



**CoDS and JODI**  
**Two Operational Solutions**

**LCDR Scott D. Heller**  
**hellers@spawar.navy.mil**  
**(843) 218-5431 (W)**





**Joint Operational Data Interface**  
**(JODI)**

- **Overview**
- **Network Architecture**
- **Data Flow**
- **System Security Features**
- **Key Benefits**

01/11/2001 UNCLASSIFIED 2

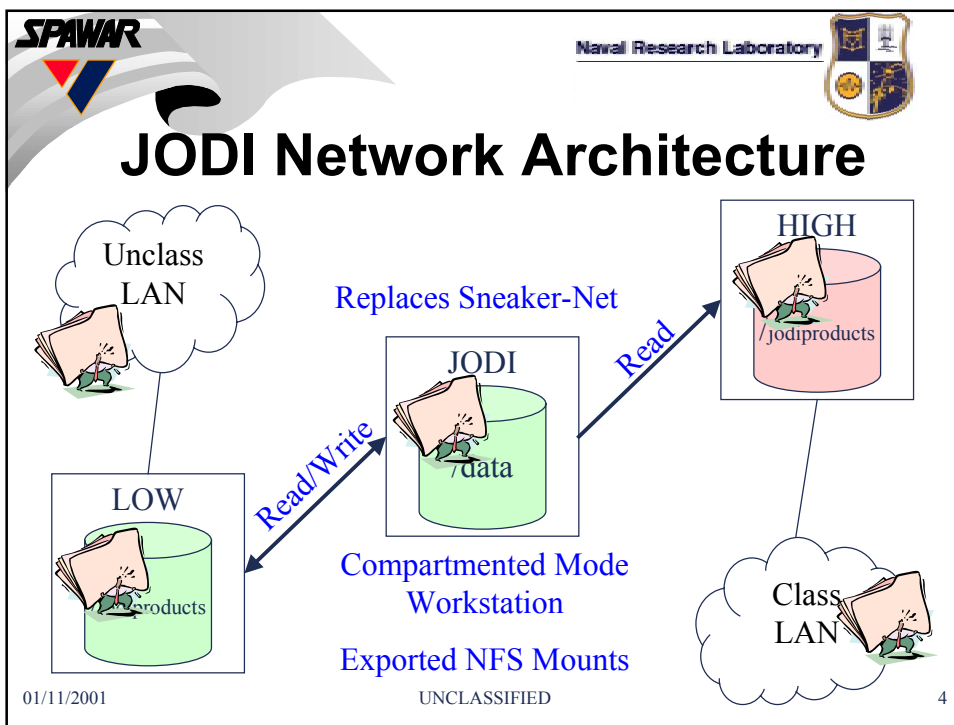
**SPAWAR** Naval Research Laboratory






## JODI Overview

- **Joint Operational Data Interface (JODI) allows one-way transfer of information from unclassified to secret systems.**
- **No “classified” data lives on JODI**
- **JODI is a low to high Guard**

01/11/2001 UNCLASSIFIED 3





## JODI Data Flow

- **Data directory is mounted (NFS) on both classified and unclassified systems.**
- **Unclassified product files are developed on the low side LAN and moved to the low side mount point.**
- **Use File Transfer Protocol (FTP) to move product to data server.**
  - FTP to Unclassified Hosts
  - Place files in /jodiproducts subdirectory
- **File is immediately available to high side server.**



01/11/2001 UNCLASSIFIED 5

## JODI System Security Features

- **HP B1+ Compartmented Mode Workstation**
  - Discretionary Access Control
  - Mandatory Access Control
  - Role-based Access Control
  - Audit Trail

01/11/2001 UNCLASSIFIED 6



**Discretionary Access Control**

- **Classic UNIX file permissions**
- **File access controls in /data directory are supported out to the mount points.**
  - NFS UID/GID synchronization
- **JODI does not have any regular user accounts.**
- **NFS Export to Highside host is read-only**



