Trusted Information Management Framework

John F. Coughlin, Ph.D.

Agenda

- Challenges
  - Multi-media and valued information
  - System maturity
  - Impacts: Laws, Industry, Information Sharing
- Service Oriented Architecture Evolution
  - Trusted Information Sharing
  - Web Software Evolution
  - Architecture Evolution
  - SOA Example
- 10 Major KM, RA, TIS Framework Objectives
  - Examples: Secure Information; Biometrics, COP

The Challenges of a Demanding Information Environment

Mission Challenges

- National and local priority for timely intelligence
- More complex, less predictable world-order; internal security
- Explosive growth in amount/variety of information available and the speed at which it is delivered

Legacy Technology Challenges

- Non-integrated systems/tools
- Disparate DBs and data structures
- Limited collaboration
- Lack of auditing, data protection

Text

Biometric

Geospatial

Signals/RFID

Video

Today's Technology Challenge:

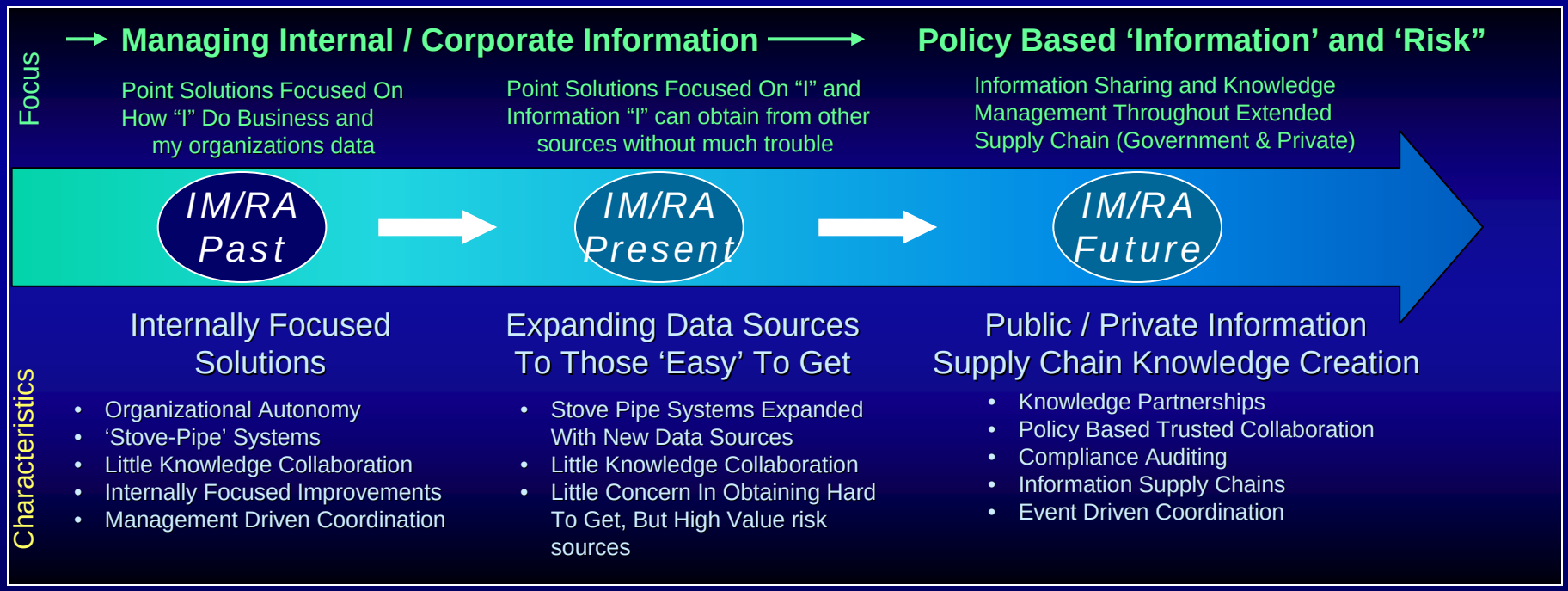
Creating Effective, Flexible Solutions

- Connectivity, Speed, Volume
- Enterprise application integration
- Workflow integration or multi-media
- Federated search capability
- Link analysis and visualization
- Automated taxonomy categorization
- Auditing and policy compliance
- Multi-Lingual Processing

