

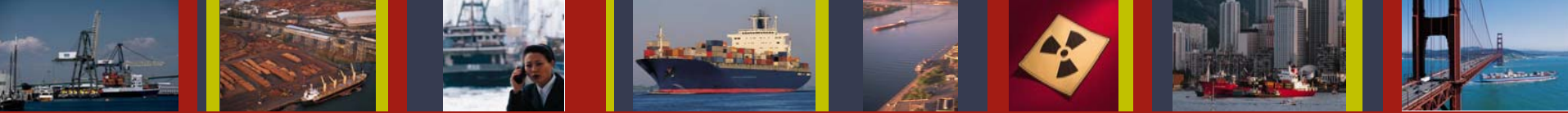
Changing the Security Paradigm: Interagency Sharing of Intelligence & Risk Assessment Data

Donald P. Bliss
National Infrastructure Institute
Portsmouth, New Hampshire, USA
14 March 2008



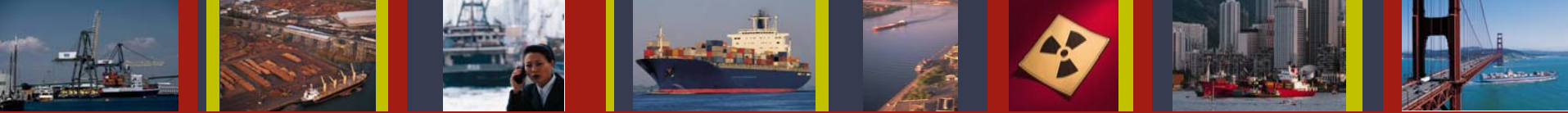
Definitions

- ***Intelligence***: information concerning an enemy or possible enemy.
- ***Fusion***: the overarching process of managing the flow of information and intelligence across all levels and sectors of government and private industry.



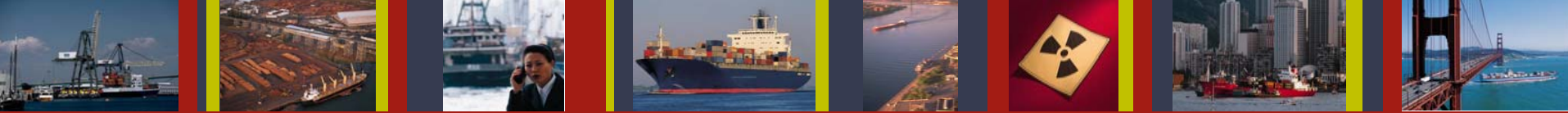
Definitions

- ***Fusion center***: the collaborative effort of two or more agencies that provide resources, expertise, and information with the goal of maximizing their ability to *detect, prevent, investigate* and *respond* to **criminal** and **terrorist** activity.



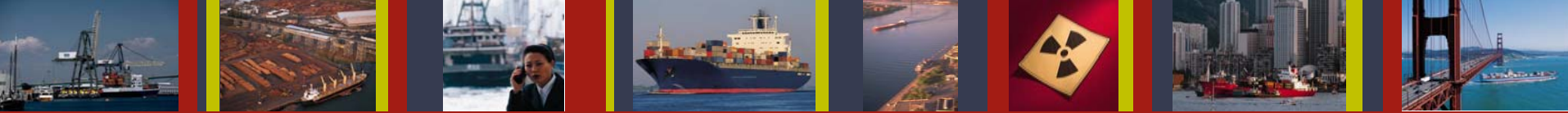
Targets

- In the U.S.:
 - 337 highway tunnels
 - 211 transit tunnels
- **Tunnels** are defined as “critical infrastructure”: i.e. systems and assets, both physical and cyber, so vital to the nation that their *incapacity* or *destruction* would have a debilitating impact on national security, national economic security and/or national public health and safety.



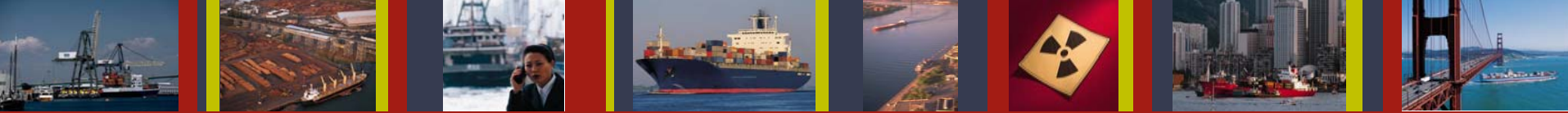
Factors affecting importance

- Location:
 - Population center
 - Economic center
- Impact of loss
- Cost, time to rebuild
- Vulnerability
- Iconic value
- Redundancy
- Interdependence with other sectors or key assets



