



JEDI Program Management Office
(AFRL, Rome NY)
COM: (315) 330-7657
DSN: 587-7657
E-Mail: jedi@rl.af.mil

AFRL Consolidated Help Desk
COM: (315) 330-IDHS (4347)
DSN: 587-IDHS (4347)

Northrop Grumman IT Help Desk
COM: (402) 682-4338

Joint Enterprise DoDIIS Infrastructure (JEDI) Whitepaper

23 August 2004

"Secure Infrastructure Management for the Enterprise"

Air Force Research Laboratory (AFRL) Rome Research Site
Information and Intelligence Exploitation Branch (IFEB)
525 Brooks Road
Rome, NY 13441-4114



TABLE OF CONTENTS

1	EXECUTIVE SUMMARY	3
2	TECHNICAL OVERVIEW	4
3	COORDINATION/SPONSOR	12
4	CONCEPT OF USE	13
5	JUSTIFICATION/REQUIREMENTS	17
6	INTEROPERABILITY/INTEGRATION	19
7	ASSESSMENT METHODOLOGY	19

1 Executive Summary

JEDI provides a Sensitive Compartmented Information (SCI) certifiable, Common Operating Environment (COE) interoperable, heterogeneous Operating System (OS) architecture using Solaris and Windows platforms. JEDI enables the transition from the legacy Department of Defense Intelligence Information System (DoDIIS) Client Server Environment - System Services (CSE-SS) SCI Intelligence Infrastructure to a pure COTS-based, SCI-certifiable infrastructure, which was mandated by the Common Operational Picture (COP), Joint Vision 2010 (JV 2010), Joint Planning Doctrine (JPD) Series 2.xx, Intelligence Support to Joint Operations, JPD 6.0, and Command Control Communication and Computers (C4) Systems Support to Joint Operations.



Figure 1 – JEDI Toolset

JEDI offers compliant tools and utilities for Command and Control (C2) systems that support both C2 and intelligence software applications on their respective workstations, servers, and networks. The ability to install software applications on C2 intelligence workstations and servers decreases the hardware footprint within DoDIIS intelligence sites. JEDI also offers Defense Intelligence Agency (DIA) and National Security Agency approved computer system security services for both C2 and intelligence systems. This allows not only intelligence, but also Global Combat Support System and Tactical Battle Management Core System (GCSS/TBMCS) based applications and non-GCSS/TBMCS based applications to utilize the same network infrastructure and security services.

JEDI provides automated system and network management, while providing secure data access to both DoDIIS and COE compliant Intelligence Mission Applications (IMAs). Access is achieved through a heterogeneous, browser based, site-configurable network infrastructure. JEDI allows network-wide system administration and location-independent unitary logon through the use of Public Key Encryption (PKI) for Solaris and Windows workstations. The installation of JEDI can be automated and is highly customizable, allowing individual components to be installed or uninstalled. Any duplicate functionality with other commercial-off-the-shelf (COTS) software is thus avoided entirely. Today, JEDI and its predecessor, CSE-SS, provide support to over 20,000 workstations and servers installed at over 200 sites including all of the Unified Commands and Numbered Air Forces.

2 Technical Overview

The JEDI software can be broken down into three major components: Security Management, Network Management, and Segmented Application Support. JEDI supports intelligence and operational personnel by providing the following capabilities and benefits:

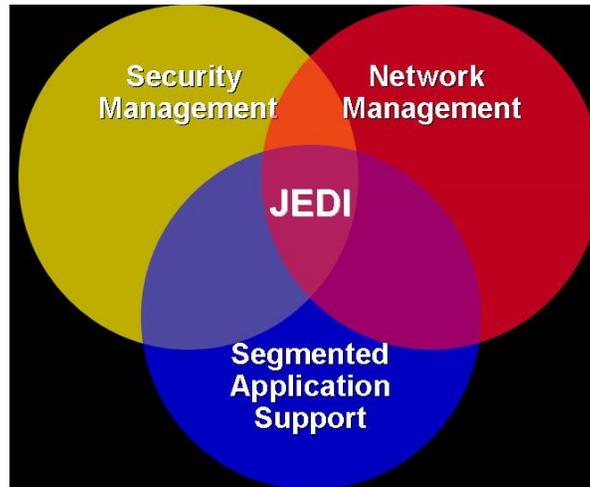


Figure 2 – JEDI Components

2.1 Example JEDI Security Services

- ✓ Provides a robust role-based access environment for delegating system administration and security management roles and responsibilities.
 - Divides administrative (root) tasks among configurable roles
 - Roles can only access assigned administrative tasks
 - Trusted user activities are audited and traceable per individual

