

State, Local and Tribal Fusion Center Identity, Credential and Access Management Requirements

Dr. Clark Smith
Executive for Programs and Technology
Information Sharing Environment (ISE)
www.ise.gov

ArchitecturePlus Seminar
June 16th, 2010

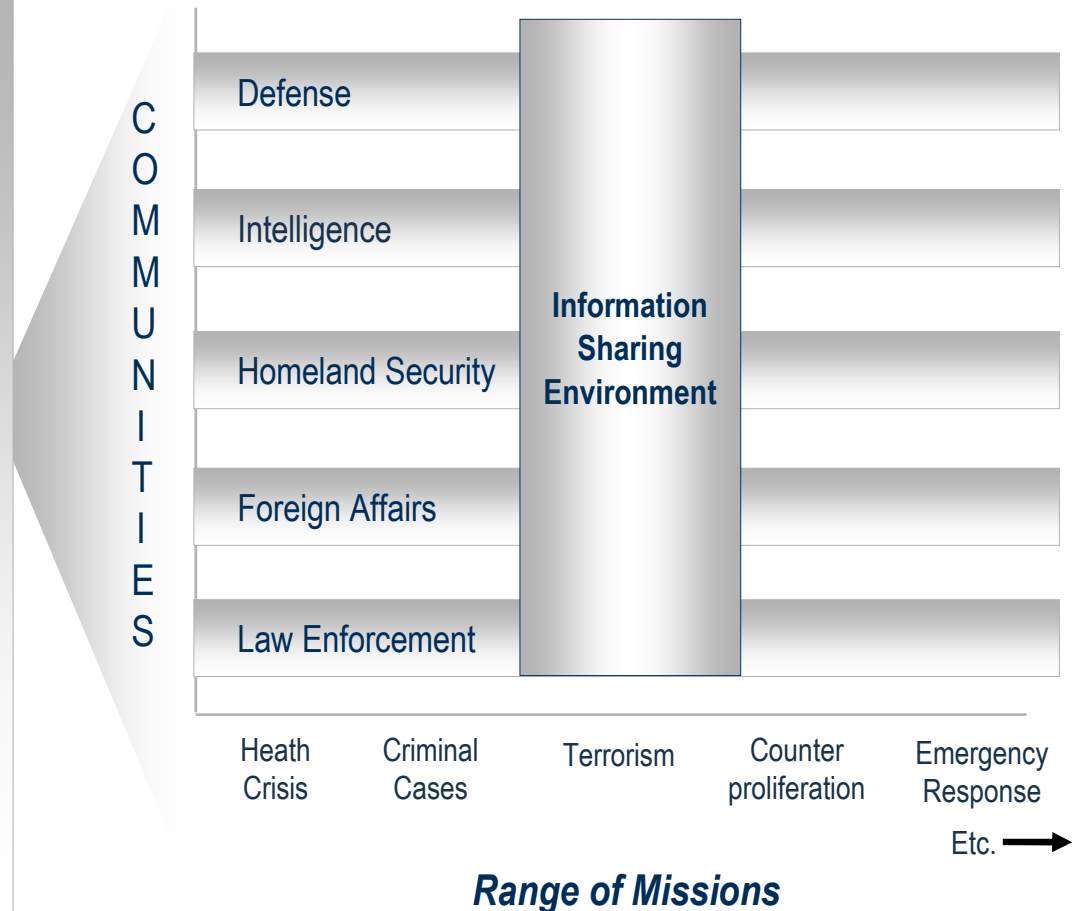
Agenda

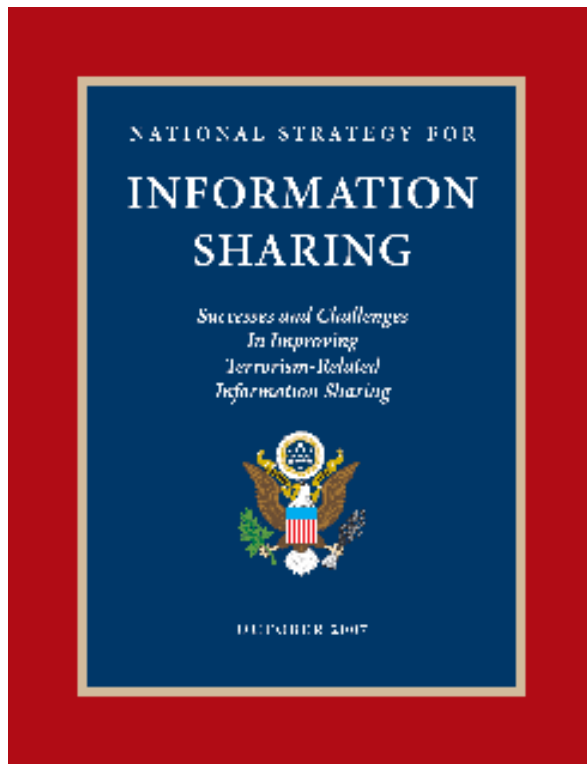
- Background
- ISE Priorities
- ISE and ICAM
- SBU Interoperability

Information Sharing & Collaboration – Congressional & Presidential Priority

Information Sharing Environment

- ✓ *Established 2004, 9/11 Commission Reforms*
- ✓ *Purpose: align and leverage existing policies, business processes, technologies, systems, and promote a culture of information sharing*
- ✓ *Terrorism, Homeland Security, and WMD Information & Law Enforcement Information relating to Terrorism.*
- ✓ *Protects the information privacy and other legal rights of Americans*
- ✓ *Controls access to data - not systems & networks*
- ✓ *Enhances accountability & oversight*
- ✓ *The largest, most developed information sharing environment in government, and the model for replication elsewhere in government.*
- ✓ *The Program Manager:*
 - ✓ *Facilitates Development of the ISE*
 - ✓ *Serves as the “honest broker” to all stakeholders*
 - ✓ *Authority for common ISE standards for Federal and non-Federal participants*





- Released October 2007 in close coordination with federal, state, local and private sector partners
- Prioritizes & unifies the Nation's efforts to advance the sharing of terrorism-related information
- Ensures those responsible for combating terrorism & protecting local communities have access to the timely and accurate information they need
- Improving information sharing with state, local & tribal governments and the private sector is critical

ISE Priorities

Common framework for sharing information across Federal, State, local, and tribal governments and the private sector.

- **National Integrated Network of State and Major Urban Area Fusion Centers** operating at a baseline level of capability.
- A nationwide approach to **Suspicious Activities Reporting**.
- **Network Interconnectivity**
- Framework to Share **Unclassified Information** that needs to be **controlled**