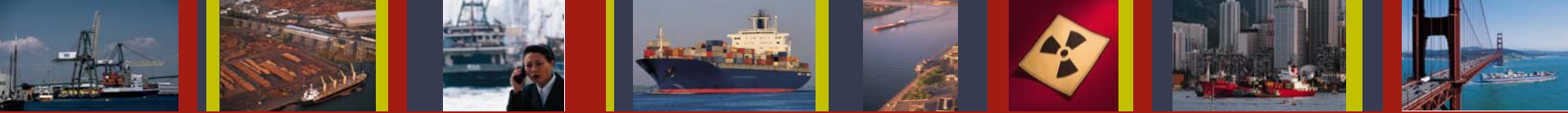
Potential Hazards

- Fire (unintentional)
- Structural Integrity Loss by Natural Causes
- Introduction of Hazardous Materials



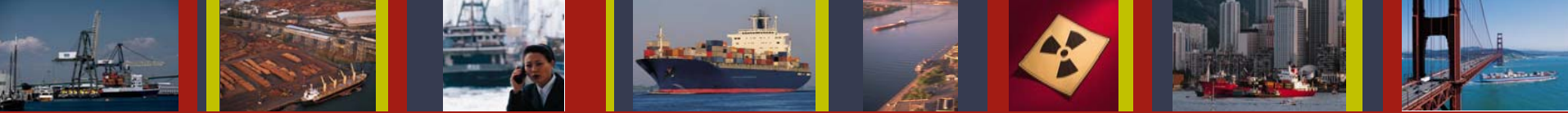
Potential Threats

- Explosives (small, medium, large)
- Chemical agents
- Biological agents
- Radiological agents
- Cyber attack
- Maritime incident
- Fire (arson)
- Sabotage of mechanical, electrical & communications



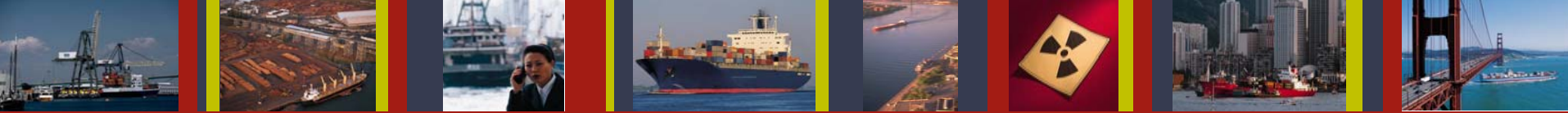
Possible Scenarios

- Use of explosives to cause collapse of tunnel
- Use of explosives to cause flooding of tunnel
- Hijacking of flammable liquids vehicle, causing catastrophic fire inside the tunnel
- Detonation of radioactive “dirty bomb” to contaminate tunnel and/or disburse radioactive material via the ventilation system.



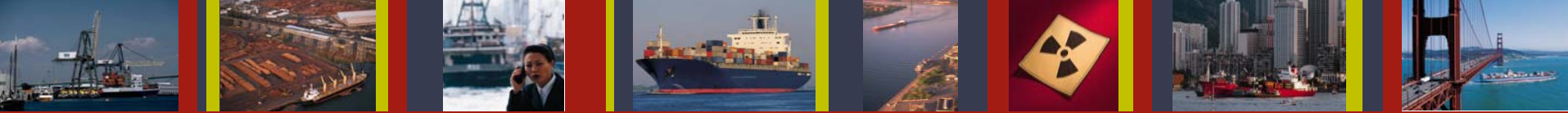
Possible Scenarios

- Release of toxic chemicals/gas in tunnel to harm occupants and/or disburse toxic material to a wide area via the ventilation system.
- Simultaneous attacks on bridges, tunnels and highway systems of a metropolitan area to shut down traffic flow in and out, thus immobilizing the economy.



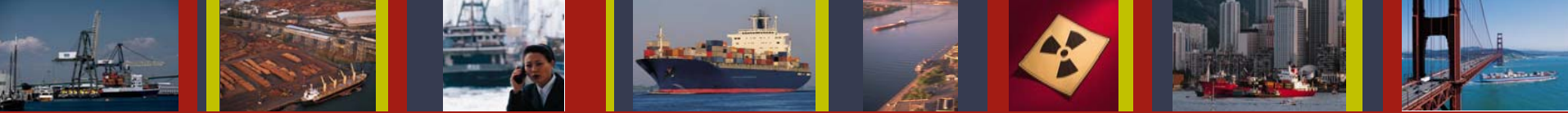
Possible Scenarios

- Attack critical weak point(s) such as ventilation system, electrical service, SCADA system.
- Use the “threat” of an attack on a tunnel to disrupt commerce, create fear, or extract concessions from a government for political or criminal gain (ransom, release of prisoners, change in policy, etc.)



