information Sharing



Presented By:
Christopher J Raney
SSC San Diego



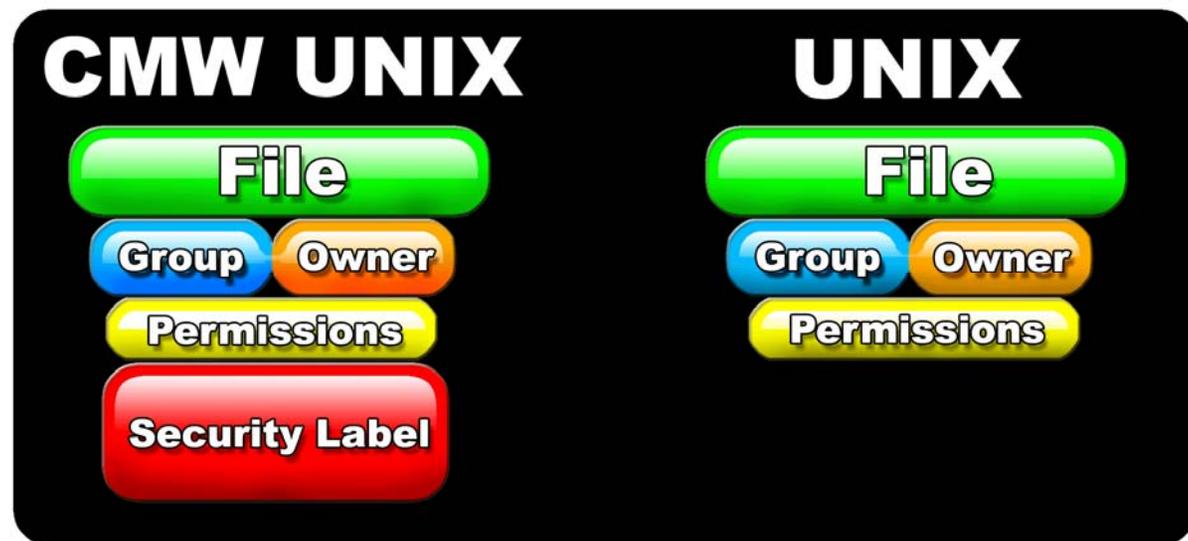
Multi-Level Secure (MLS)



UNCLASSIFIED

- MLS labels every file at the appropriate security level
- Labeled files are only accessible to users with the proper security clearance

- The labeled files are compared to the user's credentials and proper access is only given to their appropriate level



CMW:

Compartmented Mode Workstation. The core operating system of an MLS system.

UNCLASSIFIED



Multiple Security Levels (MSL) Challenges



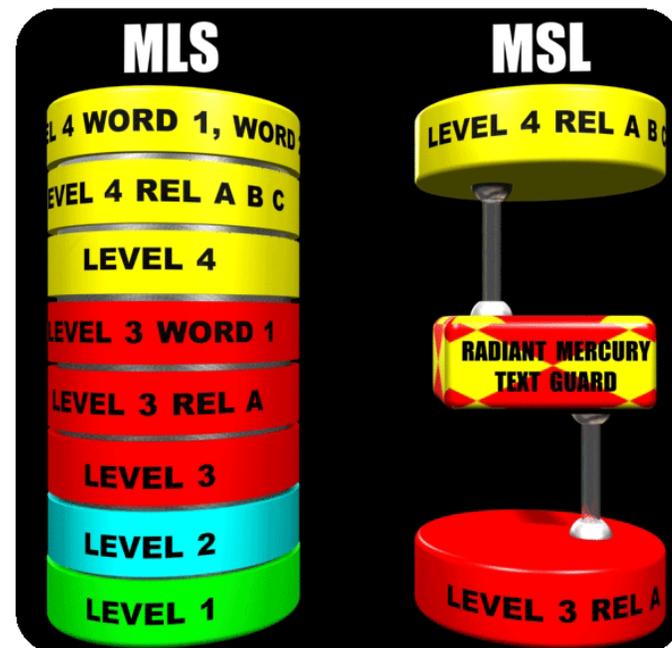
UNCLASSIFIED

■ Multiple Security Levels (MSL)

- A conglomeration of single-level workstations/servers used to provide information for analysis.
- Information is passed between the two systems utilizing security guards, which strips off valuable intelligence data from remarks lines.
- With an MLS solution such as JCDX, only a single system requires management. *MSL* environments require at a minimum, a separate system per security level.

