



The Information Sharing Environment: Lessons Learned for Environmental Management

US EPA Environmental Information Symposium
“Transforming Information into Solutions”

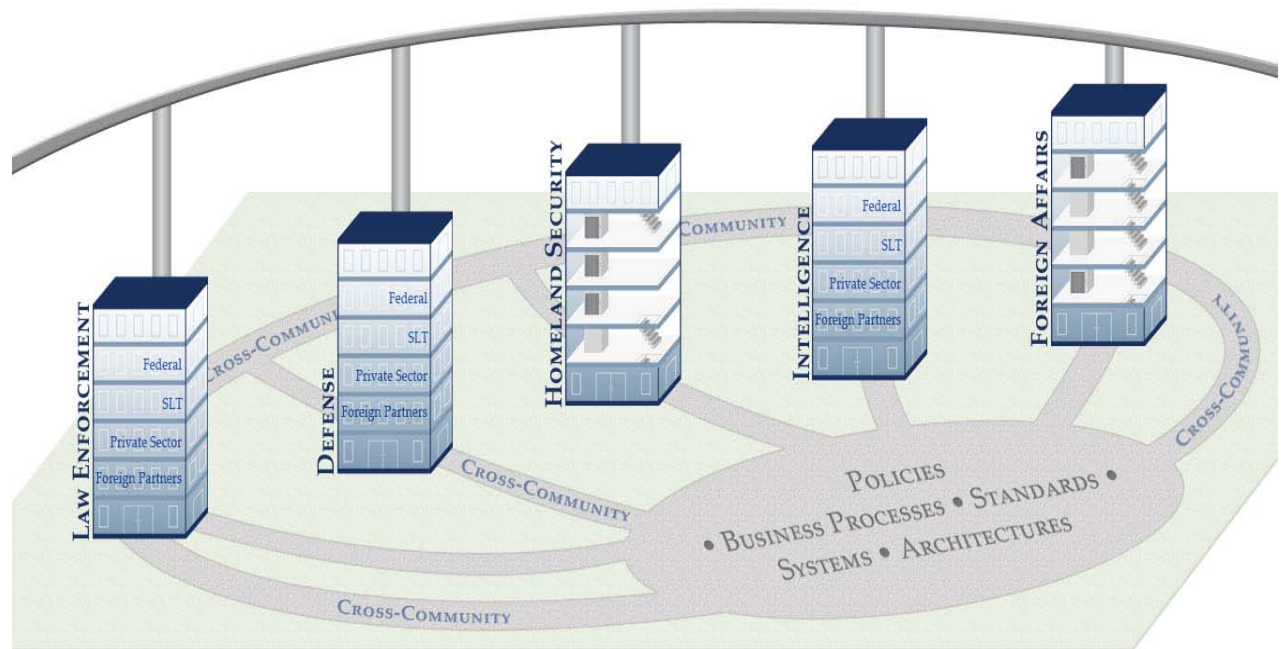
Ambassador Thomas McNamara

**Phoenix, AZ
December 11, 2008**

- Multiple Communities of Interest
- Multiple User Types
- Multiple Governmental and Non-governmental Entities

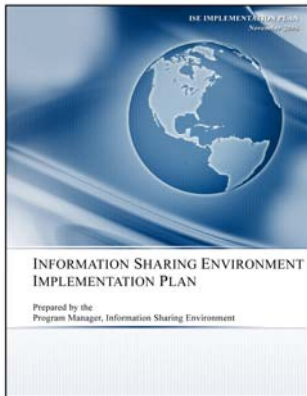


The Information Sharing Environment



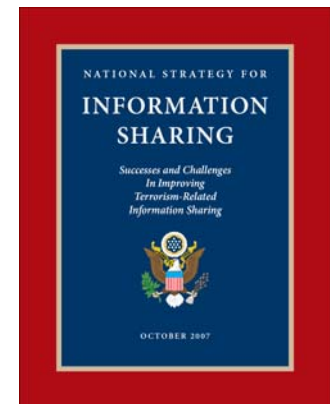
- Defined in Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 as amended (IRTPA), the ISE is ...

“an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section.”



- *ISE Implementation Plan* (Nov 06) established a vision, strategic goals, and implementation activities for the ISE.