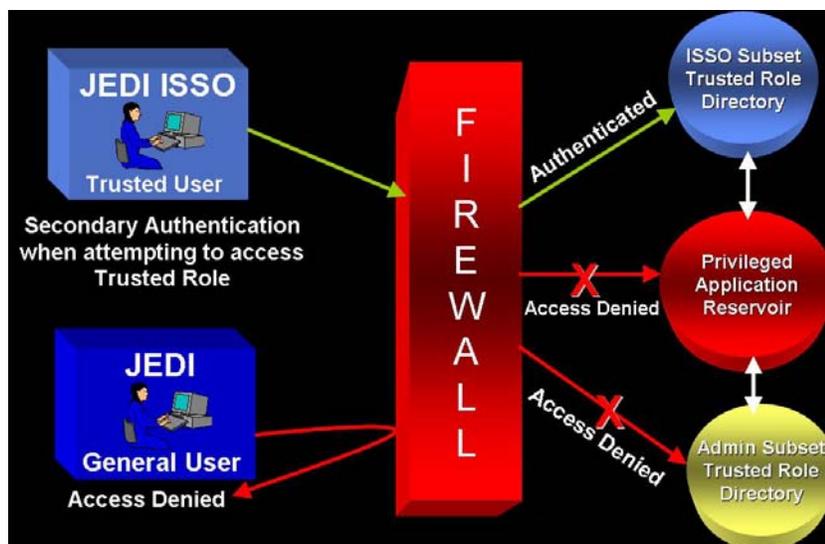


Figure 3 – JEDI Role Based Access Control

- ✓ Allows sites to maintain or acquire Director of Central Intelligence Directive 6/3 (DCID 6/3), Protection Level 2, System High accreditation
- ✓ Performs post-install security lock down of the OS (and COE)
- ✓ Provides Secure Login Management
- ✓ Provides a network-wide “3 strikes and you’re out”
- ✓ Configures per user audit mask
- ✓ Provide a “Deadman” Timeout
- ✓ Enforces strong passwords: 8 characters, no repeating characters, mixed case, no part of username, no part of GECOS field, no dictionary words (including mixed case), can’t be hostname, can’t be domain name, no reverse username, no reverse hostname, can’t be last 2 passwords, checks on character shifting...
- ✓ Provides password aging
- ✓ Allows device (CDROM, floppy, etc) allocation and de-allocation per user
- ✓ Configures TCP Wrappers



Figure 4 – TCP Wrapper Configuration



Figure 5 – JEDI Login Screen

- ✓ GOTS XDM has been removed in v1.3
 - Replaced with Solaris dtlogin
 - Five modules included in JEDI V1.3 that provide DoDIIS required security
 - is_pam_network_lockout
 - is_pam_password_aging
 - is_pam_password_rules
 - is_pam_accept_decline
 - is_pam_no_root_login

- All modules are stacked by default in the pam.conf file
- ✓ Offers automated labeling and marking of printed output with appropriate and configurable classification levels



Figure 6 – JEDI Print Utility

- ✓ Provides various screen security bannering options

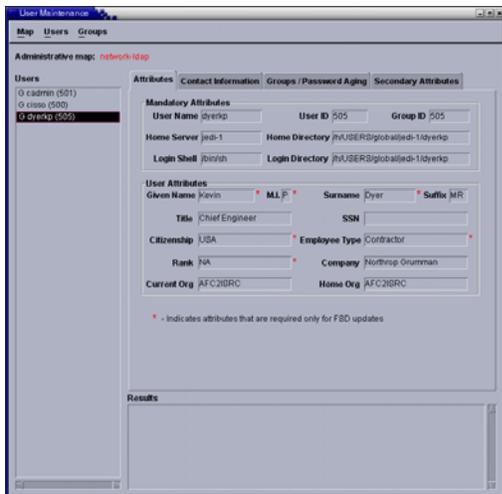


Figure 7 – JEDI User Maintenance



Figure 8 – New User Wizard

- ✓ Centralizes control of network security scans as well as log and audit collection via CLASS or PRÉCis.

