



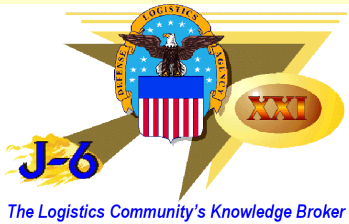
A Knowledge Management Approach to IA Policy & Reporting

Briefer: Larry Johnson, J-653 (703) 767-2195

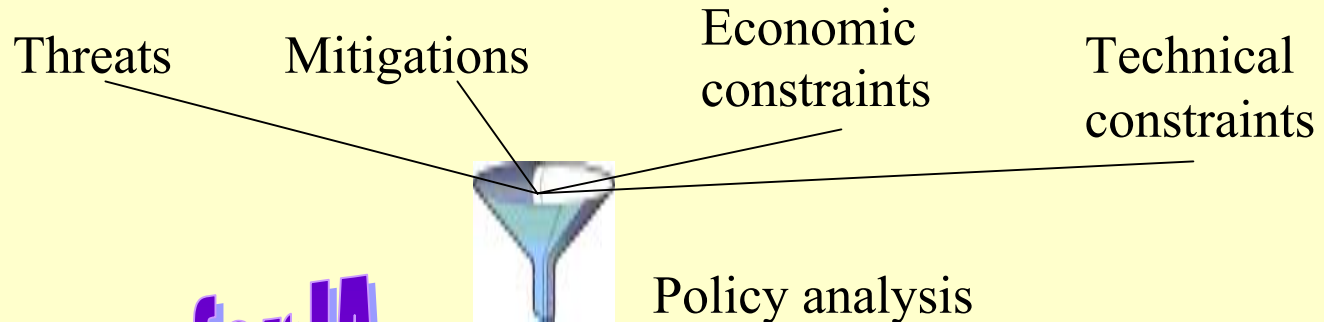


About DLA

- Defense Logistics Agency
 - 34,000 people
 - Worlds largest e-business
 - Over 5 million items in our catalog
 - 87 billion in inventory
 - 27 million transactions annually
 - 28,000 trading partners



IA Policy as a Problem Space



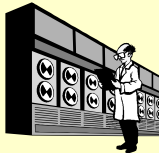
**A major vector for IA
vulnerabilities**



Policy formulation



Program development



Program execution



IA Policy as a Problem Space

Multiple policies can be duplicative

Policies can be obsolete

Policies can be incomplete

Policies can have inappropriate or inconsistent levels of abstraction

Polices can be misinterpreted



Policy Analysis



Policy formulation



Program development



Program execution



Knowledge Management



Policy Analysis



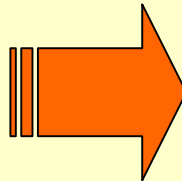
Policy formulation



Program development



Program execution



Construct a meta-level abstraction of the Policy chain

Independent of IA

Explicitly evaluate transformations

Extract factors that affect causality

Epistemological orientation



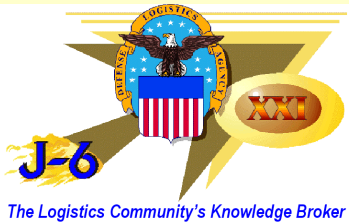
Case Study: DoD System Security Plans

- 600+ production (existing) LANs, systems & web sites must be certified and accredited under the DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
 - The product is a comprehensive security plan called a System Security Authorization Agreement (SSAA)
- Problems with the SSAAs:
 - Cost averages 75K per system: Effort was consuming virtually all IA resources
 - Virtually all are late
 - Huge variation in quality: two similar systems in the same enclave reported totally different
 - Threats
 - Mitigations
 - Risks



Case Study: DoD System Security Plans

- SSAAs were not designed for existing systems or sites
 - Phases map to new system life cycle management
 - Requirements
 - Design
 - Development
 - Testing & Implementation
 - Can generate huge amount of effort with no appreciable security improvements
 - Efforts were being “hand crafted”
 - Each project creates their own security solution



Case Study: Solution Set

- Standardize threats, mitigations and risk analysis across DLA based upon current DoD “Defense in Depth” policy
- Map LCM phases to a process that’s relevant to existing LANs and systems
- Simplify the SSAA preparation process by an order of magnitude
 - Migrate resources from document development to implementing protection mechanisms