Agile Trusted Framework Integrates Technology to Meet Mission Needs

Maturing Customer Missions and Needs

- *Customer needs for trusted Information Management and Risk Assessment moving from point to extended enterprise solutions crossing government agencies, multiple countries, public sources, and commercially owned data, information, and knowledge*
- *Customer quote "yes, I need to federate my search, but I need to do it in a secure way that ensures I am not violating any classification or use rules on the informaiton"*



Delivering right trusted information to right person at right time is forcing customers to demand more than just technology, but 'information, risk, and knowledge impacts'

Legal Implications on Trusted Information

- *The Department of Homeland Security announced … the issuance of Designations and Certifications for anti-terrorism technologies under the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act).*
- *Omnibus Congressional Bill: 2003*
- *Anti-Terrorism Acts*
  - *-Information Sharing*
  - *-Passport changes*
  - *-Commercial Insurance.*

Facilitates Deployment of Critical Antiterrorism Technology

SOA Framework for Trusted Information

Geospatial

Biometric

Text

Signals/RFID

Video

- **Service Oriented Architecture, Web-based, multi-source information management, and exploitation capability**
  - Framework developed to reduce integration complexity
  - Proactive pre-processing of multiple data sources & types
  - Predictive categorization, federated search & automated discovery of information
  - Collaborative tools to quickly share relevant information
- **Built on commercial platforms (COTS), SOA, and an enterprise infrastructure**
  - Commercial best practices; Architecture blueprints from Microsoft, IBM, EMC, Cisco, Oracle
  - Flex, extensible, scalable, reusable, component-based design
  - Open standards leveraged
- **Agile development for innovation and system evolution**
  - Rapid fielding of initial capabilities
  - Iterative, continuous improvement reduces risk
  - Promotes rapid optimization for specific business needs