- PRÉCis is a distributed application that automates all aspects of processing audits on your network. It provides cradle-to-grave support for managing audit information, simplifying your day-to-day operations, yet providing the safeguards you need.
- PRÉCis' real power lies in its ability to digest, analyze, and store large volumes of audits from various sources and give you concise summaries.
- Near real-time security alerts are triggered by definable user actions

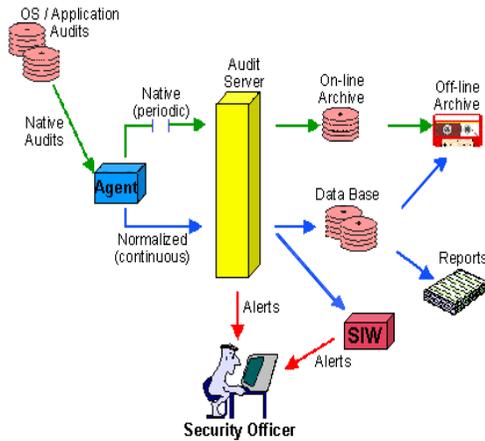


Figure 9 – PRÉCis Concept of Operations

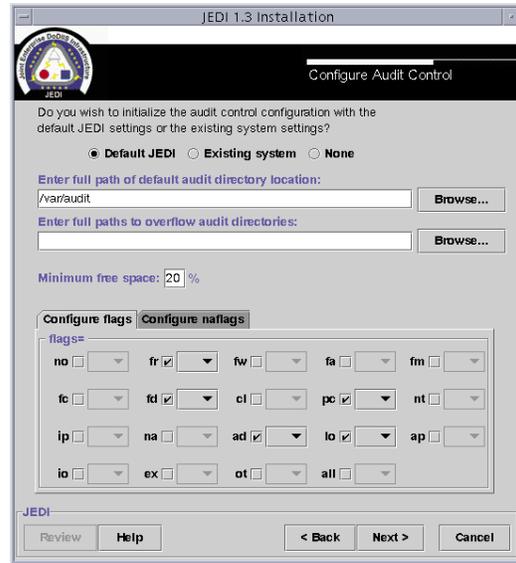


Figure 10 – Audit Control Configuration

- ✓ JEDI provides a transparent tracking and auditing system for C2 and intelligence community administrators, while users access applications, allowing them to meet today's security requirements.

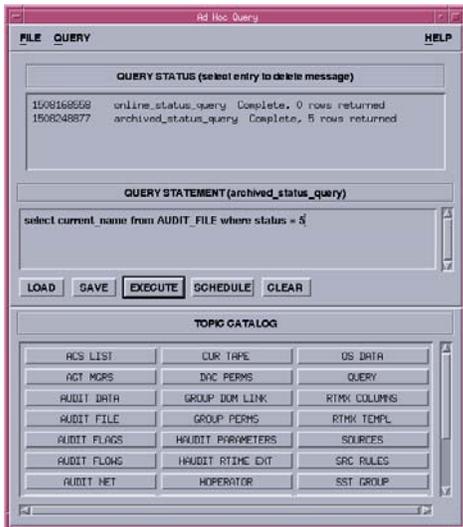


Figure 11 – Précis Ad Hoc Query Tool

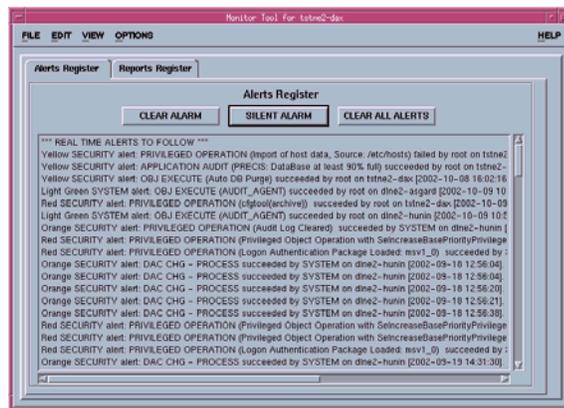


Figure 12 – Précis Monitor Console

2.2 Example Network Management Tools

- ✓ Provides seamless transition from existing CSE-SS systems to JEDI
- ✓ Provides a cost effective means of achieving COE interoperability
- ✓ Ensures high operational availability during migration of non-CSE-SS or non-JEDI infrastructure to JEDI
- ✓ Provides network monitoring and reporting tools
- ✓ Provides new technologies to the user, including web-based interfaces, jumpstart and automated installs, enhanced audit reduction and analysis, better security, and tighter Windows integration
- ✓ Provides extensive documentation and security templates (SSAA, SRTM, TFM)
- ✓ Supports the DoDIIS Full Service Directory (FSD) out-of-the-box