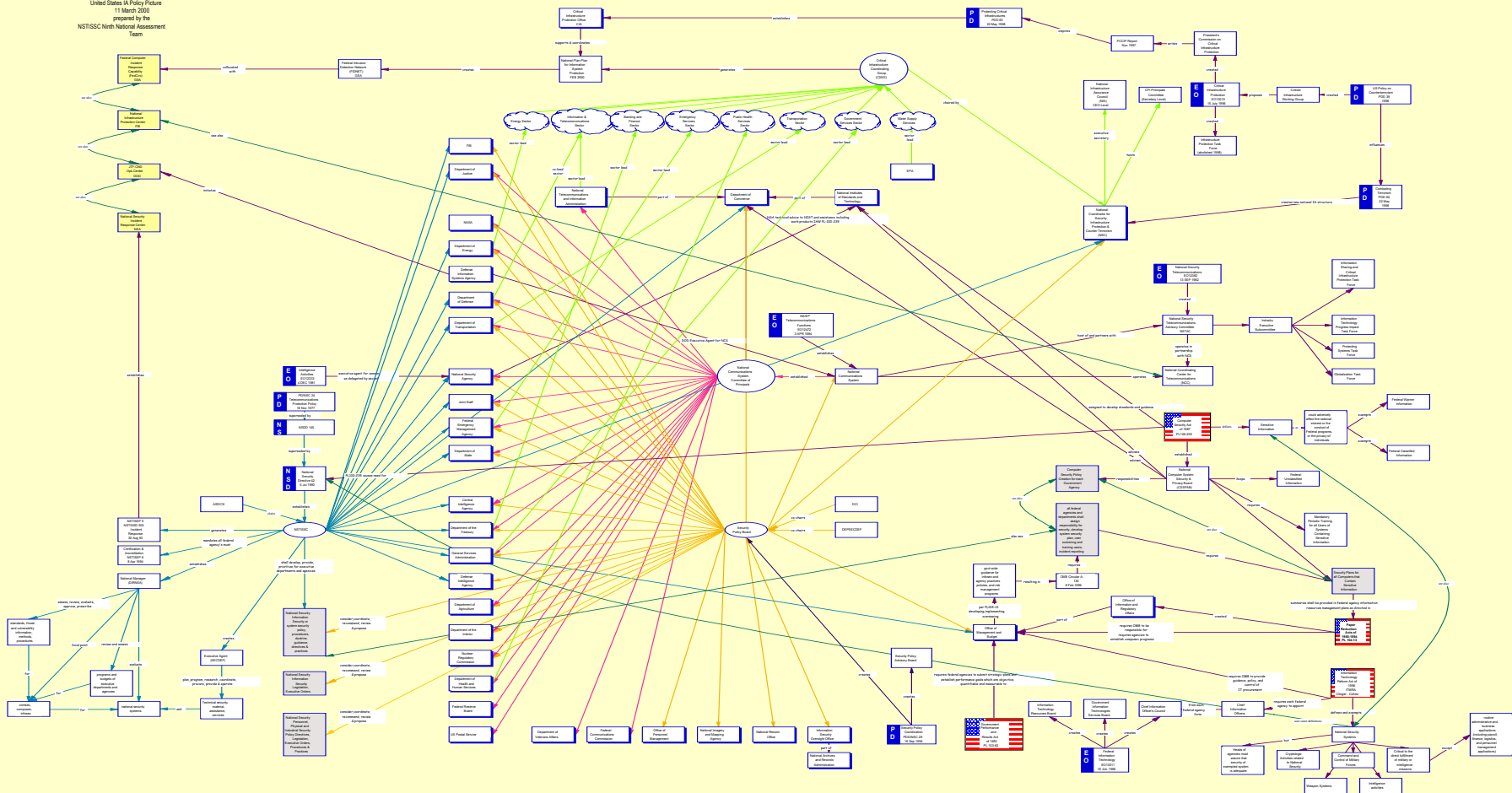
Case Study: Solution Set

- The **program** DLA created to accomplish these three critical success factors is called: ***Metrics and Controls for Defense in Depth (McDID)***
- The **system** created to support the program is called: ***Comprehensive Information Assurance Knowledge-base (CIAK)***



