

Genesis 1



In the beginning God created the heavens and the earth.

God said, “Let there be light”, and there was light.

On the sixth day God created Man and gave Man dominion over the earth.

He did *not* give Man dominion over Man...



Fusion Centers

or

"I Spy" for the Intelligence Enterprise

Copyright OK-SAFE, Inc.™ Sept. 2009

NY Times: "Chicago Links Street Cameras to Its 911 Network" by Karen Ann Cullotta, 2/20/09 Photo: Joshua Lott/Reuters

Intelligence Enterprise

- **Intelligence:** (Criminal) the product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being , or known to be, criminal.
- **Enterprise:** An undertaking, esp. of some scope, complication, and risk. A business organization.
- **Information:** “classified and open source – is the **fuel** that powers intelligence.”

(Quote source: Vision 2015, p.14)

Chicago Fusion Center Training



Source: Jon's Photos

Fusion Center

Fusion Center: A collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorism activity.

Source: Recommended Fusion Center Law Enforcement Intelligence Standards March 2005

Define Terrorism

- **Terror:** *n.* great fear/a person or thing that causes great fear/a dreadful nuisance
- **The Terror:** the period of the French Revolution from the fall of the Girondists (1793) to the fall of Robespierre (1794), dominated by the ***Committee of Public Safety.***
- **Terrorism:** *n.* the policy of using acts inspiring terror as a method of ruling or conducting political opposition
- **Terrorist:** *n.* a person who favors or practices terror

American Terrorists...?

**“What we in America
call terrorists are
really groups of
people that reject
the international
system...”**

**Henry Kissinger
May 31, 2007 Conference
in Istanbul**



Domestic Terrorists...