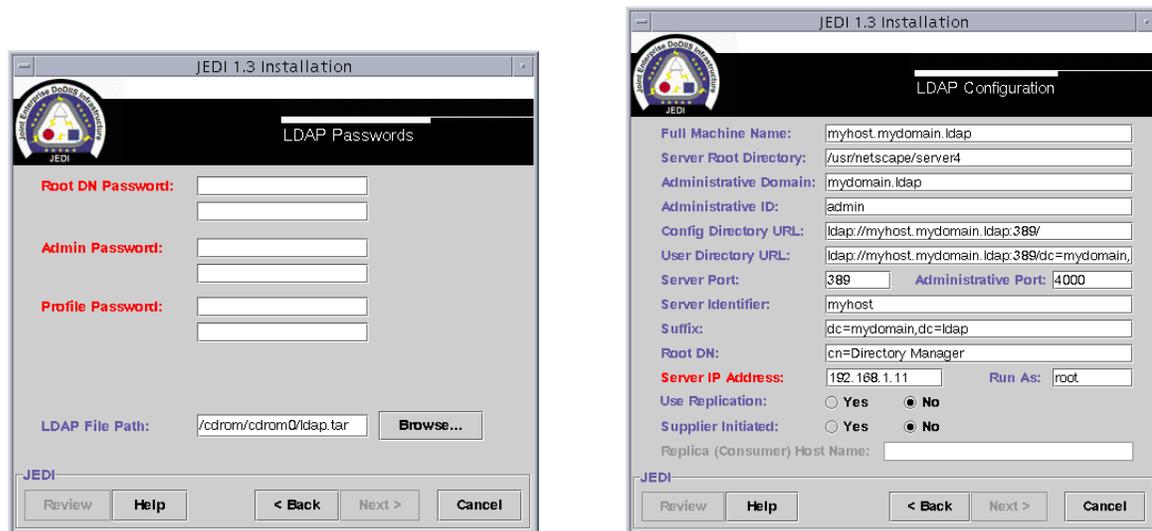


Figure 13 – JEDI LDAP Interfaces

- ✓ Supports all naming services: NIS, NIS+, LDAP, Active Directory
- ✓ Provides straightforward and powerful GUI system utilities and wizards for administrators
- ✓ Simplifies name service administration
 - NIS
 - NIS+
 - LDAP
 - /etc/files
- ✓ Simplifies user & group administration

- ✓ Simplifies host administration
- ✓ Monitors network health
- ✓ Provides automated mail configuration



Figure 14 – Mail Configuration

- ✓ Provides process management tools
- ✓ Privilege & Session Maintenance
- ✓ Remote Distribution
- ✓ Archive Management
- ✓ Alert News Utility

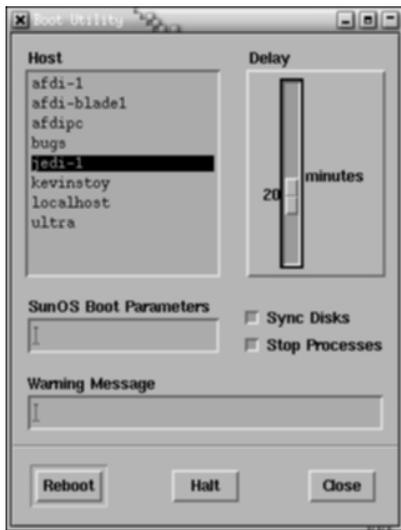


Figure 15 – JEDI Boot Utility

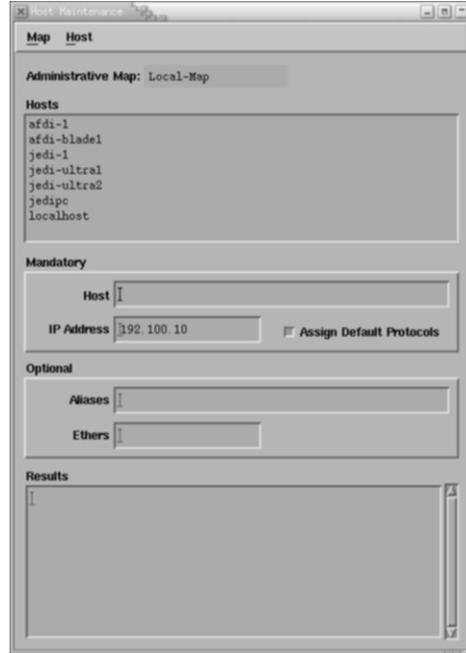


Figure 16 – JEDI Host Maintenance

- ✓ User Maintenance

- ✓ Boot Utility
- ✓ Disk Space
- ✓ User Account Information
- ✓ Printer Management