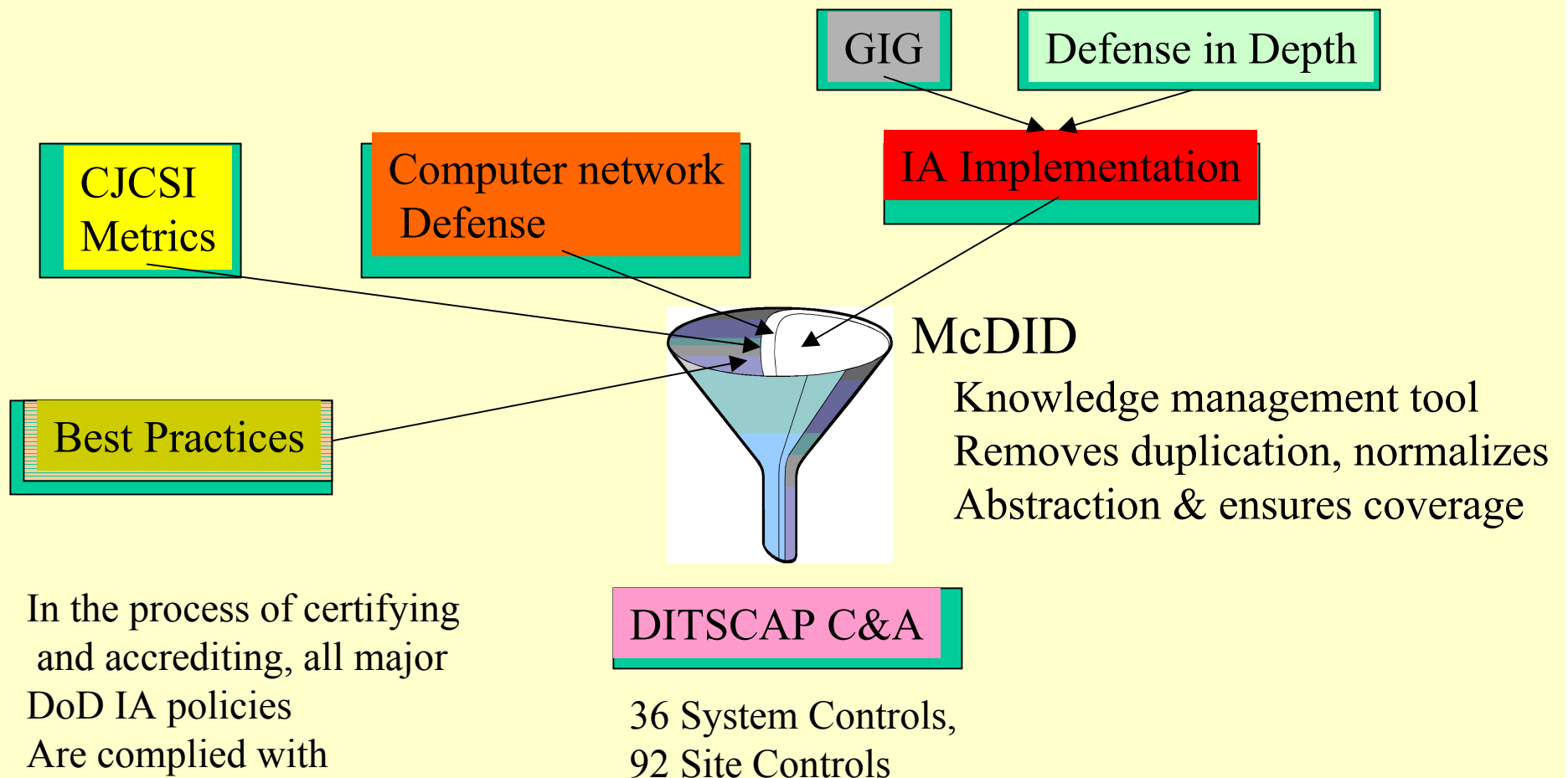
DLA's IA Policy World

United States IA Policy Picture
11 March 2000
prepared by the
NSTISSC North National Assessment
Team