01/11/2001 UNCLASSIFIED 7



**Mandatory Access Control**

- **Data flow is based on security labels and everything is labeled.**
  - Files and directories
  - Interfaces
  - Remote hosts
- **Policy Enforced.**
  - No “Read-Up” System Security Policy
  - No “Write-Down” System Security Policy
- **Communication limited to mount points.**
  - High Mount Point
  - Low Mount Point

01/11/2001 UNCLASSIFIED 8




Naval Research Laboratory

## Role-Based Access Control

- Separation of Duties
- Many basic administration tasks do not require the “root” user.
- System Administrator
- Security Officer (ISSO)
- Network Security Officer

01/11/2001 UNCLASSIFIED 9






Naval Research Laboratory

## Audit Trail

- System Auditing
  - Best set of audit events already configured
  - All administrative actions are audited.
  - Audit trail is reviewed by Security Officer Role

01/11/2001 UNCLASSIFIED 10



**SPAWAR**  


Naval Research Laboratory 

## Key Benefits

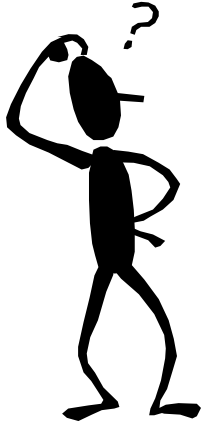
- **Timely and secure dissemination of data from Unclassified systems to Secret systems.**
- **No direct access to JODI needed to administer data.**
  - All data is administered from low side.

01/11/2001 UNCLASSIFIED 11



**SPAWAR**  

Naval Research Laboratory 

## Questions





01/11/2001 UNCLASSIFIED 12



**Coalition Data Server  
(CoDS)**


**LCDR Scott D. Heller**  
**hellers@spawar.navy.mil**  
**(843) 218-5431 (W)**



**CoDS Overview**

- **Multilevel Secure Web Server**
  - Fully integrates with existing web environment or acts as a standalone server.
  - Allows file sharing controlled by sensitivity level and/or releasability of the data.
  - Serves data files and web pages.
- **Sensitivity levels are configurable and determined by local coalition requirements.**
  - Not a one size fits all solution.
- **All reads, writes, and downgrades are auditable.**


01/11/2001 UNCLASSIFIED 14

**SPAWAR** Naval Research Laboratory 

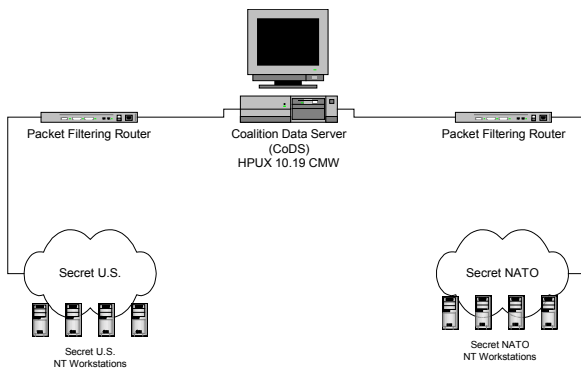
## CoDS Features

- Built on a Compartmented Mode Workstation
- Interoperable with IT-21 standards
- User access based on DoD PKI V3 X.509 certificates and client IP address
- Advisory labeling of HTML documents
- Web logging and activity report generation
- Automatic virus and “dirty word” checks on all uploaded and downgraded documents

01/11/2001 UNCLASSIFIED 15

**SPAWAR** Naval Research Laboratory 

## Example Network Architecture



The diagram illustrates a network architecture. At the top center is a computer icon labeled "Coalition Data Server (CoDS) HPUX 10.19 CMW". Below it, two "Packet Filtering Router" icons are connected to the CoDS. Each router is connected to a cloud representing a network. The left cloud is labeled "Secret U.S." and contains four computer icons labeled "Secret U.S. NT Workstations". The right cloud is labeled "Secret NATO" and contains four computer icons labeled "Secret NATO NT Workstations".