Figure 17 – Printer Configuration



Figure 18 – Segmented and non-segmented commercial applications can co-exist

2.3 Segmented Application Support Framework

- ✓ Allows non-segmented DoDIIS applications to co-exist and interoperate with segmented COE applications
 - It's optional
 - Must determine if needed at install time
 - The SASF consists of three major components
 - COE Installer
 - Common Data Store
 - APM framework
 - It can run all applications segmented for Solaris 8 and COE 4.x
 - Provides a transition path to the next generation of the “COE”
 - A full COE load is not required
 - JEDI can still run commercial unsegmented applications



Figure 19 – Optional COE

3 Coordination/Sponsor

Executive Agent	AFC2ISRC/INYI
DExA	jedi@rl.af.mil
Functional Manager	jedi@rl.af.mil
Engineering	jedi@rl.af.mil
Program Management	AFRL/IFEB – Joint Enterprise DoDIIS Infrastructure Program Management Office (PMO)
Program Manager	jedi@rl.af.mil
Deputy Program Manager	jedi@rl.af.mil

Table 1 – Points of Contact

4 Concept of Use

a. Concept of Operation, Employment, and Proposed Force Structure

Figure 20 shows the building blocks of the JEDI program. The build starts with the basic operating system software (Solaris or Windows), latest patch cluster, and then the installation of JEDI. The COE component can optionally be added at this time. Each layer adds more to the previous layer beneath it by adding desired features and functions to make the system a fully operational SCI-certifiable system that can optionally support COE segmented applications.

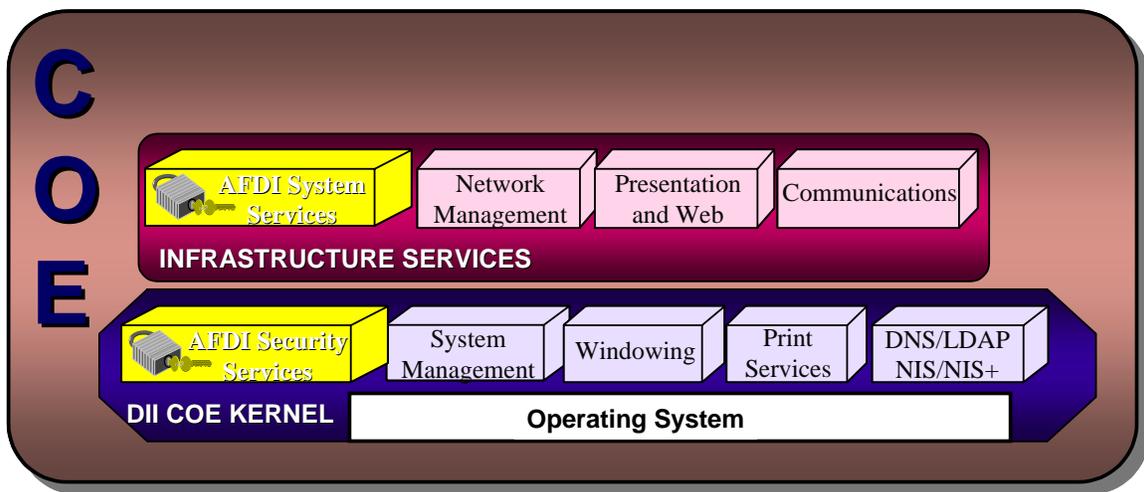


Figure 20 - JEDI System Services

It is important to note that starting with JEDI 1.3; the COE is no longer a required component. Instead, JEDI can provide the framework required to execute existing COE-based applications if required. As these services are adopted in future releases of GIG-ES (formally NCES) or supplemented by COTS applications, those same services and functions can be turned off in JEDI, if desired.

b. Technical/System Concept/Architecture Summary

Figure 21 depicts the JEDI integrated infrastructure. The JEDI segments are combined in the “Infrastructure Services” layer and “COE Kernel” layer. This is where JEDI provides its functionality. Of the services JEDI adds to the COE, the most important are the Security Services. Security Services enable system tracking and auditing, resource monitoring and administration, and file permission administration. In the “Common Support Applications” layer, which forms the top level of COE Infrastructure, COTS and government-off-the-shelf third-party applications reside. JEDI provides access to system resources by placing each user

into a profile granting specific rights and privileges. The profiles are configurable per user, per resource, and per system, thus allowing the system administrator complete control by granting access to specific resources as necessary. The system is capable of tracking and auditing multiple features, tying the audit trail to a particular user, resource, file, and/or system.