- **Privacy & Civil Liberties** is a foundational requirement across all priority areas.

The PM-ISE convenes all relevant parties to identify solutions; provides oversight; and supports implementation through development of mostly common standards, policies and business processes.

SLT and Private Sector Participation

- The ISE Strategy recognizes state, local, tribal (SLT) and private sector entities are critical to our Nation's efforts to prevent terrorist attacks.
- A number of ISE projects support the improvement information sharing with SLT and private sector organizations, including: Nationwide SAR Initiative, Fusion Centers, Interagency Threat Assessment and Coordination Group at the National CounterTerrorism Center.
- Fusion Centers are considered the ISE's primary focal points within the State and local environment.
- To work with SLT and Private Sector Partners, the ISE leverages:
 - Federal Government Advisory Councils: GLOBAL Justice / Criminal Intelligence Coordinating Council; DHS Homeland Security Advisory Council,
 - National Law Enforcement Associations: International Association of Chiefs of Police, Major Cities Chiefs Association, National Sheriffs' Association
 - National Fusion Center Association
 - National Governors Association's Governor's Homeland Security Advisors Council
 - National Conference of State Legislators
 - Critical Infrastructure Sector Partnership Structure
 - US Chamber of Commerce

ISE Priority Projects: *Progress Made but More to Do....*

- **SAR:** Nationwide Suspicious Activity Reporting Initiative (NSI) Program Management Office (PMO) was established at DOJ earlier this year to support State, Local, and Federal Agencies participating in the NSI.
- **Fusion Centers:** Last month, a National Program Management Office was established at DHS to assist the development of a national, integrated network of fusion centers operating at baseline level of capability. The PM-ISE, in partnership with the new PMO, is currently conducting a network-wide baseline capability assessment and gap mitigation project.
- **Controlled Unclassified Information**
- **Data Standards, Architecture & Enabling Technology:** NIEM; Identity/Access Management; Unclassified, Classified Network Interconnectivity, etc.