Analysts and Knowledge Workers

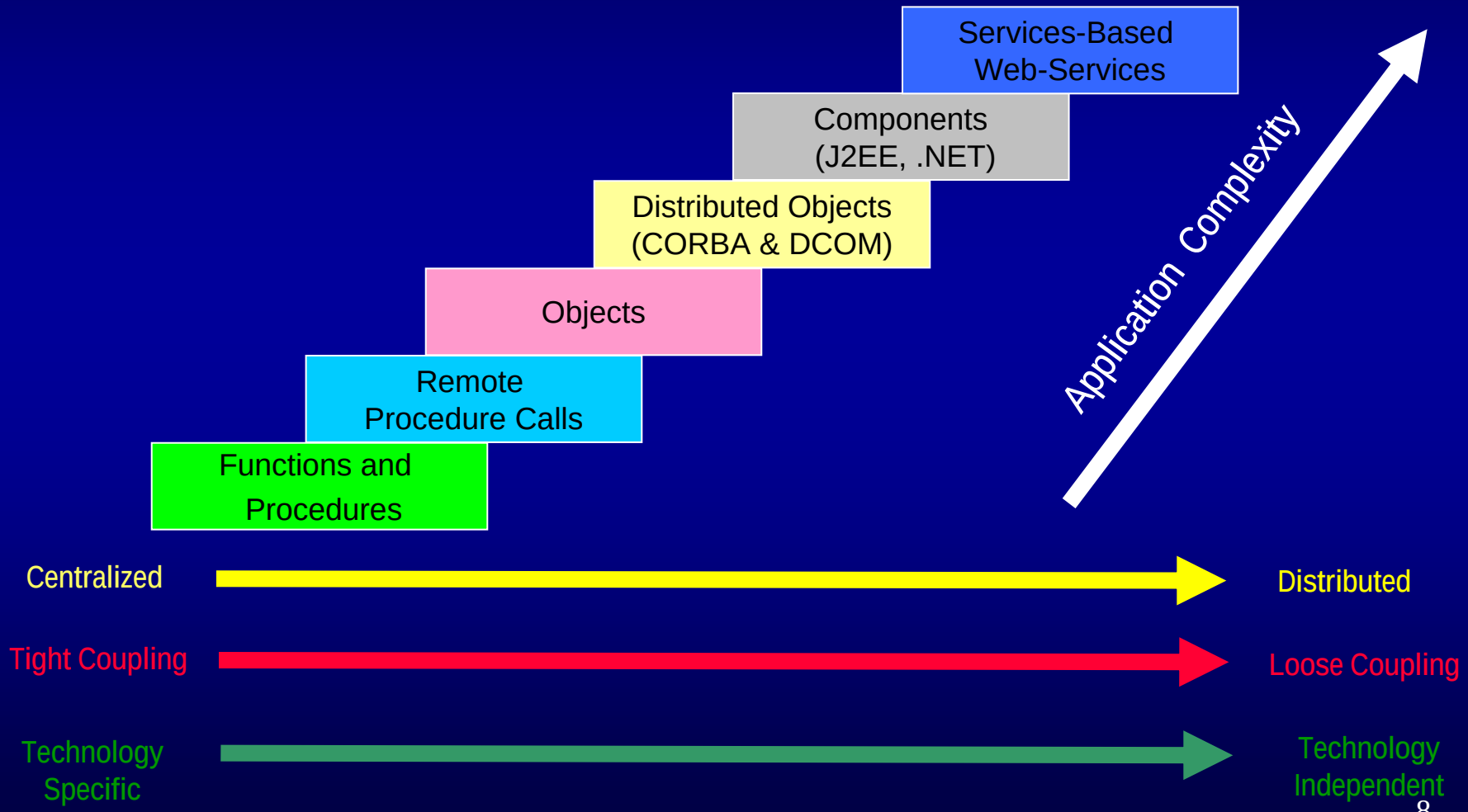
Multi-Sources/Types Data → Exploitation → Actionable Information

Information Sharing Mission Needs

- *Real-time threat-based risk assessment of terrorist events against critical infrastructure*
  - *Aircraft, airports, trucks, trains, refineries, power plants, critical supply chains, water supplies, and other national assets*
  - *Allows for real-time terrorism "situational awareness" and deployment of security measures against the highest threat assets*
- *The integration of public, commercial, and government information to assess terrorist risk while:*
  - *Enhancing the privacy and civil liberties of citizens*
  - *Protecting information shared between governments*
  - *Protecting sources & collection means of classified information*
  - *Sharing data across multiple levels of "security or policy domains"*
- *Measure and certify the effectiveness of the risk assessment and information sharing providing the potential for improved situational awareness*

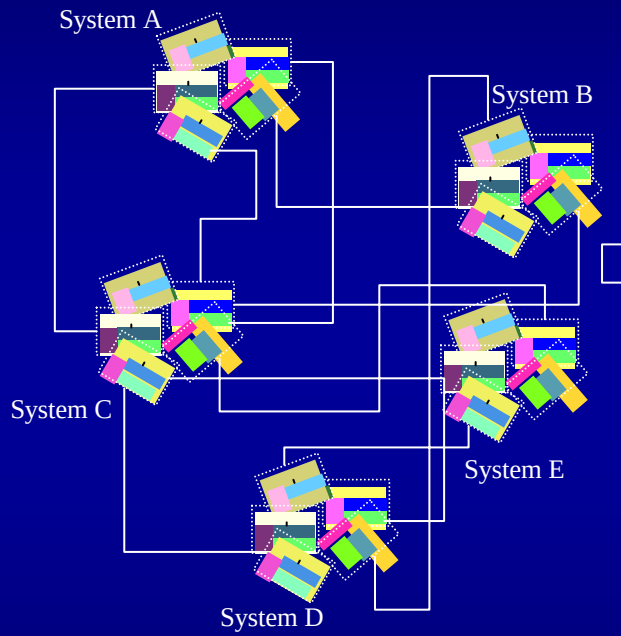
Background: Evolution of Web-based Software

