National Security
Through
Responsible
Information Sharing

Michael Howell
Principal Deputy Program Manager,
Information Sharing Environment
May 2015
SCOPE OF THE INFORMATION SHARING ENVIRONMENT (ISE)
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

300+ million
People

750,000+
Officers

18,000
LE Agencies

1.2 million
Firefighters

250,000
911 Operators

18 CI/KR Sectors

*Numbers are estimates

78 Fusion Centers

6 RISS Centers

28 HIDTAs

FBI

NCIJTF • CJIS • FIGs • JTFs • JIRGs • TSC

DHS

I&A • ICE • CBP • TSA • DNDO • NPPD

DOJ

ATF • DEA • USMS • OJP

Nets

Nlets

NCTC

JCAT

State

Air

Protection of Privacy, Civil Rights, and Civil Liberties
ISE MISSION PORTFOLIOS

Statewide & Regional ISE

Watchlisting, Screening, & Encounters

Transnational Organized Crime

Cybersecurity Information Sharing

Domain Awareness

Incident Management
**Value Proposition**

- **If we:**
  - Unify stakeholder communities’ requirements
  - Translate requirements into standardized information exchanges
  - Involve industry in development of standards-compliant solutions

- **Then we can:**
  - Build interoperability into solutions “off-the-shelf”
  - Increase the effectiveness and value of the solutions we purchase
  - Reduce total costs for both solution consumers and solution providers
The 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

the project is build upon

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

http://project-interoperability.github.io/
Geospatial Continuum

Federal Government  Whole of Government  Whole of Society

Industry

Safeguarding
Geospatial Capabilities

- Traffic cameras
- Sensors
- Windows, vessels, cargo, ...
- Web discovery/Social Media
- Security cameras
- UAV sensors/streaming video
- Weather feeds

Streams Video

Asset Information

Public Safety Tracking

Suspicious Activity

Models & Analysis
GEOSPATIAL INTEROPERABILITY REFERENCE ARCHITECTURE

Federal Enterprise Architecture

ISE Architecture Alignment

www.ise.gov/sites/default/files/GIRA.pdf
Cyber Threats and Challenges

- Advanced Persistent Threat (APT)
- Identity Theft
- Insider Threats
- Intellectual Property Threat and Corporate Espionage
- Internet of Things
- Mobile Malware and Botnets
- Phishing/Spearphishing
- Social Media
- Supply Chain Compromise
Executive Order 13636 “Improving Critical Infrastructure Cybersecurity” signed by President Obama February 2013:

• “Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.”

• “It is the policy of the U.S. Government to increase the volume, timeliness and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.”
The Perfect Storm

- Information Technology Is Increasingly Integral to Our Way of Life
- Technology Evolution Is Accelerating
- Every New Technology Brings New Vulnerabilities and Threats
- Technology Evolution, Vulnerabilities and Threats Are Outstripping Response Capabilities

Without Vigilance and Action, Our Way of Life is at Increased Risk
Cyber Information Sharing

- Standards Development
  - STIX and TAXII standards

- Threat and Risk Modelling
  - https://github.com/omg-threat-modeling/phase1
  - http://threatrisk.org/drupal/

- Enhancing Shared Situational Awareness
Visit ISE.gov