MSL should not be confused with MLS:

Multiple Security Levels are limited to separate application displays and downgrading of information can result in loss of valuable data.



UNCLASSIFIED

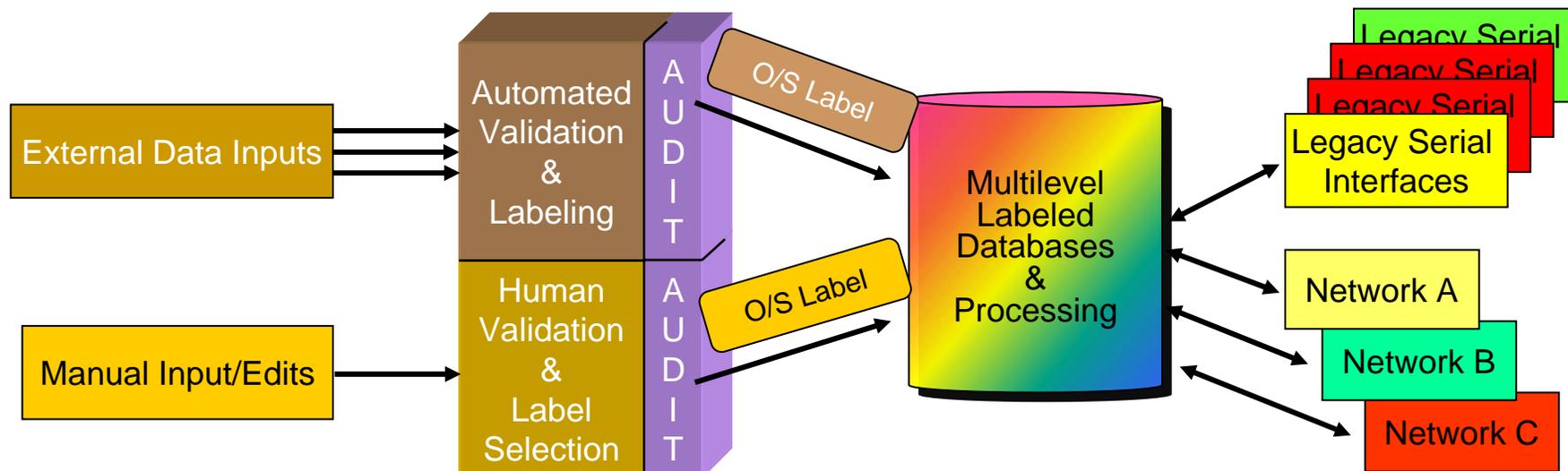


What is JCDX today?



UNCLASSIFIED

- A certified, operational, multi-level secure (MLS), PL4, all-source data management, display, fusion processing and near real-time dissemination capable system
- JCDX labels incoming data (tracks / messages / other products) from multiple sources / classification levels, manages that data (correlation, manipulation) and transmits data out to multiple sources at multiple classification levels