- *National Strategy for Information Sharing* (Oct 07), prioritizes and unifies the Nation’s efforts to advance the sharing of terrorism-related information.



- **Lesson 1: Changing the business culture is the biggest challenge**
- **Lesson 2: “Mostly Common” standards and rules are the building blocks of Change**
- **Lesson 3: Let the Federal system work for you**
- **Lesson 4: Privacy and Security must both be part of the solution**

EXAMPLES OF IMPROVEMENTS

- 1. Controlled Unclassified Information (CUI)**
- 2. State and Major Urban Area Fusion Centers**
- 3. Private Sector Information Sharing**
- 4. Suspicious Activity Reporting**

1. Controlled Unclassified Information



**Current SBU Environment
(107 Markings)**

New CUI Framework

**CUI
Controlled / Standard**

Sensitive but unclassified (SBU) information is shared today according to an unregulated and diverse body of policies and practices that confuse both its producers and users. Current sharing practices not only impede the timeliness, accuracy, and ready flow of terrorism formation that should be shared, but often fail to control the flow of information that should not be shared. Sensitive but unclassified (SBU) information is shared today according to an unregulated and diverse body of policies and practices that confuse both its producers and users.

**CUI
Controlled / Specified Dissemination**

Sensitive but unclassified (SBU) information is shared today according to an unregulated and diverse body of policies and practices that confuse both its producers and users. Current sharing practices not only impede the timeliness, accuracy, and ready flow of terrorism formation that should be shared, but often fail to control the flow of information that should not be shared. Sensitive but unclassified (SBU) information is shared today according to an unregulated and diverse body of policies and practices that confuse both its producers and users.

**CUI
Controlled Enhanced / Specified Dissemination**

Sensitive but unclassified (SBU) information is shared today according to an unregulated and diverse body of policies and practices that confuse both its producers and users. Current sharing practices not only impede the timeliness, accuracy, and ready flow of terrorism formation that should be shared, but often fail to control the flow of information that should not be shared. Sensitive but unclassified (SBU) information is shared today according to an unregulated and diverse body of policies and practices that confuse both its producers and users.

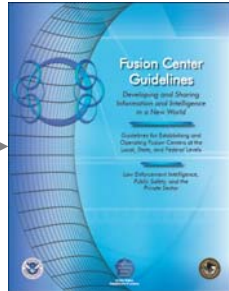
2. State & Major Urban Area Fusion Centers

Vision – Goals – Strategy – Roles and Responsibilities – Baseline Capabilities



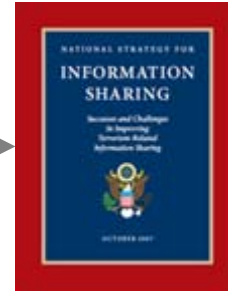
DOJ/GLOBAL, Oct 2003

Road map for criminal information sharing



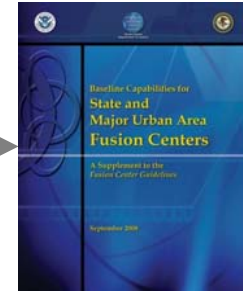
GLOBAL, Aug 2006

Fusion Center Guidelines
All Crimes - All Hazards



National Strategy, October 2007

Federal, State & local roles/responsibilities to incorporate fusion centers into the ISE