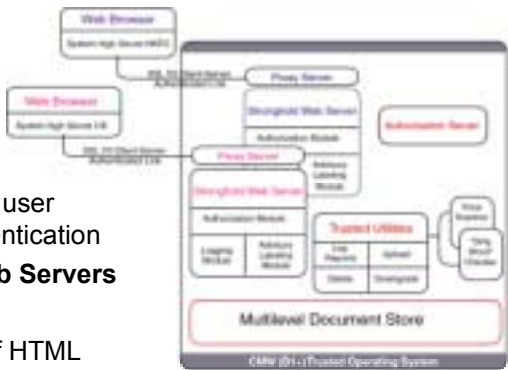
This example shows two, however the number and sensitivity level of the system high networks is configurable.

01/11/2001 UNCLASSIFIED 16

**SPAWAR** Naval Research Laboratory

## Functional Architecture

- **Foundation**
  - Trusted CMW
  - Mandatory Access Controls (MAC)
  - 128 bit SSL
  - Class 3 Certificates for user identification and authentication
- **Multiple Single Level Web Servers**
- **Custom CGI scripts**
  - Real-time Rendering of HTML
  - Content and Function determined by user privileges



The diagram illustrates the functional architecture of the system. It shows a 'Web Browser' (Secure High-Security CMW) connecting to a 'Proxy Server' (Secure High-Security CMW). The Proxy Server connects to a 'Single Level Web Server' (Secure High-Security CMW) and a 'Trusted Utilities' component. The Single Level Web Server connects to a 'Multilevel Document Store' (CMW (B1+) Trusted Operating System). The Trusted Utilities component includes 'File Access', 'User', 'Storage', and 'Management' modules. The Single Level Web Server also includes 'Authentication Module', 'Authorization Module', and 'Content Management' modules. The Multilevel Document Store includes 'File Access', 'User', 'Storage', and 'Management' modules.