Software paradigms evolved to manage greater levels of complexity



System-of-Systems to SOA Transition

Systems Architecture



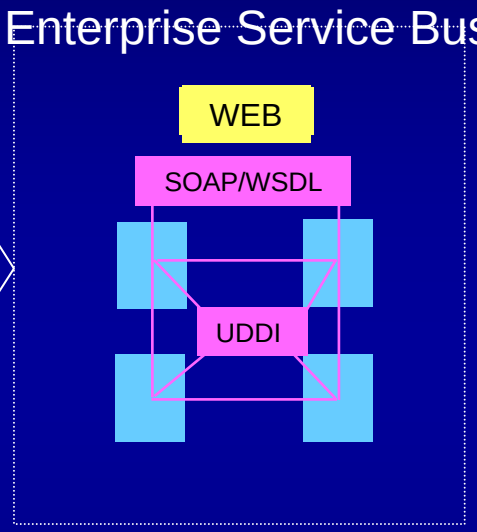
- Complex inflexible interfaces between domains
- Redundant and inconsistent frameworks

SOA Transition steps

Enterprise Service Bus

- *Wrap legacy services and expose as web services*
- *Deploy directory services*
- *Create/optimize target cycle workflows*
- *Manage services*

SOA Architecture



- Rapid integration of new functionality
- Improved scalability and reliability

Managing workflows that use services across domains are transitioning to service-oriented architectures to reduce the cost and complexity of integration

Service Oriented Trusted Architecture

-Browser-based solution
-Portal-based view
-Portable Applications
-Wireless Connectivity

Internet

User Services

Presentation Service
Search | GIS
Portal | VIZRT

Rules

Alert Management Service

Biometric Authentication & Identification

Trusted Information Services (TIS)
- Watchlists
- Intel Reports

Web Services
Exploitation Services
Natural Language Extraction
Translation
Normalization
Auditing
Data Stores

History DB
BIO DB
Cargo DB

Data Services

VIDEO
Content Management Service

Intelligent Agents
Agent Service

TRACKS
Situation Information Service

Advanced Notice Service

Modeling and Simulation Service

Enterprise Service Bus

Weather Service
CBNRE Sensor Service
Video Input Service
CCTV
Cargo Inspection Service
XRAY
Truck/Rail Tracking Service
GPS
Port Tracking Service
RFID
Sea Tracking Service
AIS | Radar