UNCLASSIFIED

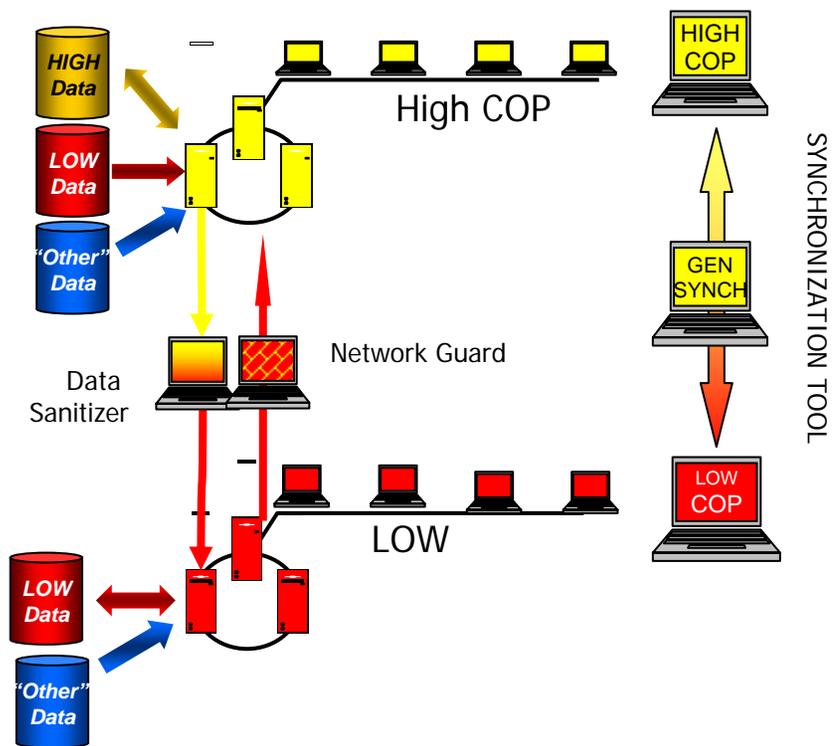


Cross Domain Solution Architectures



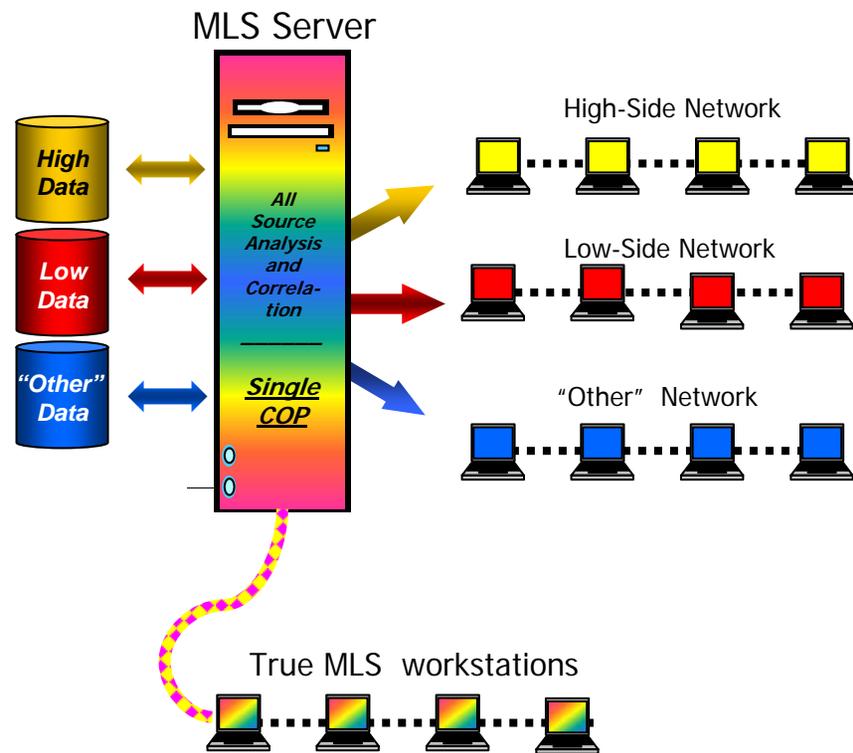
UNCLASSIFIED

Generic Architectures Today



Multiple Security Levels (MSL)

JCDX pre SOA



Multi-Level Security (MLS)

