Homeland Security
Information Sharing
Architecture

National Defense Industrial Association
Interoperability and Systems
Integration Conference
2 April 2003

William F. Dawson
Deputy Intelligence Community
Chief Information Officer
Agenda

- Objectives
- Approach
- Architecture
- Information Sharing
- Summary
Objectives

- Use existing capabilities and infrastructures to support the analytical and information dissemination needs of Homeland Security
- Provide actionable access to information
- Provide a roadmap for future system development which ensures interoperability across the Federal Government and beyond
Approach

- Interconnect a Homeland Security Community of Interest (COI) at each security level:
  - Top Secret SCI
  - Secret Collateral
  - Sensitive but Unclassified (SBU)

- Establish a governance process at each security level:
  - Policies
  - Standards
Intelligence Community System for Information Sharing (ICSIS)

- Provides the enterprise capabilities to store, manage and disseminate HS information using:
  - Joint Worldwide Intelligence Communications System (JWICS) for Top Secret connectivity
  - Secret Internet Protocol Routed Network (SIPRNET) for Secret connectivity
  - Open Source Information System (OSIS) for Unclassified/SBU connectivity
Intelligence Community System for Information Sharing (ICSIS)

- Provides the controlled interfaces to securely transfer HS data to analysts at lower security levels
- Provides a governance structure for sensitive compartmented information
IC PKI provides identification and authentication for HS COI users.

DoD PKI provides identification and authentication for HS COI users.

Commercial PKI provides identification and authentication for HS COI users.

SCI Network (JWICS)  Collateral Network (SIPRNET)  Unclassified Network (OSIS)
TS/SCI Infrastructure

- Managed by the Intelligence Community
  - Takes full advantage of the existing ICSIS and Comms infrastructure
  - CT-Link provides an existing operational Secure Community of Interest:
    - Profiled cable/message reports/traffic
    - Community products (Warnings, Assessments)
    - Community databases
      - Examples: State, FBI, CIA, etc.
    - E-Mail
    - Tailored Forums (bulletin boards)
Collateral Infrastructure

- Managed by Defense Department (and others)
  - Takes full advantage of the DoD’s existing Secret infrastructure
  - Takes full advantage of Secret version of Intelink
  - Communities of Interest for Homeland Security can be established
  - One department (e.g., Defense) could lead a governance activity
Sensitive but Unclassified Infrastructure

- Managed by Department of Homeland Security (and others)
  - Takes full advantage of the existing Federal Government infrastructure, including
    - DOJ/FBI’s Law Enforcement Networks
    - DoD’s Unclassified Networks
    - State’s SBU Networks
    - IC’s Unclassified Networks
  - Communities of Interest for Homeland Security can be established
  - One Department (e.g., DHS) could lead a governance activity
Homeland Security Information Sharing

Information Flow
- Sources and Methods
- Sensitive Data
- Actionable Data

Data
- Foreign Intelligence
- Military and other Secret Level
- Law Enforcement and Domestic

Participants
- IC Analysts
- DoD Operators
- LE and Domestic Agencies

Governance
- IC
- DoD +
- DHS +
Summary

- Existing operational capabilities and IT infrastructures can and are being leveraged to support the analytical and information dissemination needs of DHS
- Actionable information and connectivity is required at three distinct security levels
- Coordinated governance processes will facilitate timely exchange of Homeland Security information