Environmental Services

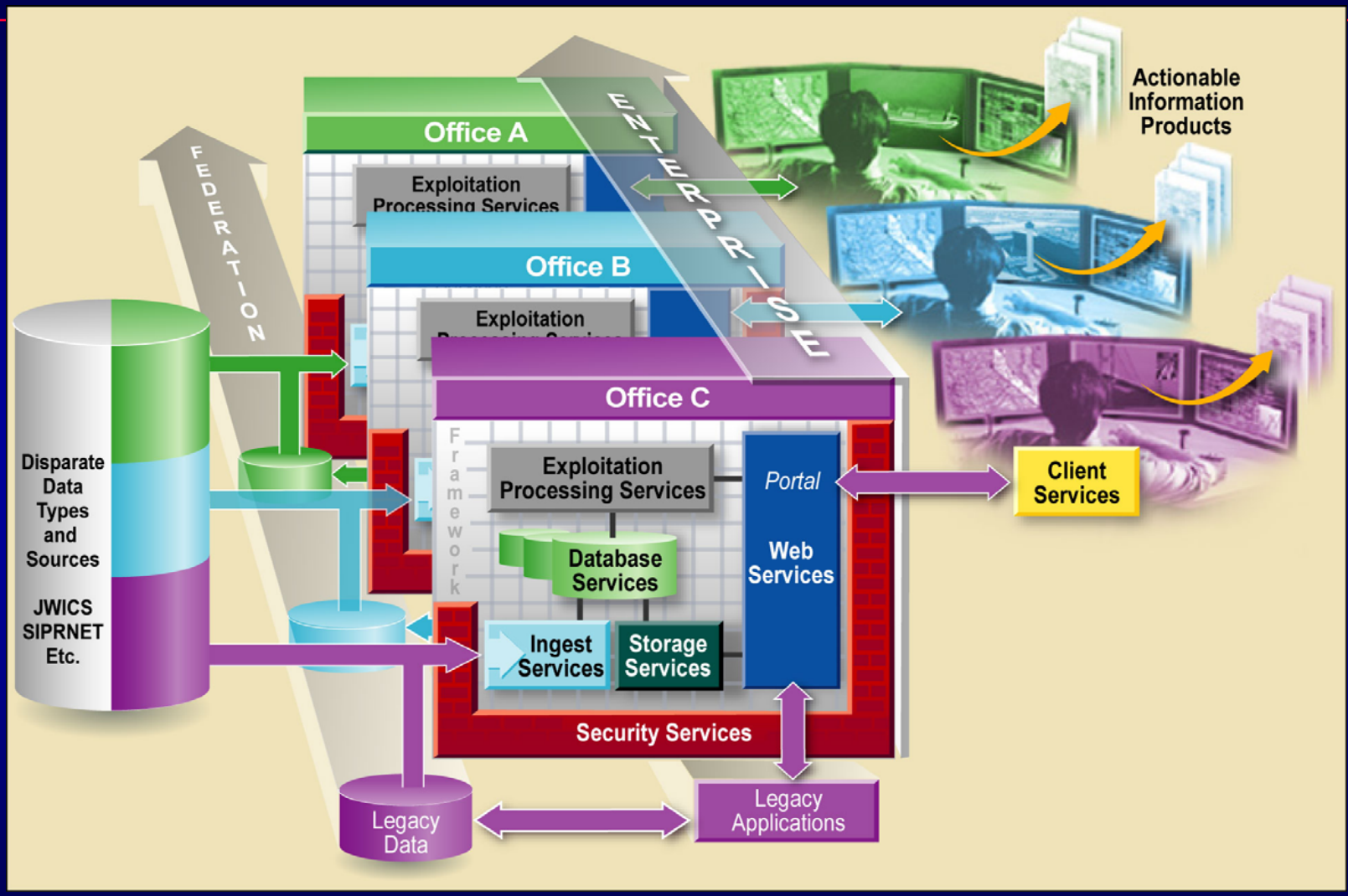
Security Services

Tracking Services

10 Major KM, RA, TIS Framework Objectives

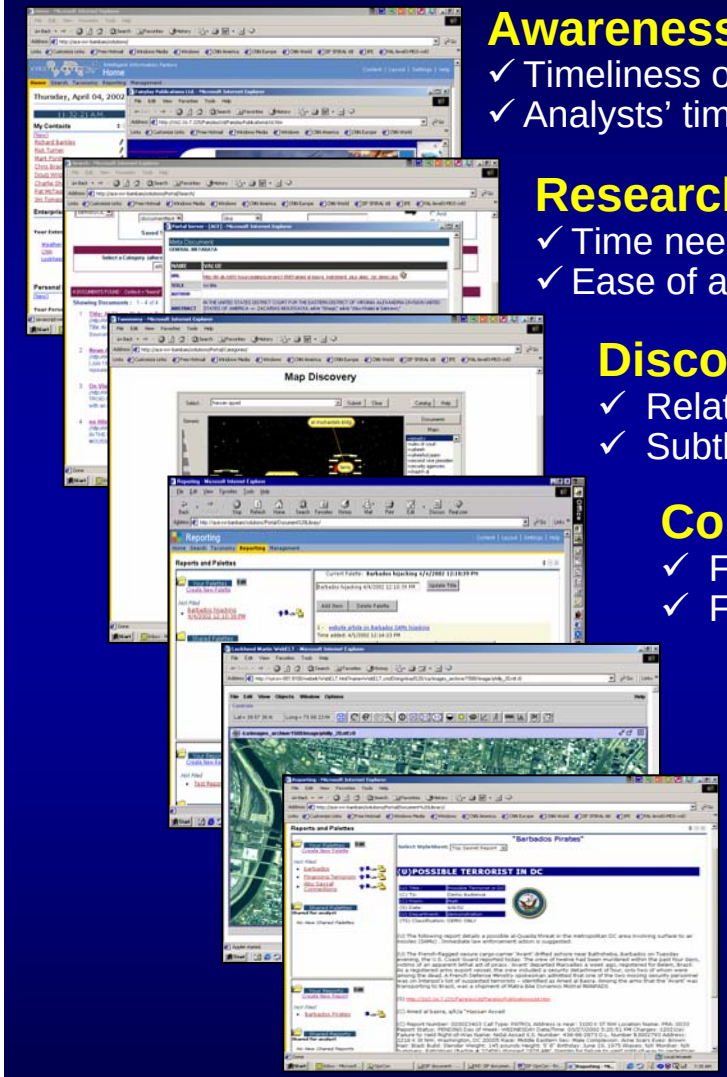
- Ubiquitous access. A user-specific layout enables each analyst to personalize the applications that he/she have on the desktop; enterprise applications (email, etc.) are integrated as well as specific applications.
- Security Access Control. Access control lists are maintained using a distributed, controlled system. Industry standard access control mechanisms are placed between the system and the client machines.
- Awareness/Notification. Information detection enables the establishment of analyst "profiles" for monitoring selected internal and external data sources; and provides an automated mechanism for "pushing" information (including threat warnings/alerts).
- Information/Data Research. Framework capabilities including the ability to search against multiple data sources (and types) such as text, multi-media, and geospatial information; and the ability to conduct 'federated' searches of selected external (legacy) databases.
- Data Ingest. Mechanisms for ingesting data from lower security levels as well as data from the same security level automatically generate metadata providing date and time of ingest, classification, title, abstract, and other simple automatically generated metadata. Automated policies decide based on the source location whether or not to persist a copy of the original data.

Security Services for Information Management



SOA Solution Comprises a Standards Based Framework and COTS Analysis Tools to Meet Mission Performance and TCO Objectives

Integrated Application of Technology Supports Improved Analytic Results



Awareness –

- ✓ Timeliness of info improved by high-speed ingest and advanced pre-processing
- ✓ Analysts' time is free to concentrate on analysis

Research –

- ✓ Time needed to conduct research is reduced by parallel search
- ✓ Ease of access to multiple data sources supports comprehensive results

Discovery –

- ✓ Relationships hidden by data volume are quickly made evident
- ✓ Subtle/indirect relationships are more readily identified

Collaboration –

- ✓ Facilitates easy/timely access to full breadth of available expertise
- ✓ Facilitates integration of independent results

Fusion –

- ✓ Integration of multiple data types provides efficiency and improves accessibility to comprehensive data

Production –

- ✓ Analysts spend less time formatting and disseminating results
- ✓ Results become cumulative through automatic re-ingest
- ✓ Policy compliance and trusted control of data