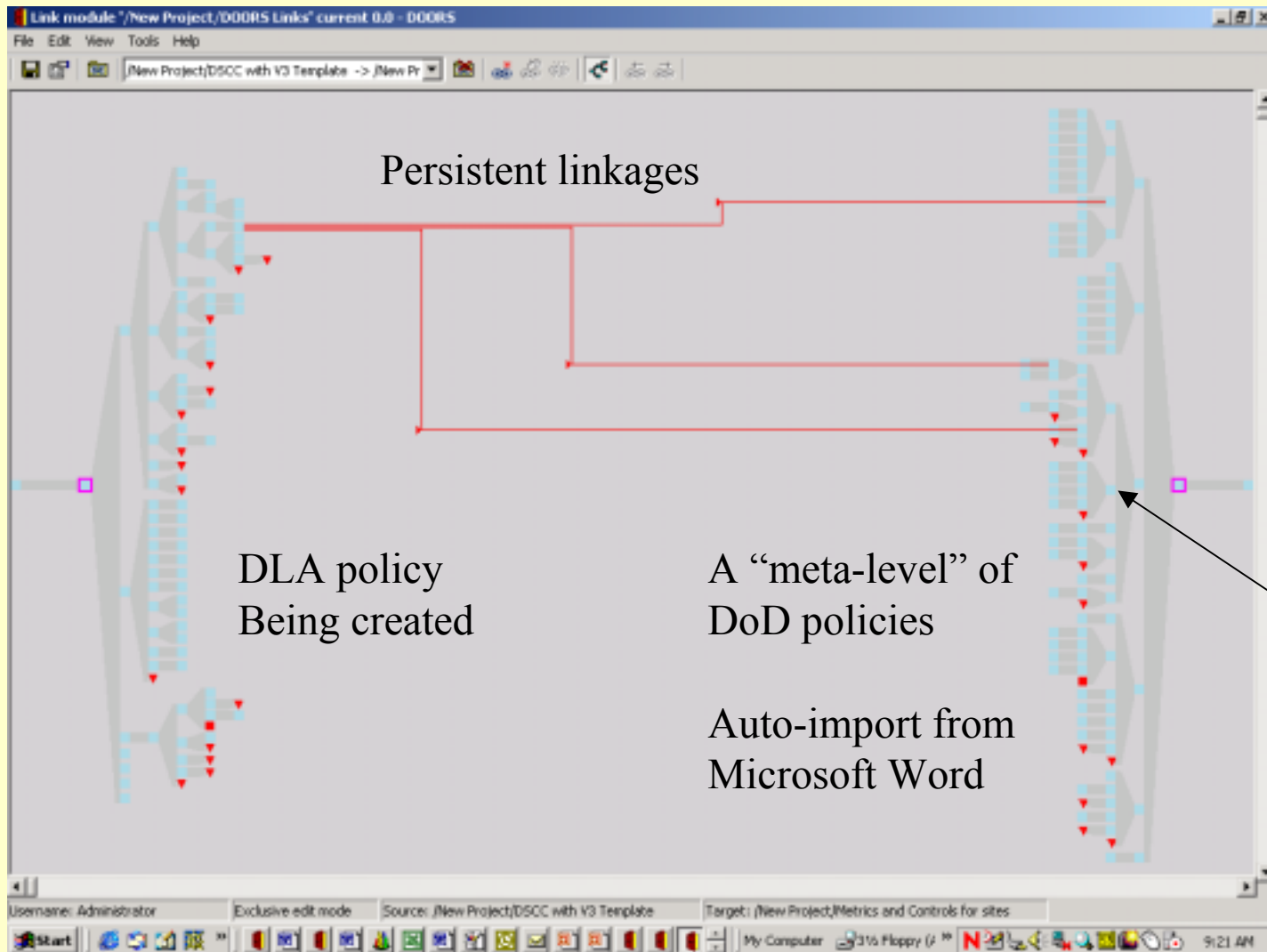


McDID: Using DITSCAP for Policy Integration





CIAK Knowledge Management Tool



DOORS object-oriented database



CIAK

Formal module "/DATABASE/STIG/Database Security Technical Implementation Guide" current: 6.0 - DOORS

Standard view All levels

ID	Object Name
375	2 Integrity
376	Area Commands, RSAs and Regional Operations and Security Centers (ROSC) achieve data integrity by managing the database management files, database itself. Off-the-shelf installations offer limited

Object 376 properties - DOORS

General Access History Attributes Links

User	Session	Date	Modification
DBA	1	10/17/00 12:48:12	Create Object
DBA	5	10/25/00 09:50:34	Modify Object Attribute: Object Text
DBA	5	10/25/00 09:52:02	Modify Object Attribute: Object Text

Details of selected history record

From: Area Commands, RSAs and Regional Operations and Security Centers (ROSC) achieve data integrity by managing the

To: Area Commands, RSAs and Regional Operations and Security Centers (ROSC) achieve data integrity by managing the

Only show entries with

Dates: from [] to []

User: []

Details... Refresh Export... Previous Next OK Cancel Apply Help

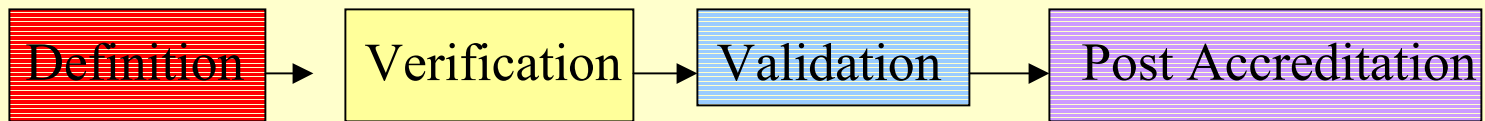
Username: DBA Exclusive edit mode

9:52 AM

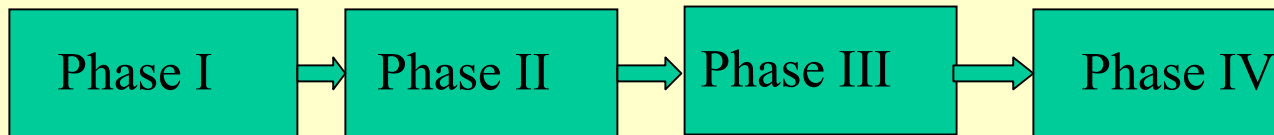
CIAK provides automatic configuration management & workflow



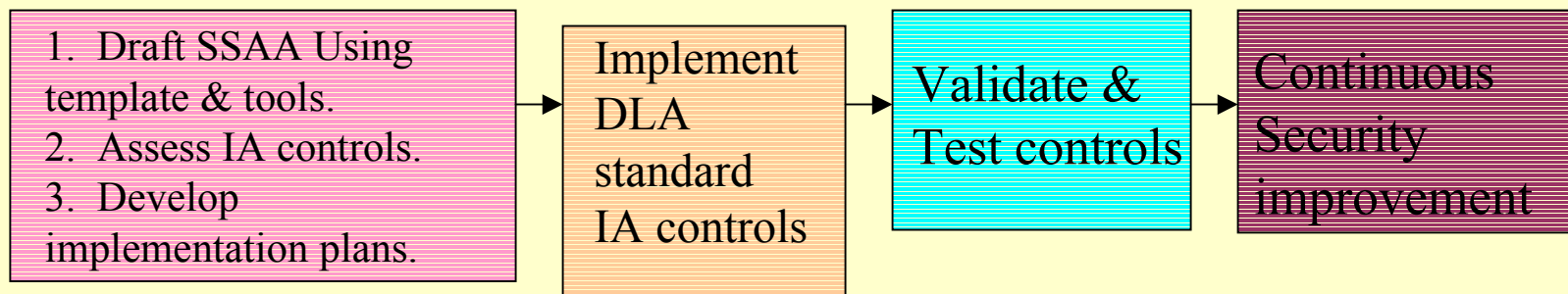
Mapping LCM Phases to Existing LANs and Systems