Importance of Intelligence

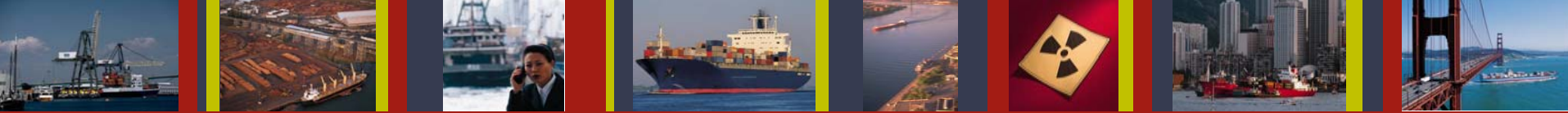
- Useful to law enforcement
- Useful to first responders
- Useful to tunnel operators
 - Deterrence
 - Detection
 - Defense



But to be useful.....

.....intelligence must be validated.

- Is the threat credible?
- Is the threat corroborated?
- Is the threat specific and/or imminent?
- How grave is the threat?



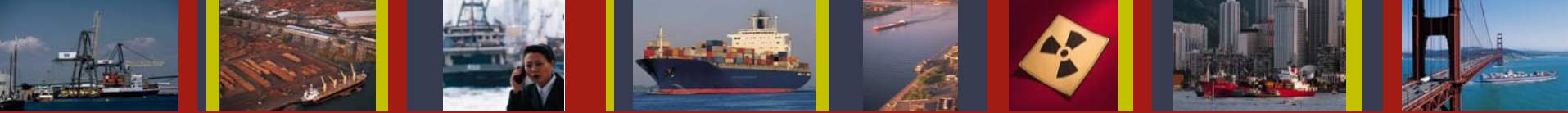
Intelligence Needs

- General threat data
- Threat data specific to the tunnel
- Threat data specific to nearby or interdependent infrastructure
- Supply chain data
- Pattern anomalies
- Behavior anomalies
- Employee background checks



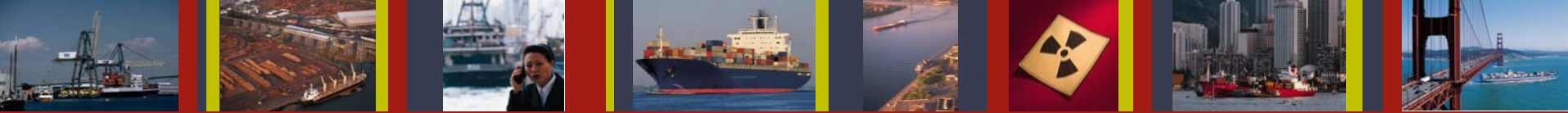
Intelligence Sources

- Law enforcement
- Intelligence community
- Employees
- Transportation/shipping industry
- General public
- Data feeds:
 - Video
 - Sensors



Information Sharing

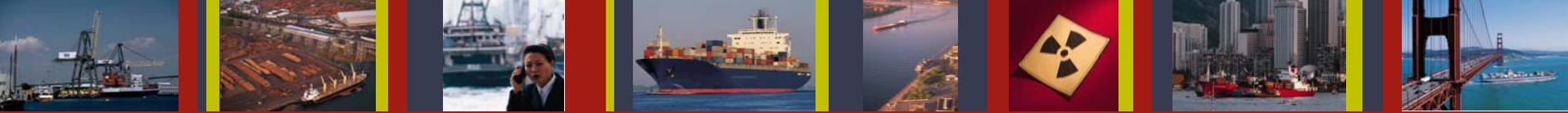
- Need to establish inter-agency and personal relationships
- Need to establish a culture for information sharing
- Need to establish a system for prioritizing information
- Need to develop a methodology for classifying/declassifying information and sharing it effectively



Fusion Center

- Multi-agency participation
- Receive and analyze threat data from multiple sources
- Provide assessments to assist in the deterrence, detection and response to terrorist events.