Secure, Faster, Better Analytic Result

10 Major Objectives continued

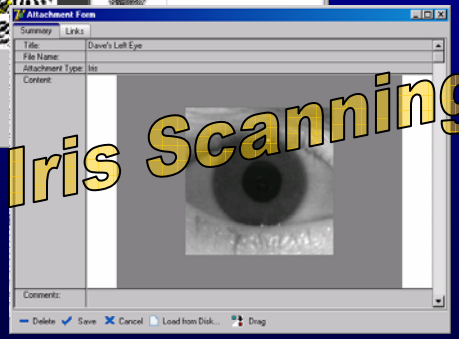
- Data Storage Extending the Databases. Storage, as an extension of database access, insures that all source data used for analysis are searchable and (ingested and indexed). All source data has the classification metadata stored along with the data. Source de-confliction for identical copies collected from multiple locations prevents duplication. Data search and retrieval will be in a time frame consistent with accessing a typical web page.
- Advanced Data Analysis/Fusion. Framework accommodates numerous analytic tools (link analysis, data mining, extraction, natural language processing, etc.) to fuse relevant information into a "big picture" of the threat/alert.
- Information Sharing/Collaboration. Framework accommodates integration of existing collaborative tools/capabilities to enable multiple analyst to contribute and to enable federal/state/local subject matter experts (SMEs) to interact.
- Report Production/Dissemination. Information sharing needs incorporate capabilities to streamline the creation of reports/products outlining threats and detailing operations for mitigating; including multiple auto-redactable versions of the same report for dissemination at different classification levels.
- Information-Centric Secure Environment. The Trusted architecture provides information security for the traditional network and beyond as well as enterprise auditing. Emphasis is placed on guaranteeing the information assurance attributes of identification, authentication, non-repudiation, integrity, and confidentiality in an information system and auditing compliance with policy directives or laws.

Biometric Authentication and Identification

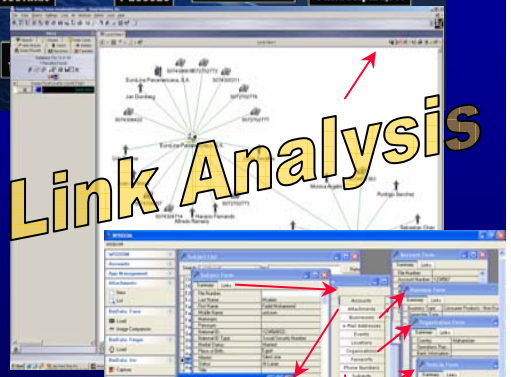
- Hardware Configurations, Biometric Algorithms, and Information Management Capabilities Can be Customized and Combined to Create Integrated Solutions For Mission Specific Applications