Traditional SSAA



McDID





The Logistics Community's Knowledge Portal

CIAK

Formal module 'SSAA Template/Site SSAA Template Version 3' current 0.0 - DOORS

File Edit View Insert Link Analysis Table Tools User Help

Overview Level 2

Site SSAA Template

SSAA

- MAIN BODY
- APPENDICES
- McDID SELF ASSESSMENT
- POAM
- VALIDATION
- RISK ASSESSMENT
- CERTIFICATION & ACCREDITATIO

Username: glenda Exclusive edit mode

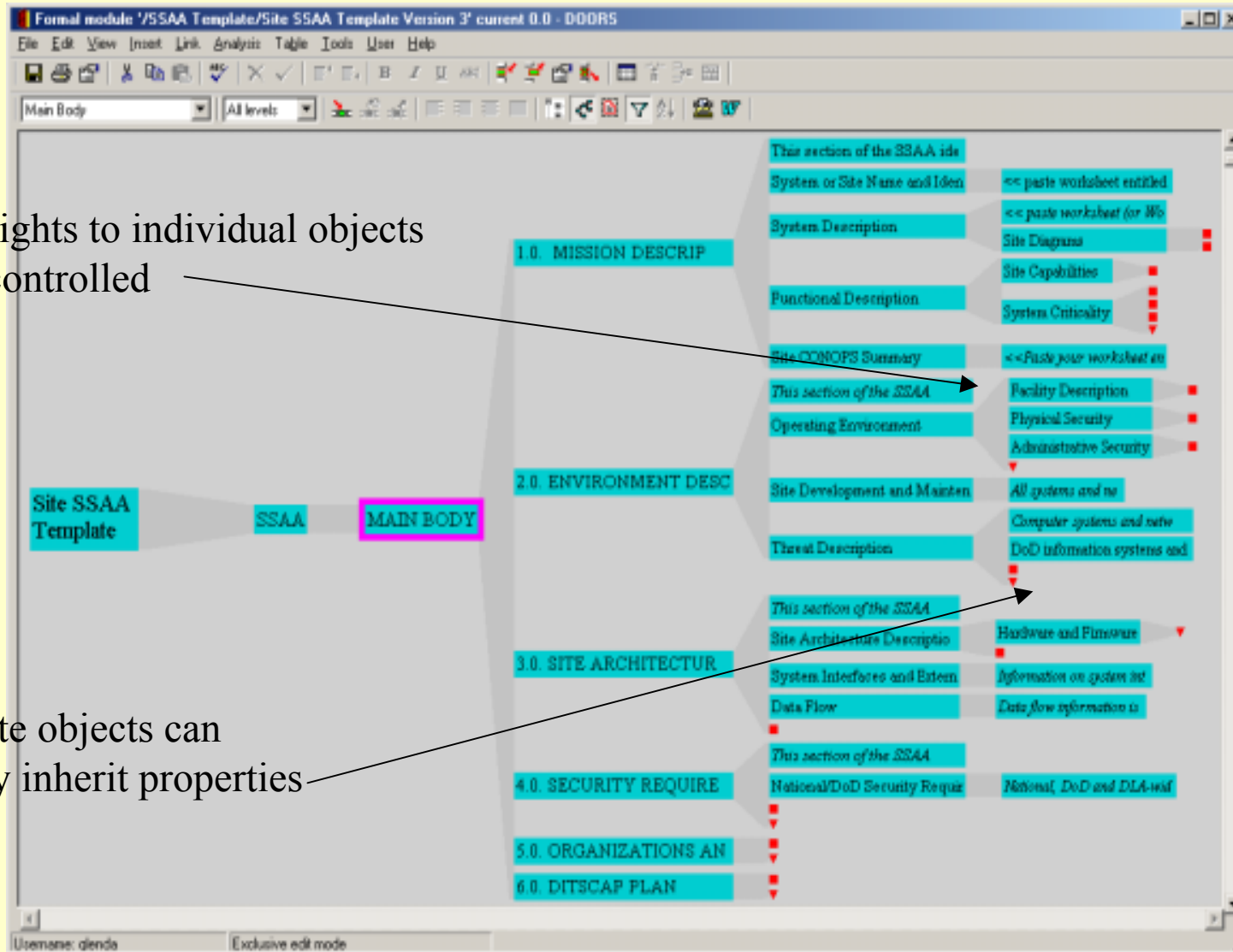
CIAK decomposes documents visually
For easy navigation