No guard; security is inherent within the system

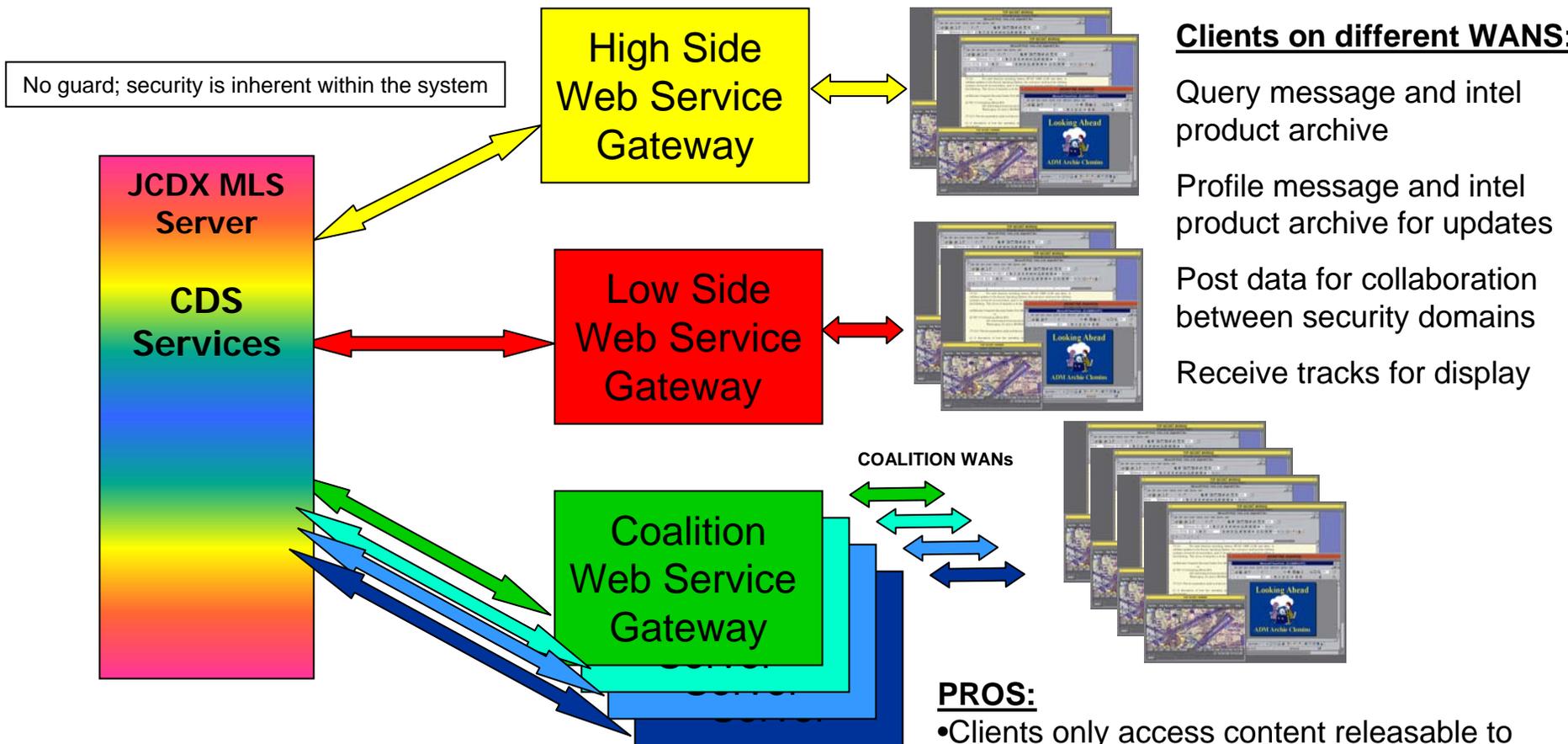
UNCLASSIFIED



JCDX Architecture with SOA Extensions



UNCLASSIFIED



Clients on different WANS:

- Query message and intel product archive
- Profile message and intel product archive for updates
- Post data for collaboration between security domains
- Receive tracks for display

PROS:

- Clients only access content releasable to their domain (Mandatory Access Control)
- Data producers only need to “Post Once” for data to be available to all applicable domains
- No unnecessary data loss from sanitizers