Hardware

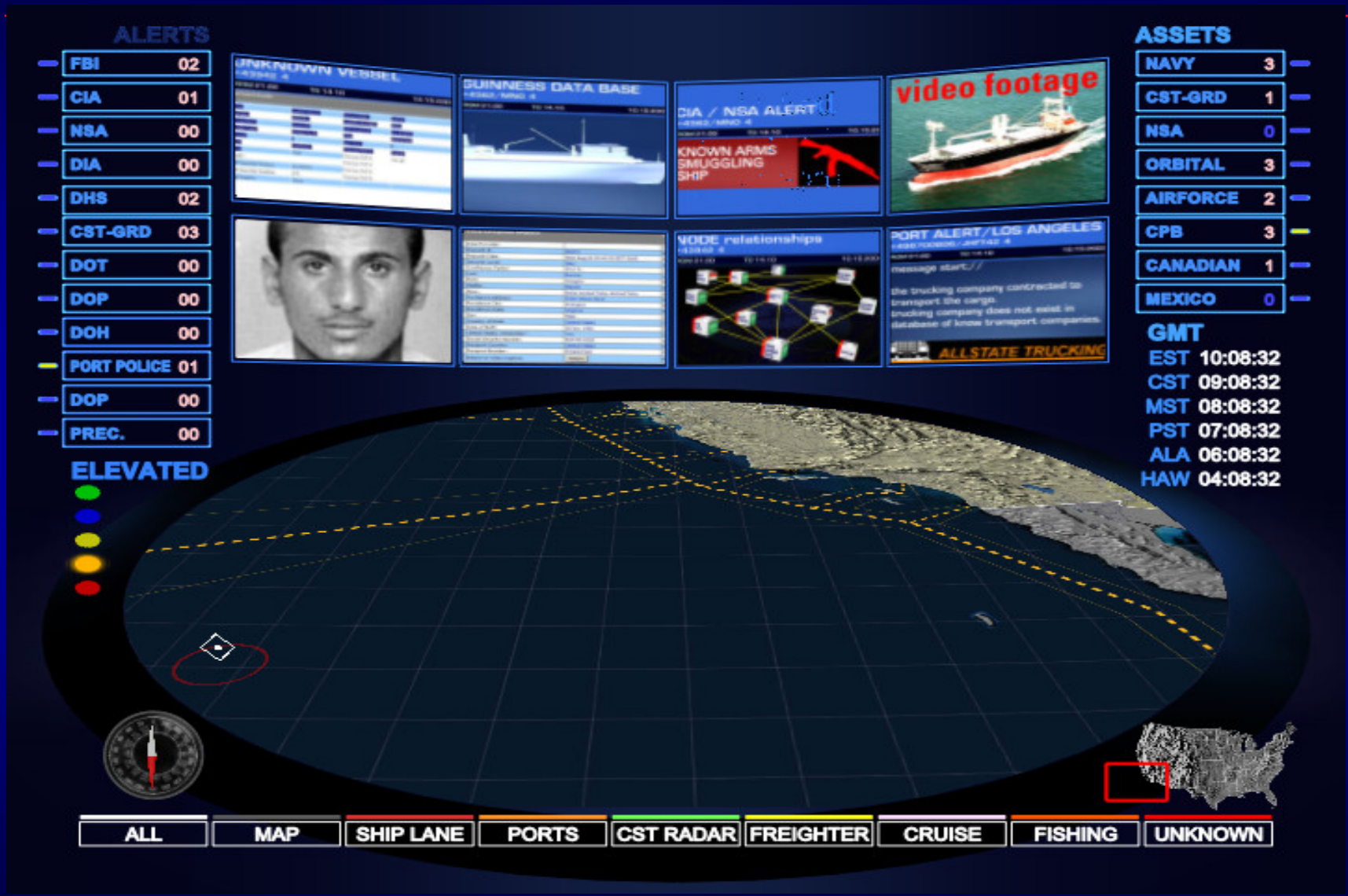
Algorithms



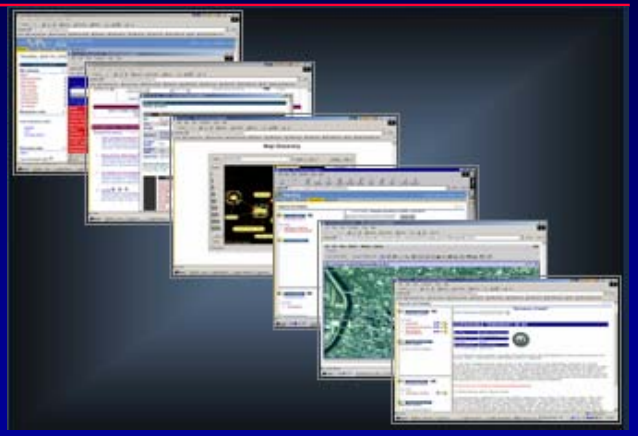
Knowledge Base



Common Operating Picture



Trusted Information Management Summary



Focus on innovation and mission needs

- Early and continuous User involvement, directly tied to initial deployment and spiral enhancements
- Use of commercial architectural practices emphasizes ease of use, ease of existing systems integration, and ease of new technology insertion

Quality, Timeliness and Productivity

- Enables rapid initial operating capability
- Deploys mission-specific configuration
- Captures and retains domain knowledge
- Supports analysis process consistency
- Promotes sharing tools, methods & results
- Automates data preparation
- Enhances overall awareness