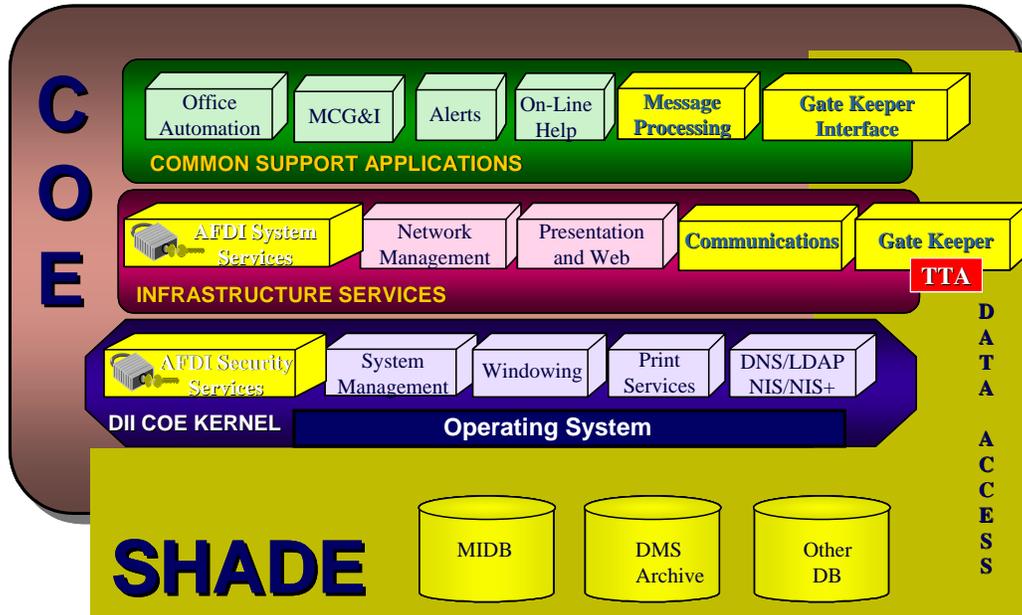


Figure 21 - Integrated JEDI/COE Infrastructure

Figure 22 reflects an enterprise perspective and the interrelationships within the DoDIIS Community needed to manage, develop, test, train, field, and sustain an infrastructure and the IMAs needed to satisfy mission requirements. The term “Intelligence Mission Application” or “IMA” is used here to emphasize the need to use a community-centric versus systems-centric approach when delivering software capabilities to the field. The community-centric approach to acquiring information technology capabilities permits individual DoDIIS sites to acquire, integrate, install, and maintain an infrastructure that meets their specific mission requirements.

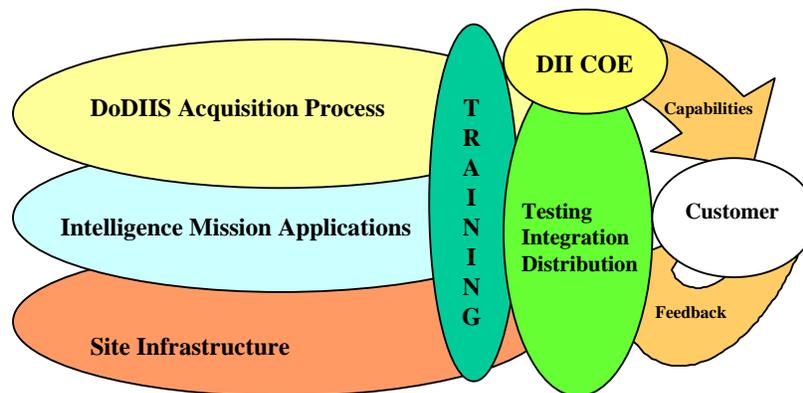


Figure 22 - DoDIIS Enterprise

The transition to a community-centric approach is also consistent with the DoDIIS Management Board (DMB) decision to implement an accreditable infrastructure that supports integration of COE-based segments throughout the DoDIIS Community, using an enterprise approach to achieving the highest levels of compliance.

The current development/fielding plan for JEDI is shown in Table 2.

AFDI/JEDI	COE	OS	Release Date
1.1	4.2P1	Solaris 7, Windows NT	May 01
1.1	4.4	Solaris 8	Nov 01
1.1	4.5	Windows NT	Feb 02
1.2	4.5	Solaris 8	June 02
1.2	N/A	Windows 2000	Oct 02
1.3	Opt 4.7	Solaris 8	Oct 03
DTW 3.1	N/A	Trusted Solaris 8	July 04
2.0	N/A	W2K/Win XP/W2K3	Aug 04
JMDI 1.0	N/A	Trusted Solaris 8	TBD
2.0	N/A	Solaris 10	TBD

Table 2 – Current JEDI Releases

JEDI supports the COE releases as they become available. As the COE/NCES develops versions that support the latest operating systems, such as Solaris 10 and Windows 2003, JEDI releases compatible segments. Functionality is built in with requirements prioritized by the user community. Table 3 lists future functionality requirements needed to maintain network integrity while incorporating the latest advances in information assurance technology.