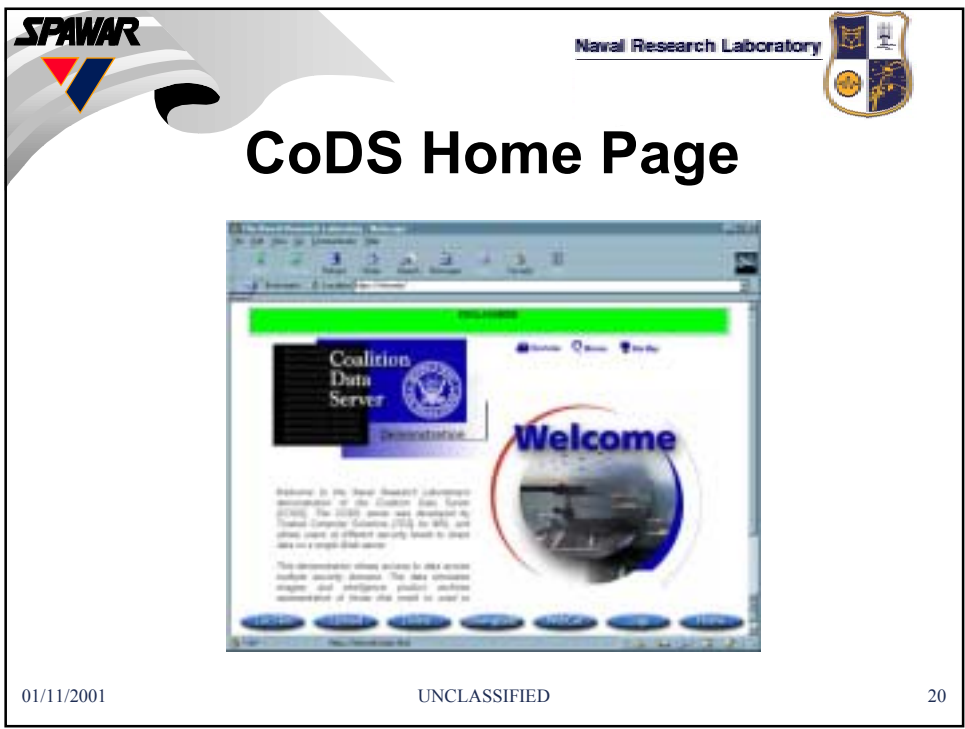
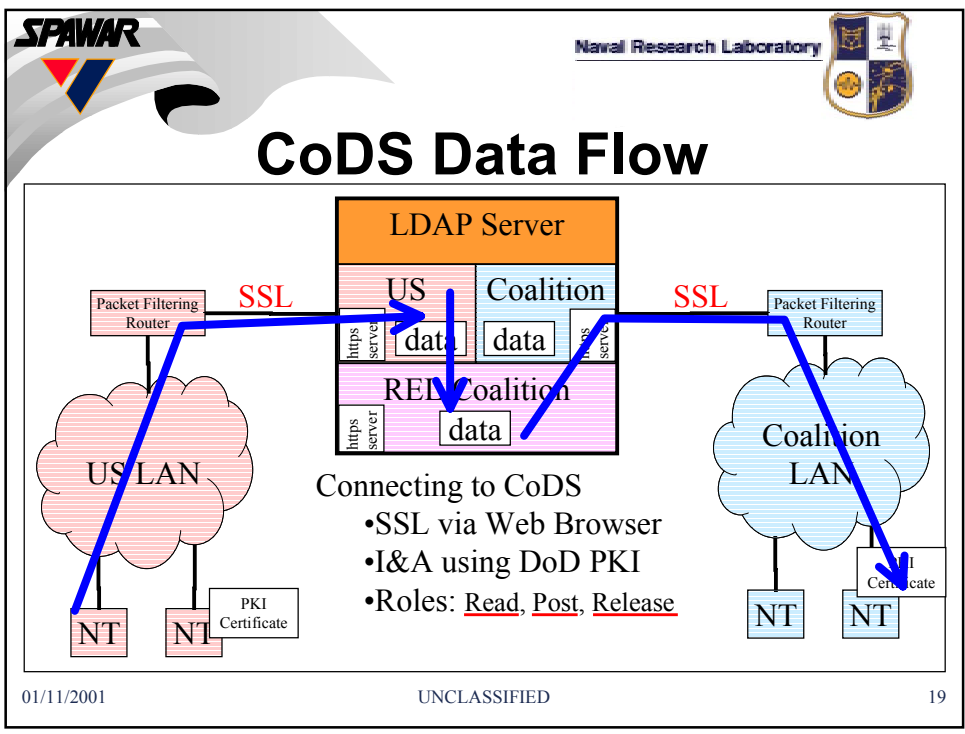
01/11/2001 UNCLASSIFIED 17

**SPAWAR** Naval Research Laboratory

## End User Privileges

- **Read**
  - Access information at or below their sensitivity level.
    - US Secret user can read US Secret Releasable UK/CAN/AUS/NATO/etc...
    - UK Reader may not read US Secret data, only releasable data
- **Post**
  - Write data at the user's sensitivity level.
- **Release**
  - Downgrade data files to a dominated sensitivity level (e.g. Secret US moved to Releasable NATO)


01/11/2001 UNCLASSIFIED 18





**SPAWAR** Naval Research Laboratory

## Deletion Interface File List



CoDS Server File Delete Form


SECRET 00

File Type	Sensitivity Level	Actions	Delete
SECRET 00	SECRET 00	SECRET 00	<input type="checkbox"/>
SECRET 00	SECRET 00	SECRET 00	<input type="checkbox"/>
SECRET 00	SECRET 00	SECRET 00	<input type="checkbox"/>
SECRET 00	SECRET 00	SECRET 00	<input type="checkbox"/>

01/11/2001 UNCLASSIFIED 23

**SPAWAR** Naval Research Laboratory

## Deletion Interface Top Level



CoDS Server File Delete

Select Sensitivity Level Folder

SECRET 00

SECRET 00/SECRET 00

01/11/2001 UNCLASSIFIED 24

**SPAWAR** Naval Research Laboratory



## Audit Review

### Log Report Parameters

Select a date range for the report:

Start Date:	Year: 1999	Month: Aug	Day: 24	Hour: 14	Min: 23
End Date:	Year: 1999	Month: Aug	Day: 25	Hour: 23	Min: 59

Select a severity level range:

Minimum:  UNCLASSIFIED Select the minimum and maximum severity level for the logged severity of message.