GLOBAL, Sept 2008

Baseline Capabilities Guidance for Fusion Centers

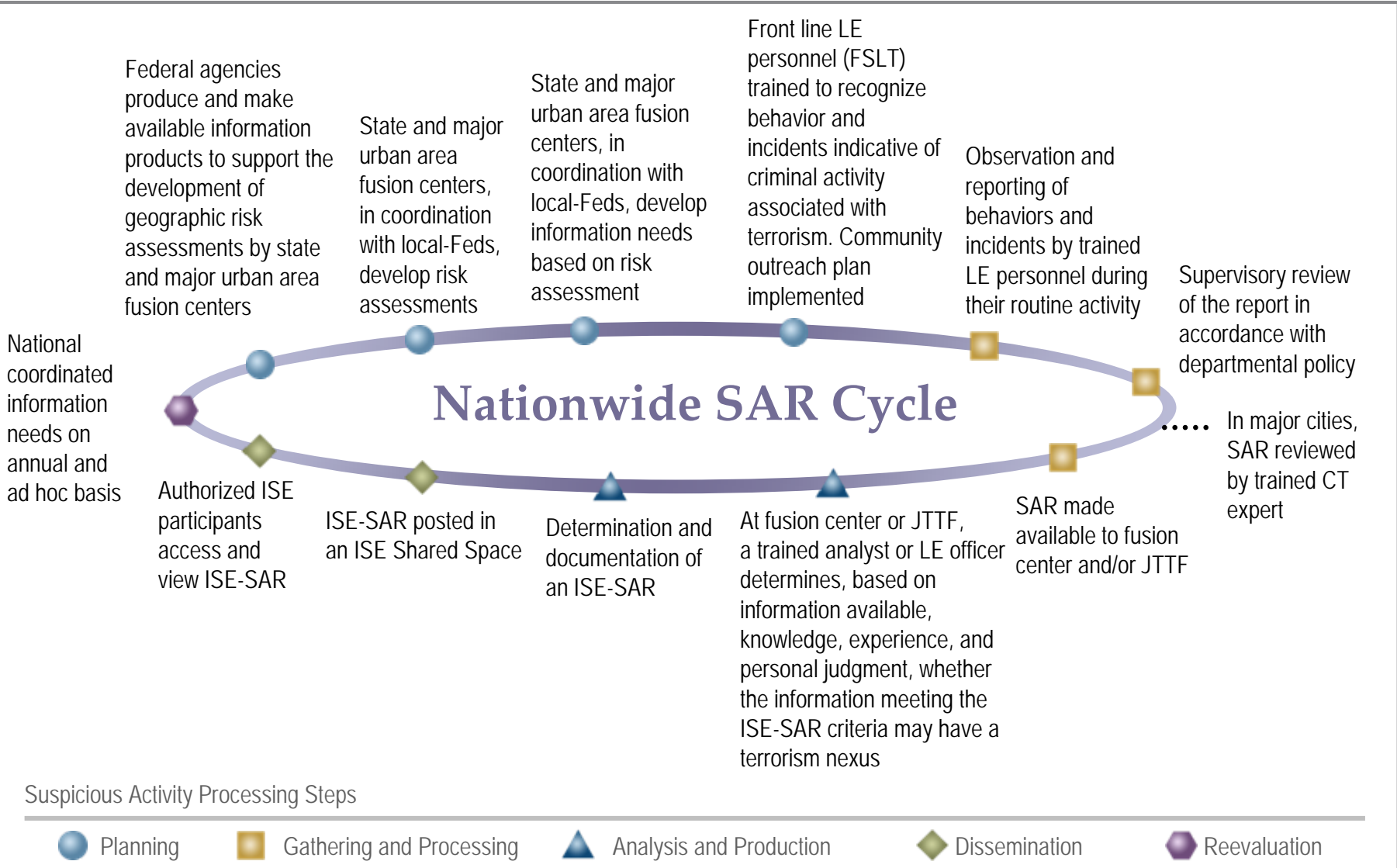
- Goal: Establish an Integrated, National Network of Fusion Centers
- Strategy's Appendix, developed jointly with State and local officials, identifies Roles and Responsibilities for establishing this Integrated Network
- Fusion Centers will serve as the primary focal points for the receipt and sharing of terrorism-related information
- Federal Government is providing support to fusion centers to achieve a baseline level of capability
- Baseline Capabilities Guidance Released Sept 2008; may take 5 years to achieve

3. Private Sector Information Sharing

- 85 % of Critical Infrastructure and Key Resources (CIKR) owned or operated by Private Sector
- CIKR Sectors' ISE – Being Implemented by DHS, Office of Infrastructure Protection
- 2 Primary Mechanisms
 - Sector Based Partnerships – 18 Sectors including Drinking Water and Water Treatment Systems
 - Regionally-Based Sharing Partnerships – Federal Government is encouraging fusion centers to support CIKR Information Sharing needs.



4. Suspicious Activity Reporting



- 1. Modernizing Identity Management and Access**
- 2. Creating Mostly Common Processes & Standards**
- 3. Maintaining and Enhancing Privacy & Legal Rights**
- 4. Abolishing SBU and Implementing CUI**
- 5. Ending Risk Aversion & Mandating Risk Management**

Ambassador Thomas McNamara

Program Manager, Information Sharing Environment

(202) 331-2490

www.ise.gov