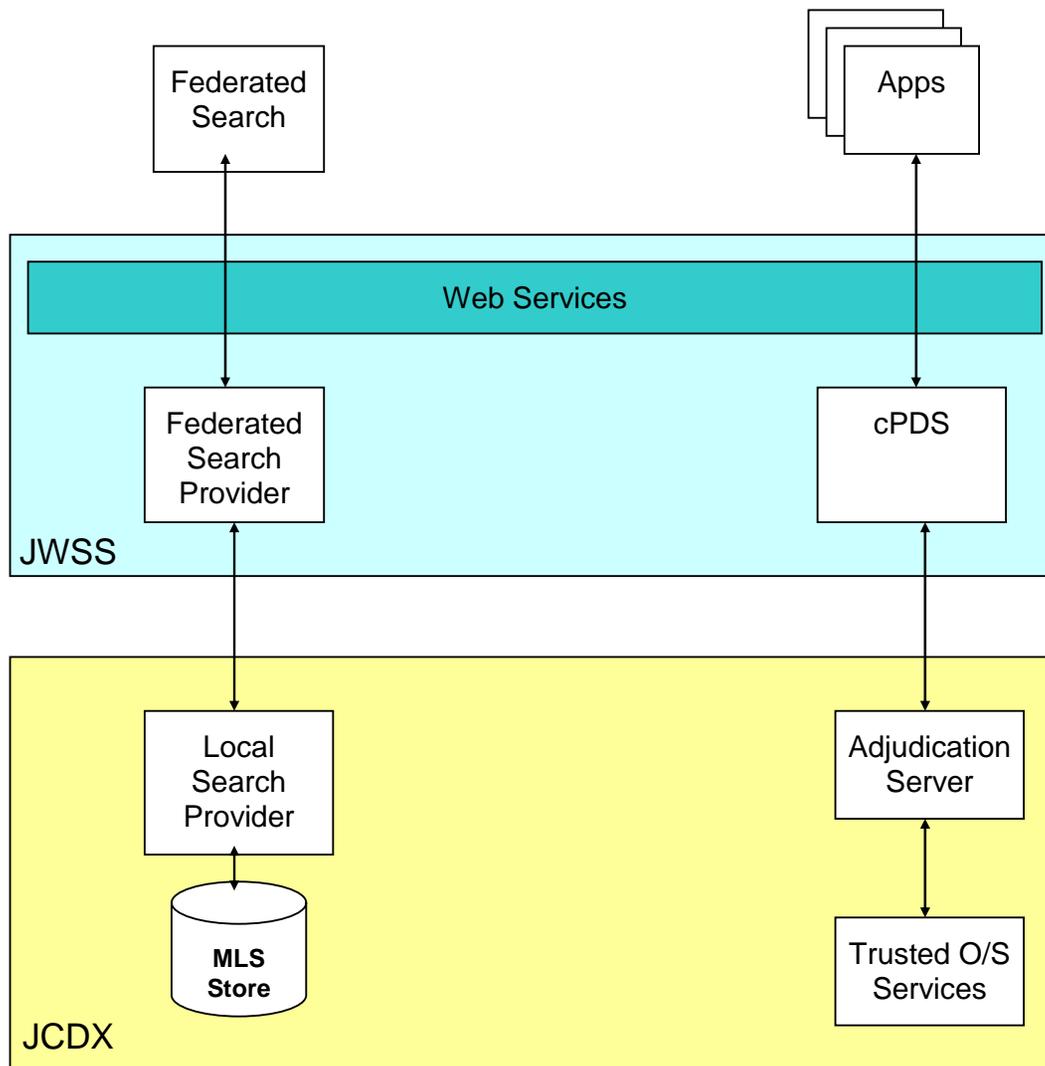
UNCLASSIFIED



SOA Architecture



UNCLASSIFIED



UNCLASSIFIED



UNCLASSIFIED

- **Classification Policy Decision Service (cPDS)**
 - provides other systems with methods for handling labeled data such as label comparison
- **Federated Search Provider**
 - allows users and applications to search multi-level data stores from single level networks and provides a “read down” capability to all lower level domains

UNCLASSIFIED

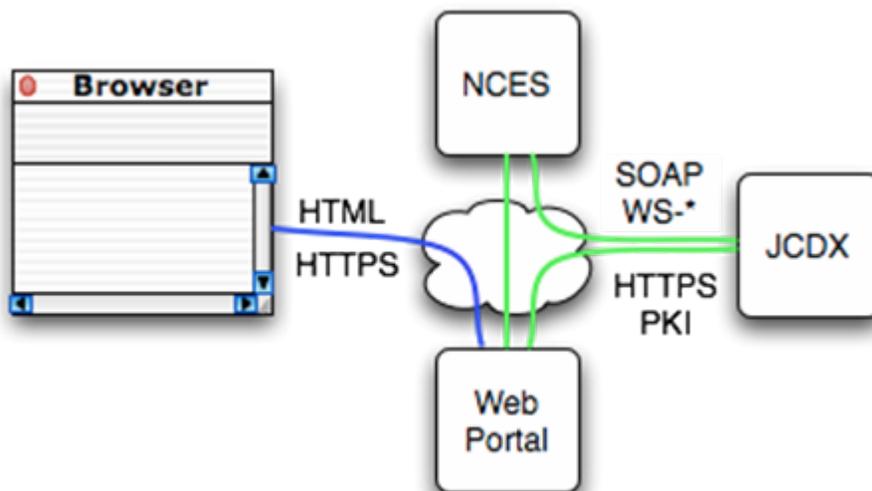


cPDS clearance based authentication



UNCLASSIFIED

- Current NCES Security Services only implements role based access control
- First attempt to authorize the user via NCES RBAC, and then attempt to authorize the user's clearance via JCDX cPDS