Maximum:  UNCLASSIFIED


Select a message level range:

Minimum:  INFO Select the minimum and maximum message level to include in the report. INFO, DEBUG represents the minimum amount of information. DEBUG the maximum.

Maximum:  SEC\_ALERT


01/11/2001 UNCLASSIFIED 25

**SPAWAR** Naval Research Laboratory






## System Footprint

- **Physical Elements**
  - HP 712 Workstation
    - Desktop Workstation
    - Monitor, Keyboard, & Mouse
    - 20" H x 17" W x 36" D
  - Packet Filtering Router
    - Depends on site survey




01/11/2001 UNCLASSIFIED 26

**SPAWAR**  



Naval Research Laboratory 


## System Footprint - 2

- **Connections**
  - Category 5 Ethernet
  - One network interface for each system high network
- **Server Location**
  - Secret US Space



01/11/2001 UNCLASSIFIED 27



**SPAWAR**  

Naval Research Laboratory 

## Platform Impacts

- **Training**
  - Users (Existing Role)
    - Use and care of DoD PKI certificates
    - Use of a web browser
  - Information Manager (Existing Role)
    - Use and care of DoD PKI certificates
    - Understanding Command Releasability Policy
  - ISSO
    - CoDS Admin
    - Certificate Management



01/11/2001 UNCLASSIFIED 28

## Platform Impacts - 2

- **Security Requirements**
  - End users: No additional requirements.
    - Readers
    - Posters
    - Releasers (Info. Managers)
  - System Administrator and ISSO
    - Must be cleared for each compartment served.
    - (i.e. Secret US and Secret NATO)

01/11/2001 UNCLASSIFIED 29

## Conclusions

- **Elegant Functional Design**
  - Minimum Manpower Impact
  - Web Server Functionality
  - Your data shared securely with coalition partners via a web interface.
- **Minimal Physical Impact**
  - Integrates with existing infrastructure.
- **Limited Training Requirements**
  - ISSO/Web Master
  - Care and Handling of DoD PKI Certificates



01/11/2001 UNCLASSIFIED 30

## POC List

- **Basit Syed, SPAWAR PMW-161**
  - CoDS Program Office
  - syed@spawar.navy.mil
  - (619) 524-7504
- **Eather Chapman, NRL**
  - CoDS Development
  - chapman@itd.nrl.navy.mil
  - (404) 202-7311
- **LCDR Scott D. Heller, SPAWARSYSCEN-CH**
  - Certification and Install Coordination
  - hellers@spawar.navy.mil
  - (843) 218-5431

01/11/2001 UNCLASSIFIED 31

## Background Slides

**SPAWAR** Naval Research Laboratory

## Example Data Flow - Reading

In this example a user with read rights on the Secret US System High Network may read Secret US data and Secret REL Coalition data. Like wise a Secret NATO user may read Secret NATO data and Secret REL Coalition data.


01/11/2001 UNCLASSIFIED 33

**SPAWAR** Naval Research Laboratory


## Example Data Flow - Posting

In this example a user with Post rights on the Secret US System High Network may write Secret US data. Like wise a Secret NATO user may write Secret NATO data. A user with Post rights may not write to the Secret REL Coalition compartment as this would be a downgrade.

01/11/2001 UNCLASSIFIED 34


**SPAWAR** Naval Research Laboratory 

## Example Data Flow - Downgrade



**SECRET  
U.S.**

CoDS	
SECRET U.S.	SECRET NATO
↓	↓
SECRET REL Coalition	



**SECRET  
NATO**

In this example a user with Release rights on the Secret US System High Network may move Secret US data to the Secret REL Coalition compartment. Likewise a Secret NATO user may write Secret NATO data to the Secret REL Coalition Compartment. This allows readers from both networks to view the releasable files.

01/11/2001 UNCLASSIFIED 35