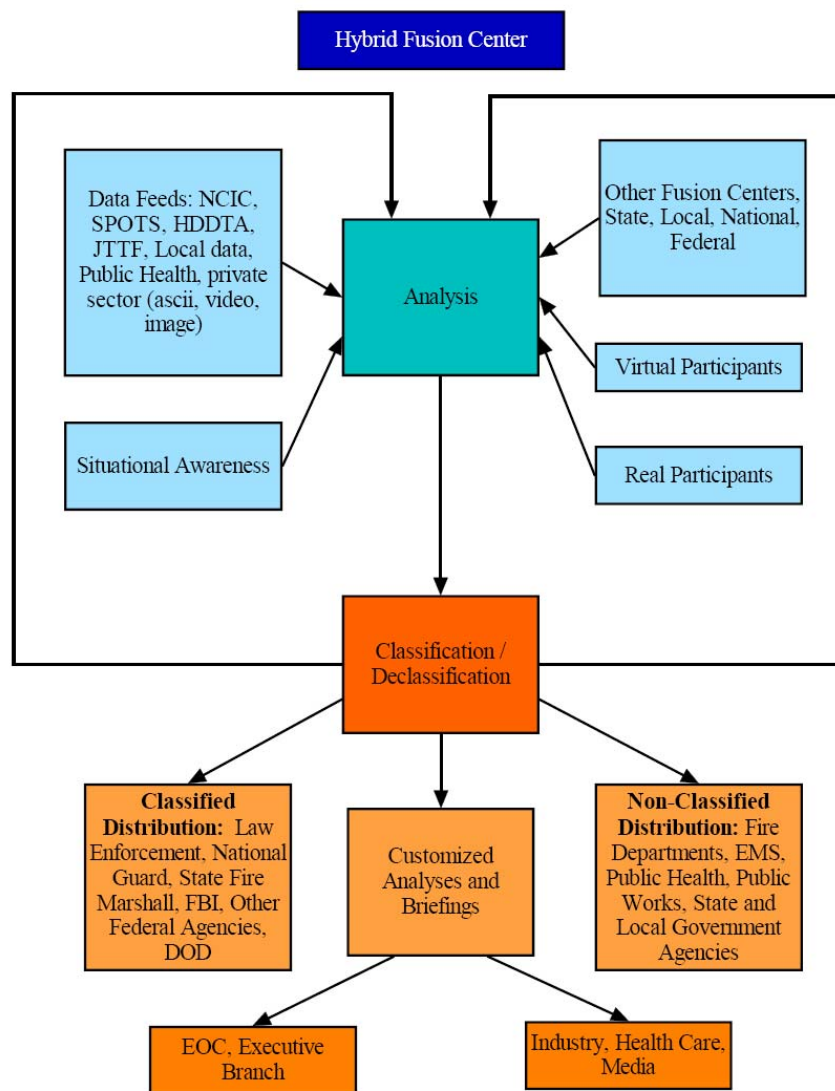


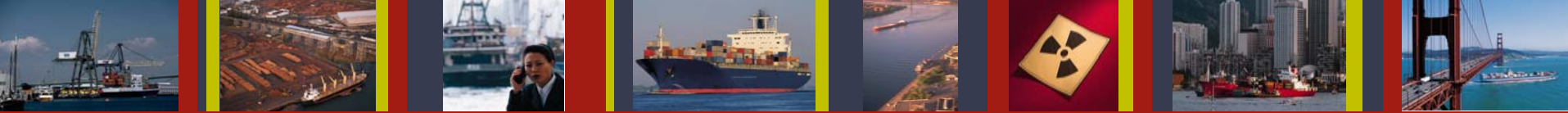
Problems

- Too much data?
- Inability to rapidly detect pattern anomalies
- Inability to receive data from multiple disparate sources
- Data privacy concerns, particularly with private sector data
- Who receives feedback?



Hybrid Fusion Center





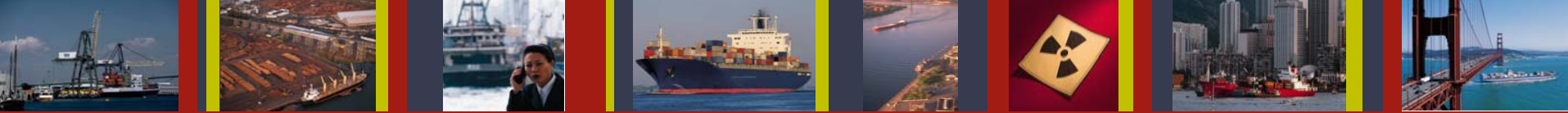
Data Management

- Establish meta-data system to
 - Parse data
 - Assign identifying meta-tags
 - Results in rapid assembly of data for analysis
 - “Google on Steroids”
- Pattern recognition capability
- Mask/encrypt proprietary data
- User defined screen views
- Receive data from any source: ASCII, image, video



Public-Private Partnership

- Need to maintain continuous, on-going relationship between law enforcement community and the tunnel operator.
- Establish trust
- Continually review intelligence needs
- Continually revise threat potential
- Need for “two-way” sharing of intelligence data and results



Questions?

Donald P. Bliss
+1 603 677 2480
dbliss@ni2.org