UNCLASSIFIED



Other cPDS methods



UNCLASSIFIED

- **isValid:** takes a classification and returns whether the classification is valid
- **getRelationship:** takes two arguments, a Subject Clearance and an Object Classification and returns the relationship. The relationship can be one of the following: Subject Strictly Dominates, Equal, Object Strictly Dominates, and Incomparable
- **getAggregateClassification:** takes a list of classifications and produces a classification that is the 'sum' of the arguments. (e.g. *getAggregateClassification* 'SECRET REL GBR' 'SECRET' 'UNCLASSIFIED' yields 'SECRET').
- **getGroupClearance:** takes a list of user clearances and produces a group clearance. This group clearance is the highest classification that can be read by all of the users in the group
- **isReleasableTo:** takes a data classification and a list of clearances and determines whether the data can be released to all of the users whose clearances were used as arguments
- **canReceive:** The *canReceive* method takes a user clearance and a list of data classifications and determines whether the user can see all of the data whose classifications were used as arguments

UNCLASSIFIED



Federated Search Provider



UNCLASSIFIED

- Allows searching of the JCDX MLS PL4 data repository through a Web Service
- Authenticates the search request via NCES and cPDS and then returns messages at the appropriate classification (including “read-down”)

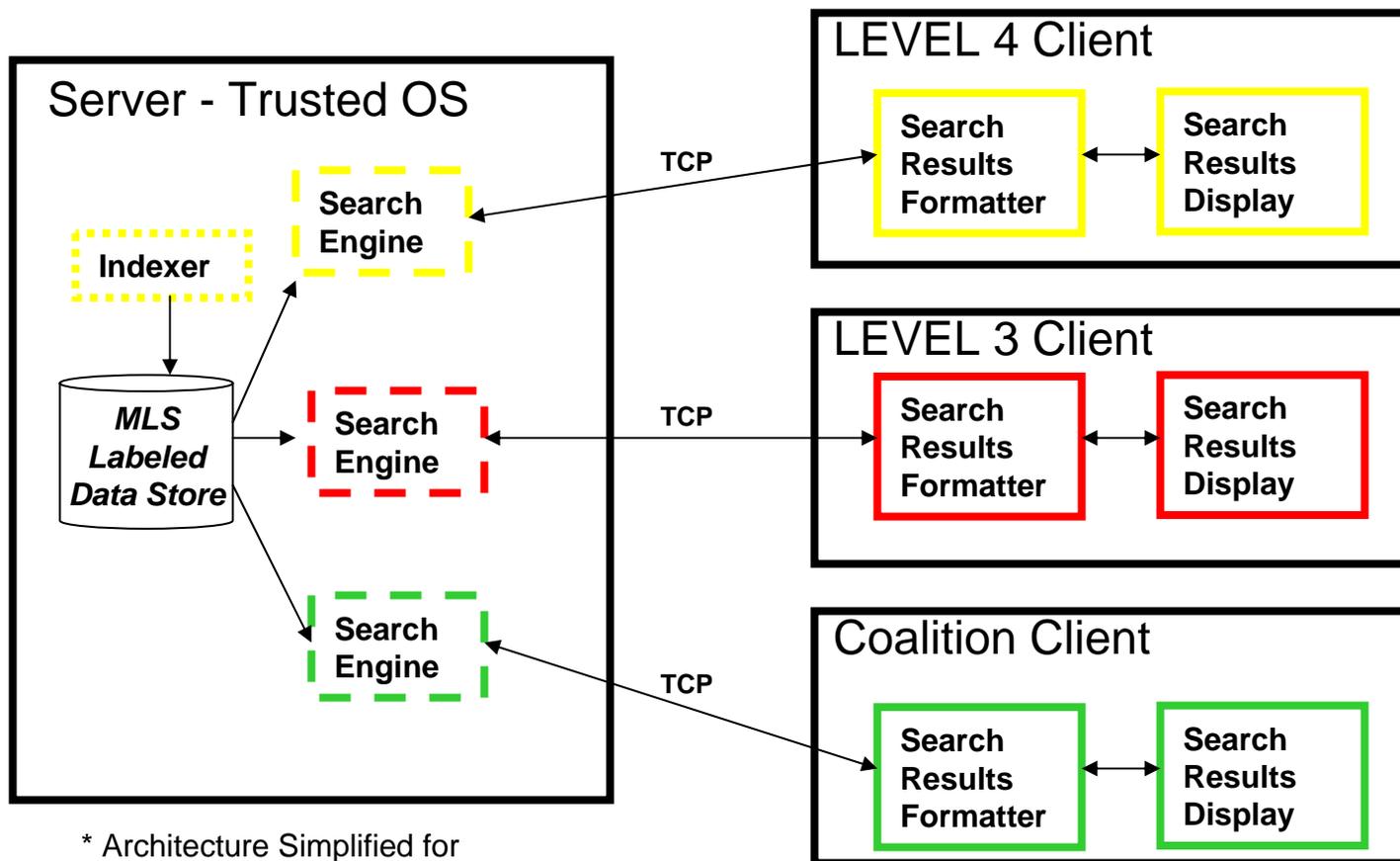
UNCLASSIFIED



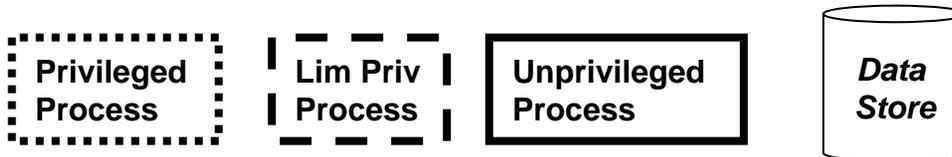
Applying JCDX Design Approach to Achieve Enterprise Wide CDS Capability



UNCLASSIFIED



* Architecture Simplified for Illustrative Purposes



UNCLASSIFIED



Other Critical Pieces (Future Work)



UNCLASSIFIED

- Trusted Editor
- Trust Service
- Labeling Service
- Accreditation / Policy Changes