	FY00	FY01	FY02	FY03	FY04
<u>AFDI 1.0</u>	• Conversion of CSE-SS to JEDI				
	• Integration of NT 4.0 SP 4				
	• BETA Release for user input				
	• DII COE version 4.1				
<u>AFDI 1.1</u>		• Upgrade to DII COE 4.2 Patch 1 (for Solaris 7)			
		• Upgrade to DII COE 4.4 (for Solaris 8)			
		• Upgrade NT to SP 6 with servers and clients			
		• Upgrade to Perl 5.0			
		• TCL/TK Upgrade			
		• Xlock more integration and enhancements			
		• Upgraded alert support			
		• Increased logging support			
		• Automatic password expiration			
		• Unattended NT installs			
		• Solaris jumpstart installs			
		• SPI integration for NT			
		• Limiting access to devices			
		• "su" utility on NT 4.0			
		• Network wide lockouts			
		• Password upgrades			
		• Integrated secure RPC			
<u>AFDI 1.2</u>			• Upgrade to DII COE 4.5		
			• Integrate Windows 2000 clients and servers		
			• Integrate Web Interface		
			• Increased dead man functions		
			• Creation of default profiles		
<u>JEDI 1.3</u>				• Improved Point & Click installation GUI	
				• COE is now OPTIONAL	
				• Enforces "3 Strikes" rule for remote logins	
				• Integration of Précis Audit Reduction and Normalization	
				• Provide full LDAP support	
				• Support pluggable authentication modules	
				• New User Wizards	
				• Removal of GOTS XDM code, replaced with Solaris dtlogin	
				• Integrated DoDIIS Full Service Directory Support	
				• Security Bannering	
				• Improved Modularized Jumpstart scripts	
<u>JEDI 2.0</u>					• Port to Solaris 10/TSol 8/Windows XP/Server 2003
					• Solaris Management Console Based via Snap-ins
					• Removal of JEDI specific maps
					• Solaris FLASH archive support
					• Utilizes Native Solaris RBAC
					• Significant reduction of GOTS footprint

Table 3 – JEDI Roadmap

5 Justification/Requirements

JEDI is a joint program sponsored by DIA. The AFC2ISRC is the JEDI functional manager. DIA is the JEDI Milestone Decision Authority (MDA). The Air Force Research Laboratory (AFRL) serves as the Program Management Office (PMO) for implementation of the JEDI requirements. The AFC2ISRC wrote the JEDI Requirements Document for the AF/XOI as the executor, at the direction of Unified Commands, Services, and Agencies. As a DIA directed program, the JEDI Requirements Document is written in accordance with Chairman, Joint Chiefs of Staff Instruction 3170.01A, Requirements Generation System, 10 August 2000.

In August 2000, the Chairman of the DMB directed a transition from the CSE-SS to the COE. AFDI (at that time) was voted on and approved in a unanimous decision by the DMB voting members as the mandated migration from CSE-SS to DII COE on 2 August 2000.

Implementation of JEDI contains a clear migration path from the former DoDIIS infrastructure to a COTS-based infrastructure that can still support segmented COE applications. Currently, migratory paths and associated funding include segmentation of both the data and the application of the data. Implementing JEDI in this fashion precludes the need to focus scarce future resources on both the data and the application by allowing the concentration of those same resources exclusively on the application or presentation of the data.

Mission Need

JEDI responds to areas of the DCID 6/3, to ensure Information Assurance for Intelligence Systems processing SCI data at Protection Level 2, High Integrity, High Availability. JEDI provides information integrity and availability by satisfying security and functional requirements needed to ensure information assurance.

JV 2020 states (pg. 3):

The overarching focus of this vision is full spectrum dominance—achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection. Attaining that goal requires the steady infusion of new technology and modernization and replacement of equipment. However, material superiority alone is not sufficient. Of greater importance is the development of doctrine, organizations, training and education, leaders and people that effectively take advantage of the technology.

It goes on to state that these elements will be influenced primarily by two factors: Unfolding information technologies and the military's innovative application of them.