Why PM-ISE Cares About IdAM

- The 72 recognized Fusion Centers require access to national security and public safety information on certain federal systems
 - Expansion of CAC/PIV and other credentials to further control access to data and sites has a major impact
 - Access control decisions can have major consequences for non-Federal partners
 - Fusion Centers have a legitimate need to access multiple assets and sources of information on a variety of Federal Networks
- Fusion Center Connectivity is a Top Priority
 - Sensitive But Unclassified (SBU) / Controlled Unclassified Information (CUI)
 - Secret

PM-ISE Activities in the IdAM Space

- Information Sharing and Access Interagency Policy Committee, Information Standards and Architecture (ISA) Sub-IPC Task 4: Track and Support Coordination of Identity, Credential and Access Management (ICAM) Efforts (ICAM Documents are available at www.idmanagement.gov)
- Privilege Management and Data-Level Access Control Pilot
- SBU/CUI Interoperability

SBU Interoperability Initiative

- **Consistent with the SBU/CUI Interoperability Initiative Segment Architecture**
- **Specific network interoperability capability**
 - ✓ Single sign-on for access to all SBU/CUI networks.
 - ✓ Access across SBU/CUI networks including provisions for federated search.
 - ✓ Secure electronic mail between SBU/CUI networks.
 - ✓ Common collaboration tools used jointly across SBU/CUI networks.”

Challenges for Sharing

1. Search capability:

By resource versus domain-wide

2. Security philosophy:

If you're not currently authorized to access the data,
are you entitled to know it exists?

3. Access methodology

Is a resource enabled for web-access or not?

4. Access controls

Determined by user role versus resource owner

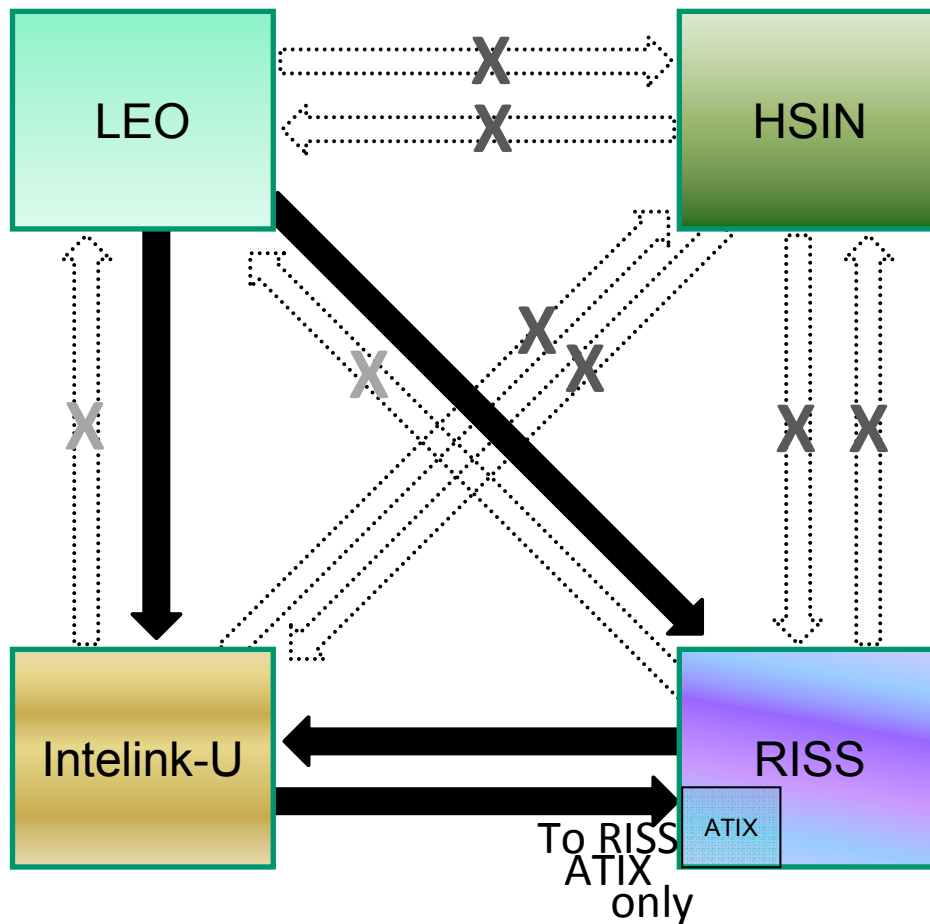
SIGs/COIs/Hosted Sites/Resource Permissions