CIAK

Access rights to individual objects
Can be controlled

Subordinate objects can
Selectively inherit properties



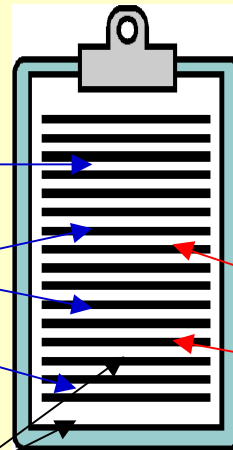


Making C&A Easier (but more comprehensive & consistent)

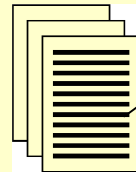
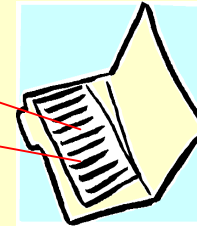
“Standard” SSAA Outline

1. Write the enterprise parts

Threats
CONOPS
Mitigations
Risk Assessment

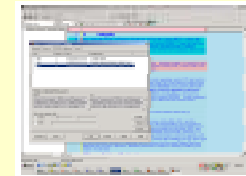


2. Translate narrative
Into “fill in the blank”



3. Provide templates
(for both authors & evaluators)

4. Use a web-based
Automated configuration
Management system for
workflow





The Logistics Community's Knowledge Broker

Policy Simplification

Formal module 'New Project/DSCC with V3 Template' current 0.0 - DOORS

File Edit View Insert Link Analysis Table Tools User Help

Standard view All levels

DSCC with V3 Template

- 1 DSCC SSAA
 - 1.1 MAIN BODY
 - 1.1.1 MISSION DESCRIPTION
 - 1.1.1.1 Systems or Site
 - 1.1.1.1.1 Systems or Site Description
 - 1.1.1.1.2 System Description
 - 1.1.1.1.3 Functional Description
 - 1.1.1.1.4 Site CONOP
 - 1.1.1.2 ENVIRONMENT DESCRIPTION
 - 1.1.1.3 SITE ARCHITECTURE
 - 1.1.1.4 SECURITY REQUIREMENTS
 - 1.1.1.5 ORGANIZATIONS
 - 1.1.1.6 DETSCAP PLAN
 - 1.2 APPENDICES
 - 3.0 DODD SELF ASSESSMENT
 - POAM
 - VALIDATION
 - CBA RECOMMENDATION
 - CERTIFICATION AND ACCREDITATION

Demonstration SSAA with DSCC Data

17 In accordance with DoD CIO P&GM 6-8510, paragraph 4.10, the site's Information Assurance level of robustness is **Basic**, which requires information assurance practices commensurate with industry best practices.

21 1.1.1.3.2.1 Classification and Sensitivity of Data Processed

22 The following matrix describes the functional category of data processed (e.g., e-mail, network management traffic, personal transactions, financial transactions), the classification and sensitivity of the data (e.g., Unclassified, Privacy Act, Financially Sensitive, Proprietary, Administrative/Other, Confidential, Secret, Top Secret, Compartmented/Special Access), the user clearance level required for access, the data source (originating application), the data target (receiving application), and the transmission mode (e.g., Internet, Web, File Transfer Protocol (FTP), Telnet, Stand Alone, Manual Procedure, Value Added Network(VAN)). For transmissions outside the boundary of this SSAA, the matrix also includes the protection measures in place and the certification and accreditation (C&A) status of the interfacing system or network.

23

Date Last Updated:		10/29/2003					
Functional Data Category (e.g., e-mail, network management traffic, ADS data, financial, contract, requirements, etc.)	Data Type (Unclassified, Privacy Act, Sensitive, Administrative/Other, Confidential, Secret, Top Secret, Compartmented/Special Access)	User Clearance Level (Unclassified, Sensitive, Other)	Data Source (Originating System, System or Module)	Receiving System or Module	Transmission Mode (Internet, Web, FTP, Telnet, Stand Alone, Manual Procedure, VAN, Other)	Protection Mechanisms (VPN, SSL, Secure Shell, Other)	C&A Status of Interfacing System
email	administrative	Unclassified	Internet/Intranet	Exchange/Outlook	SMTP	PGP as required	N/A
office automation	administrative	Unclassified	App Servers	Workstations	Intranet	Not Required	N/A
personal	privacy act	Unclassified		CORD			N/A
LEADS	privacy act	Non-Critical Sensitive	State of OH	Investigator Workstation	Internet - State related circuit		N/A
USMMS	Administrative	Non-Sensitive	DSCC	HP1, HP6, HP6, HP13	FTP, Telnet	with DSCC/DSCC online	In Process

24 1.1.1.3.2.2 System User Description and Clearance Levels

Username: Administrator Exclusive edit mode

Start My Computer 3 1/2 Floppy (J) 9:36 AM

SSAA's can go directly in CIAK via the web for automated configuration management and workflow



Policy Simplification

Microsoft Access - [Control Table]

File Edit View Query Format Records Tools Window Help

Status Bar

Subject Area: PHYSICAL SECURITY Group: Environmental Security

Control

The site maintains a written inventory/accounting of all site critical servers and IA Technology for temperature and humidity range requirements. If requirements exceed site office environment settings, the site must possess automated temperature and humidity recording devices with range setting and alarms.