Current underlying infrastructures are a collection of unique, non-interoperable systems operating in organizational environments capable of exchanging data only slowly and clumsily. Such systems are widely known as “stovepipe” systems. A stovepipe environment functioned

adequately during the relatively static Cold War, but later showed severe drawbacks, even during the straightforward, long lead-time scenarios of Desert Storm. In today's dynamic war fighting environment, however, stovepipe systems are clearly unacceptable. Thus, Joint Chiefs of Staff (JCS) has directed the equipment, architectural, and cultural difficulties be resolved immediately. Integration at all levels, from national to war fighter, strategic, operational, tactical, and among allies and coalition partners, are the baseline expectations.

JEDI addresses the JCS directive, providing the DoD community the capability to create an information infrastructure that is seamless, collaborative, knowledgeable, focused, decisive, correct, and fast. JEDI provides a comprehensive system-to-systems-related program, allowing end-to-end enterprise infrastructure management, composed of a suite of automated infrastructure and security services. The underlying goals of the JEDI program are information assurance and information superiority in an interoperable, integrated environment.

Overall Mission Area

JEDI addresses key JV 2020 areas of Joint Operations: Information Superiority, Information Environment and Innovation, Interoperability, Dominant Maneuver, Precision Engagement Information Operations, and Joint C2. The operational concepts articulated in JV 2010 remain: Dominant Maneuver, Precision Engagement, Focused Logistics and Full Dimensional Protection. Of these, JEDI addresses Information Superiority, Environment and Innovation, and is desirably focused on Interoperability. JV 2020 continues its predecessor's focus on the operational setting, the regime in which JEDI functions. JEDI is aligned with JV 2020's changes from JV 2010's priorities. The concept of Full Spectrum Dominance has moved to the fore, with its emphasis on engagement throughout the continuum of force projection. Likewise, Information Superiority pivots on "decision superiority." All these require joint and combined interoperability in a common operating environment demanding unprecedented agility. This JCS statement defines the character and direction of JEDI.

Information Superiority: JEDI supports enhanced interoperability among intelligence organizations and operational combatant commands within the Global Information Grid. This is accomplished by ensuring a standard underlying infrastructure capable of hosting critical mission applications in a secure environment.

Innovation: JEDI's developmental cornerstone is a dynamic requirements-to-development process. As an open system, leading edge technologies and applicable prototypes will be incorporated into JEDI. It will be designed to accommodate continuous upgrading in keeping with enhancements available from both industry and government research and development sectors.

6 Interoperability/Integration

Interoperability: JEDI provides capabilities for use with multiple applications, both segmented (for use with COE) and unsegmented. Segmentation is the process of modifying an application by rendering only those processes that are not yet available within COE. For example, if one has an application that runs a calculator as one of its tools, it would be removed from the application because it is already available in the COE baseline. JEDI is easily adapted to Solaris and Windows applications and is virtually transparent to the end user, while still supporting and managing the System Security Administrators role in theater management.

7 Assessment Methodology

The JEDI assessment is conducted at each of JEDI's three phases. Phase I, (JEDI Version 1.0), a proof of concept developers release, was the foundation of an SCI accreditable COE compatible baseline and is complete. Phase II (JEDI Version 1.1) is the first operational release representing the Initial Operating Capability (IOC) and was released on April 2001. The completion criteria for Phase II involved the successful completion of DoDIIS JITF/JITC/Security testing, BETA I/II testing, unit OT&E events, and the acceptance of JEDI v1.1 as the system of record for DoDIIS. Phase II also means Milestone III has been completed. Phase III (JEDI version 1.2) implements a full Web-based capability, additional user functionality and continued compliance and tighter interoperability with current versions of the COE, DoDIIS and USMTF formats. The first operational release for JEDI version 1.2 was completed May 2002. The final operational capability (FOC) will be declared when all service core systems and Unified Commands supporting the JFC have a common look and feel, working within a secure, standards based, shared architecture.

Testing of JEDI is completed as directed by the JEDI Program Office, Executive Agent, and at the discretion of the DoDIIS Milestone Three Authority. Large-scale formal testing, normally led by an operational test organization, is conducted on all version releases as deemed necessary by the DoDIIS Test and Evaluation process.

JEDI is developed and fielded on a planned five-year development and integration cycle. The cycle entails maturing of software application functionality into a common baseline and jointly interoperable workstations for fielding at combined Air Operations Centers. IOC was achieved with the delivery of a deployable JEDI v1.1 which met the minimum requirements identified by the DoDIIS DMB and the JEDI Requirements Matrix. Deployable is defined as the JEDI software package with integrated COTS software applications, support material, and unit level training delivered to Service and Unified Commands core systems.