System/ Network	SIGs/COIs/ Hosted Sites	Access Control
LEO	760+	<ul style="list-style-type: none"> • “Moderators” establish SIGs. • Access specified by user name and password. • Moderators also clear items put into the SIGs.
Intelink-U	738	<ul style="list-style-type: none"> • Share by default; limit by exception. • Organization producing data is accountable for managing, maintaining and controlling its products. • Site owner can limit access to its data via Intelink Passport.
RISSNET	600+ ¹	<ul style="list-style-type: none"> • Certain resources available via RISSNET are available to all authorized, vetted RISSNET law enforcement users and are controlled via group permission. • Certain resources available via RISSNET are available to all authorized, vetted RISSNET users, such as the ATIX Program resources, and are controlled via group permission. • All resource owners with resources available for access via RISSNET control the level of access to their resource. Control is exercised via individual access permissions and/or group permission which can be administered by the resource owner.
HSIN	690+ ²	<ul style="list-style-type: none"> • Sponsors Establish National and Regional COI’s and Define Governance • Users are Nominated and Validated into one or more COIs/Sub-COIs • Automated Identity Proofing Validates Initial Access to HSIN Portal and COIs • Tiered Authentication (User Name and Password +, NIST Level 3 Compliance) • User profile based access control to content viewing and dissemination • HSIN offers federated search, notification about new/updated documents and RSS feeds • HSIN will treat information queries from federated partners the same as searches originated by full HSIN members, based on the personal attributes of the requestor

30/60/90 Day Quick Win Projects

Title	Goal/Outcome
SBU User Requirements	<ul style="list-style-type: none"> -Identification of the challenges/frustrations/issues for Users -Common set of User requirements
SAR-DHS	<ul style="list-style-type: none"> -Federate DHS data into the Nationwide SAR Initiative
Protected E-Mail Exchange	<ul style="list-style-type: none"> -Enhanced capability to protect emails with sensitive content <ul style="list-style-type: none"> -Rerouting of email to leverage capabilities of other systems -Plan of action for recognized gaps, if any -User awareness of email vulnerabilities and handling options
White Pages and Service Directories	<ul style="list-style-type: none"> -White Pages and Directories of Network Services made available to users on other domains (Some releasability policies being addressed)
Shared Services	<ul style="list-style-type: none"> - Retain today's cross - domain access to services -Begin granting temporary access to FBI's Virtual Command Center
1-800-Help-Desk	<ul style="list-style-type: none"> -Help Desks work problems in association with each other -Help Desks receive basic training to recognize cross domain problems -Standard troubleshooting scripts developed for cross -domain use -Help Desk personnel stay with User until problem area is identified and issue is successfully handed off to appropriate experts -Table top exercise with scenarios

Current + 90 Day Environment



- Users will see by mid-July
- DHS data in NSI through RISS
 - Protected email exchange and training on-line
 - Sharing of White Pages and Directory of services
 - Sharing of LEO's VCC service
 - 1-800-Help-Desk for Interoperability

Long term pacing items to address "X's" will be addressed in the 90+ timeframe