ENTRI_ID: 1.1.1.1

Check if Completed

Close

Level	Level Text	Status	Est Start	Est Comp	Approved
C1	All equipment is operating within the range of its operating environment, OR Automated recording and alarm devices are completely installed and fully operational.	<input type="checkbox"/>			1.1.1.1
<input type="checkbox"/>	The plan has been approved, funded and are partially but not completely implemented.	<input type="checkbox"/>			1.1.1.1
<input checked="" type="checkbox"/>	A plan to meet temperature and humidity requirements is being developed.	<input checked="" type="checkbox"/>			1.1.1.1
C1	Temperature and humidity operating range of site critical servers and IA Technology are not documented.	<input checked="" type="checkbox"/>			1.1.1.1

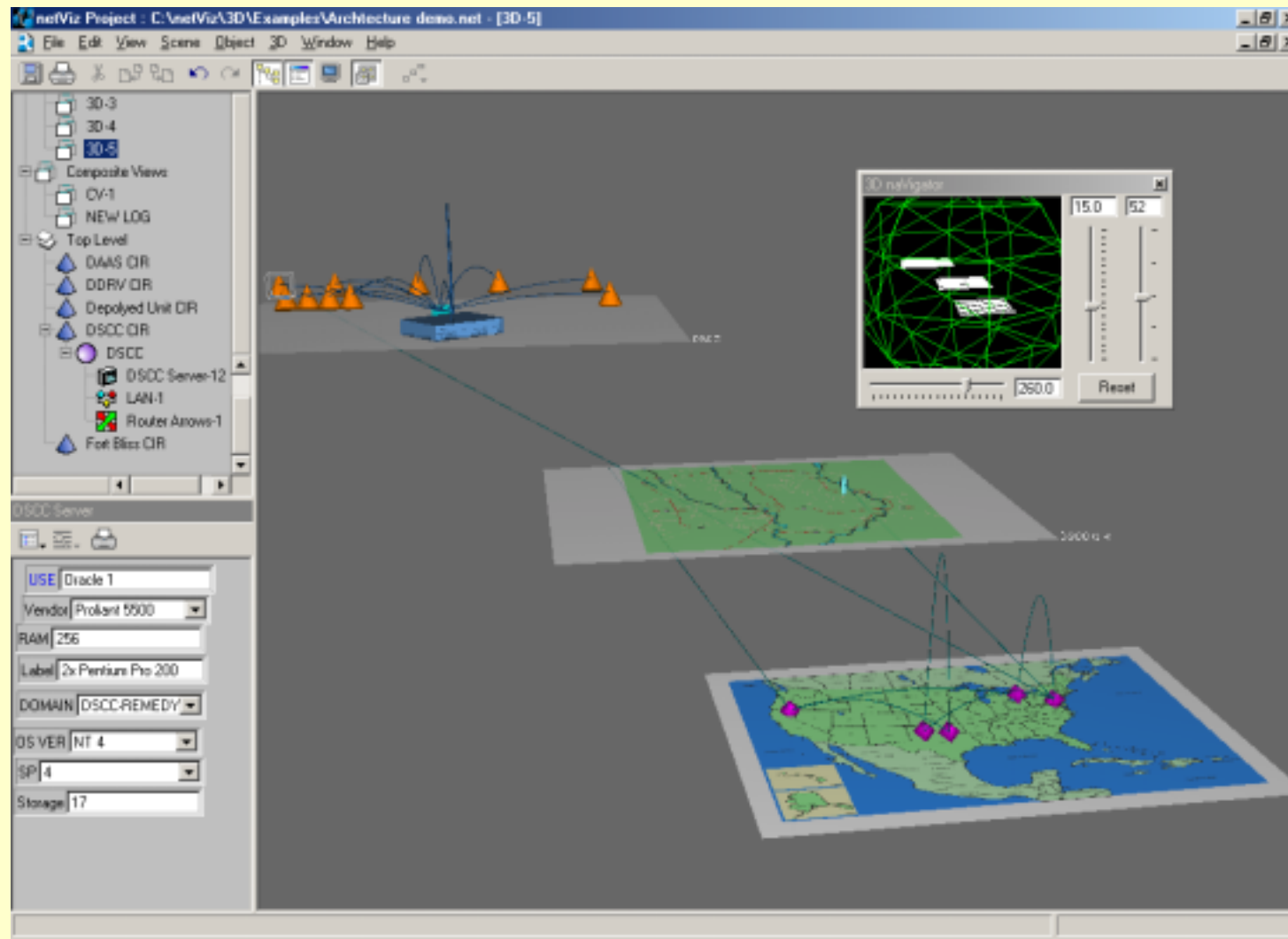
Records: 4 of 11

9:00 AM

Self assessment & plan of action tool

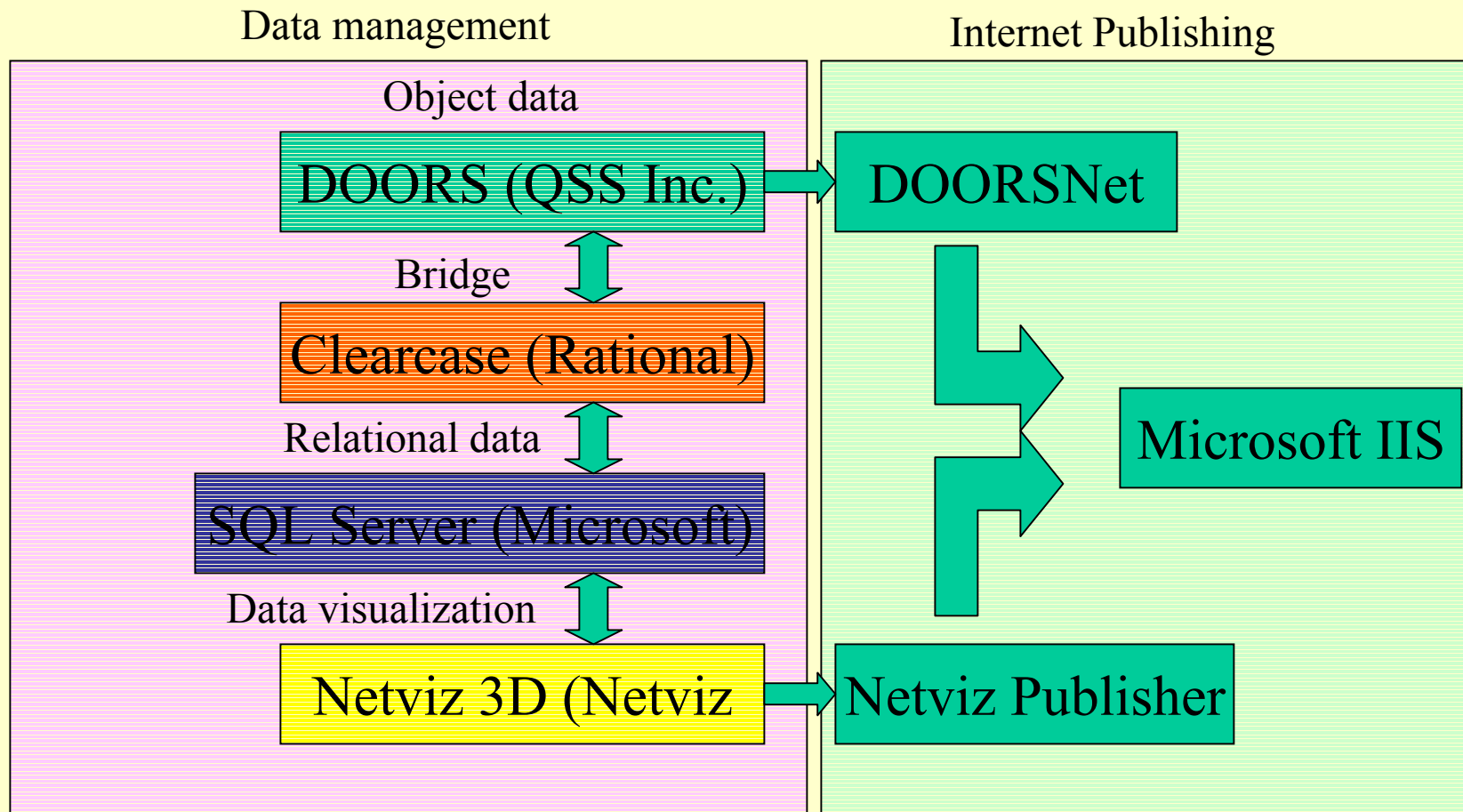


3D IA Architecture





CIAK Architecture





Status

- CIAK recently came on-line in early December
- First production system showed 90% savings in time and cost
- CIO briefed and requested Deputy Director briefing
- Planning integration with DLA's Asset Management Program



Other Uses?

- Taxonomic based research
 - Threat taxonomies
 - Attack signatures
- A possible mechanism for protection against litigation
 - Reasonable
 - Prudent
- Mapping complex policies
 - Common Criteria to BSI 7799
- Integration with other automated tools
 - Asset management
 - Configuration management



Conclusion

- Policy is a major vector of IA vulnerabilities in large, complex organizations
 - A formal policy analysis methodology based upon knowledge management tools (particularly object oriented databases) can substantially reduce policy based vulnerabilities
 - Tools are very inexpensive & easy to use
- DLA's McDID/CIAK programs is showing some early successes
 - Large delta in time & cost
 - Standardized security across sites & systems
 - Web-based workflow & configuration management
- DLA would like to see the IA community adopt formal policy analysis methodologies



Points of Contact

- Larry Johnson
 - (703) 767-2195
 - Larry_johnson@hq.dla.mil
- Glenda Turner (Booz Allen & Hamilton)
 - (703) 289-5279
 - Turner_glenda@bah.com