UNCLASSIFIED



Trusted Editor



UNCLASSIFIED

- Content producers need a method to produce labeled content
 - Must be able to “trust” the label
- Unreasonable to expect all users to have MLS clients
 - Microsoft Windows has a very low “trust” level

UNCLASSIFIED



Trust Service



UNCLASSIFIED

- Transferring labeled data between two **systems** must involve a trusted interaction
- In non-SOA these trust relationships are statically defined
- SOA needs an automated method to determine which services on the network are trusted
- Trust service could be queried to determine the level of trust that a given service/system has

UNCLASSIFIED



Labeling Service



UNCLASSIFIED

- Must be able to transition unlabeled content in to labeled content
- Labeling service would provide an interface to allow the submission of content for labeling
 - assign a security label to the content based on a pre-defined ruleset
 - then “sign” the associated label to allow other services to verify the given label

UNCLASSIFIED



Summary



UNCLASSIFIED

- JCDX has begun to bridge the gap between traditional MLS systems and SOA and has developed an architecture that can be applied to other MLS systems
- JCDX Web Service Gateway's can be used to extend MLS capabilities to single level clients
- Extending MLS systems to a SOA enables coalition operations

UNCLASSIFIED



Points of Contact



UNCLASSIFIED

PEO C4I PMW160	CDR Wayne Slocum	619-524-7511	Wayne.slocum@navy.mil
PEO C4I PMW160 APM	Maureen Myer	619-553-9748	Penney.myer@navy.mil
PEO C4I PMW160 Chief Engineer	Robert Fish	619-553-6406	Robert.fish@navy.mil
JCDX Chief Engineer	Paul Kennedy	619-553-9541	Paul.kennedy@navy.mil
JCDX Chief Scientist	Chris J. Raney	619-553-5282	raneyc@spawar.navy.mil
PEO C4I FMS Case Manager	Steve Reddick	619-524-7274	Steven.reddick@navy.mil

UNCLASSIFIED