National Security Through Responsible Information Sharing

Kshemendra Paul
Program Manager, Information Sharing Environment
September 2015
**Nationwide Challenges**

- Evolving & Converging Threats & Risks → National Approaches to Interoperability
- Collaboration Imperative → Common Operating Models
- Strengthening Legitimacy → Consistent, Transparent, & Distributed Policies
- Enterprise Data Management → Integrated Capabilities & Shared Services

Diagram notes:
- Critical Infrastructure Sectors
- International Standards Organizations Creating Interoperability Standards
- Standards Coordinating Council (SCC) Members
- Regional Information Sharing System (RISS) Centers
- Law Enforcement Agencies
- Suspicious Activity Reports Filed Annually
- White House Policy Committee
- Fusion Centers
- High Intensity Drug Trafficking Areas (HIDTAs)
- Sworn Law Enforcement Officers
- Intelligence Community Agencies
- Statewide ISEs
- 780,000
- 18,000
- Suspect
- 1
- 4
- 17
- 4
- 6
- 14
- 16
- 28
- 4,800
ISE Mission Portfolios

Statewide & Regional ISE

Cybersecurity Information Sharing

Watchlisting, Screening, & Encounters

Domain Awareness

Transnational Organized Crime

Incident Management
Scope of the ISE

Information Sharing Environment (ISE)

Frontline
- Investigators
- Analysts
- Operators

Communities
- Diplomacy
- Homeland Security
- Intelligence
- Defense
- Law Enforcement

Mission Partners
- International
- Federal
- State
- Local
- Tribal
- Private Sector

Information Technology Industry
PARTNER ENGAGEMENT TO ADVANCE THE ISE

MISSION PARTNERS

Advancing implementation of the NSISS

CICC
CRIMINAL INTELLIGENCE COORDINATING COUNCIL
Supporting federal, state, and local law enforcement and homeland security agencies

SCC
STANDARDS COORDINATING COUNCIL
Developing information sharing and safeguarding standards
Build Interoperable Services

Discover Interoperable Services

Extend Interoperable Services

Build on

Authorities, Governance & Policy, Performance Management, Budget and Resourcing, Communications & Outreach

Capabilities

- Architecture Alignment
- Attribute Exchange
- Common Profile
- Data Aggregation (DARA)
- Exchange Patterns
- Geospatial (GIRA)
- Identity and Access Management
- Maturity Model
- National Information Exchange Model
- Reference Architecture
- Standards and Specification Framework
- Springboard

www.standardscoordination.org
Upcoming International Events

OGC Technical Planning Committee
Sept. 14-18, 2015
Nottingham, England

OGC 12th Plenary Session of the Group on earth Observations GEO (XII)
Nov. 11-13, 2015
Mexico City, Mexico

OGC Technical Planning Committee
Nov. 30 - Dec. 4, 2015
Sydney, Australia

For more information: http://www.standardscoordination.org/events.
OASIS Shapes Future of STIX, TAXII, CybOX

- Develop and promote STIX, TAXII and CybOX to enable cyber threat intelligence sharing
- Share threat information, address physical intrusions and perform attack mitigation planning
Fusion Center Cyber Pilot

- **Kick-off Event (February 2013):** Cybersecurity Evaluation Environment Meeting

- **Pilot (May 2013-2015):** Collected and analyzed cybersecurity information sharing requirements from five fusion centers

- **Outcome: (May 2015):** Developed a fusion center cyber capability addressing information collection, sharing, and intelligence analysis
Law Enforcement Cyber Center

- Launched: May 18, 2015
- One-stop shop for cyber-related information
- Vetted and easily accessible
- Facilitates training, provides technical assistance, encourages collaboration
- For more information: http://www.iacpcybercenter.org/about-the-cyber-center/
Visit ISE.gov
Backup Slides
Perceived cybersecurity threat

- ISIS and ISIS-styled attacks abroad
- Similar attempts domestically

Increased investment in cyber at the S/L level

- Capacity building in
  - Social media
  - Cyber-based CI
  - Cyber threats to critical infrastructure

Growth in S/L LE conducting operations in cyberspace

- Real-time social media analysis to inform operations
- Spot/assess/recruit in cyberspace
- Authorized offensive cyber operations

Increased risk of operational fratricide in cyberspace

- Compromise/exposure of ongoing investigations

Current deconfliction framework needs to integrate cyber-related information before new cyber operators come on line
Standards Coordinating Council Meetings 2015-2016

2015:
• OMG Technical Meeting – Sept. 21-25
• SCC Meeting at OMG Technical Meeting – Sept. 24
• ACT-IAC Executive Leadership Conference – Oct. 25-27
• Port Security Operations Conference & Expo – Nov. 10-12
• OGC Technical Planning Committee – Nov 30-Dec. 4

2016:
• IJIS Institute National Symposium – Jan. 19-21
• Workshop on Informational Sharing & Safeguarding Standards (WIS3) – March

http://www.standardscoordination.org/events
Structured Threat Information eXpression - STIX

- Structured language for cyber threat intelligence information
- STIX use cases include:
  - Analyzing cyber threats
  - Specifying indicator patterns for cyber threats
  - Managing cyber threat prevention and response activities
  - Sharing cyber threat information
- Community-driven solution, providing structured representations of cyber threat information
  - Expressive, flexible, extensible, automatable, and readable
- Enables sharing of comprehensive, rich, “high-fidelity” cyber threat information across organizational, community, and product/service boundaries

Show NIEM/STIX alignment
+Talking points only on threat risk
The Cyber Integration for Fusion Centers document is an appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers. This document identifies recommended actions and guidance for Fusion Centers to integrate IT, cyber security, and cybercrime prevention and intelligence analytical capabilities.
Law Enforcement Cyber Center

• Addresses needs of Chiefs of Police and decode cyber security by providing resources across job types and job functions

• Intended outcome is to identify methods to link existing agency cybercrime units with regional/national cybercrime operational groups such as the FBI’s Cyber Task Forces

• Will assist law enforcement in providing prevention, education, and information to citizens who are likely targets of cybercrime