Oklahoma Information Fusion Center



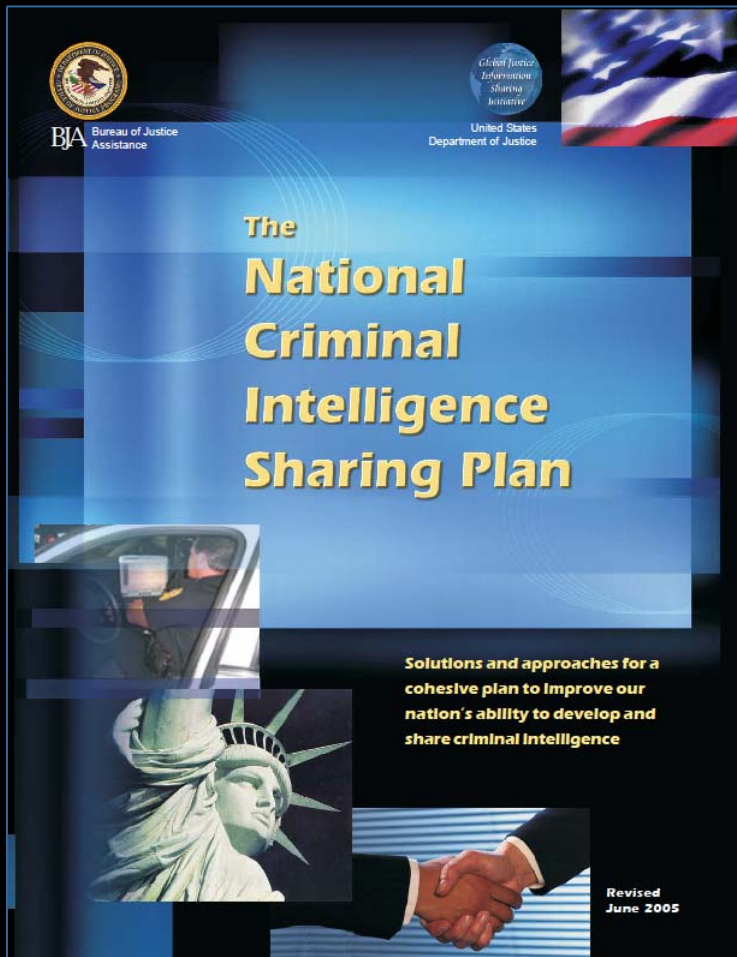
8/25/09

OIFC = Oklahoma Information Fusion Center



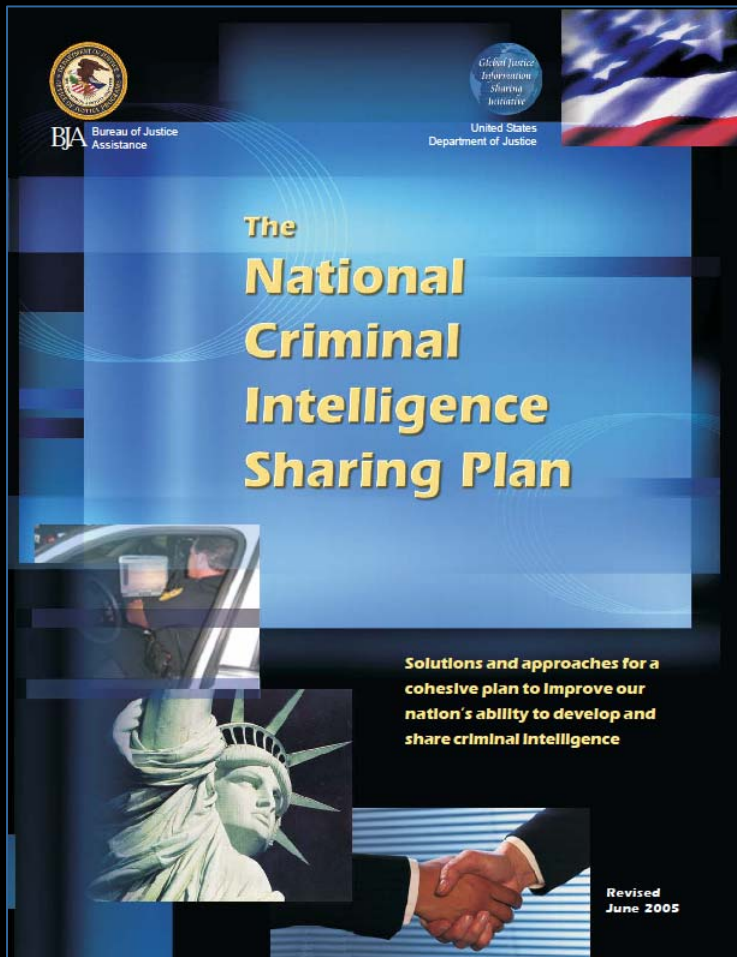
Oklahoma Information Fusion Center Tour

The NCIS Plan



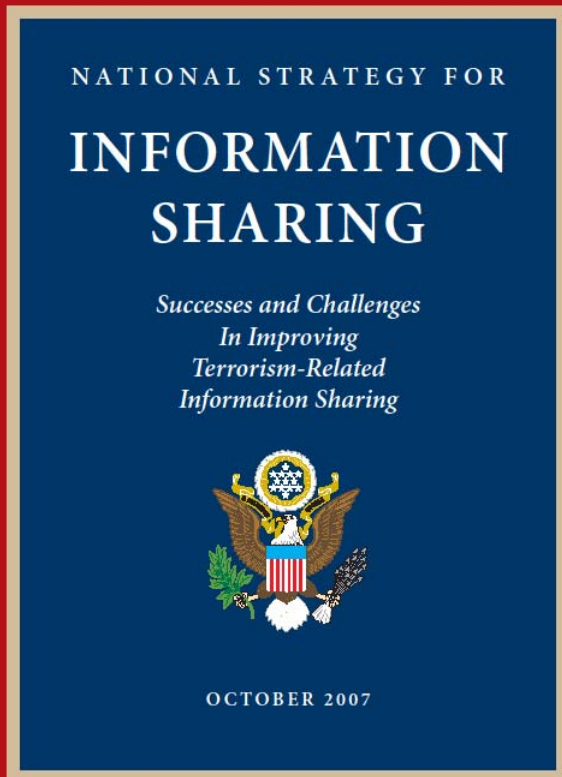
- “Developed” after 9/11/2001
- 2002 International Association of Chiefs of Police (IACP) Criminal Intelligence Sharing Summit
- Goal: Gathering information, producing intelligence (referred to as *product*)

The NCIS Plan



- **Global Justice Information Sharing Initiative – (*Global*)**
- **Global Intelligence Working Group (GIWG)**
- **Global Extensible Markup Language**
- **Set standards for *intelligence-led policing***
- **Interoperability of existing communication systems**

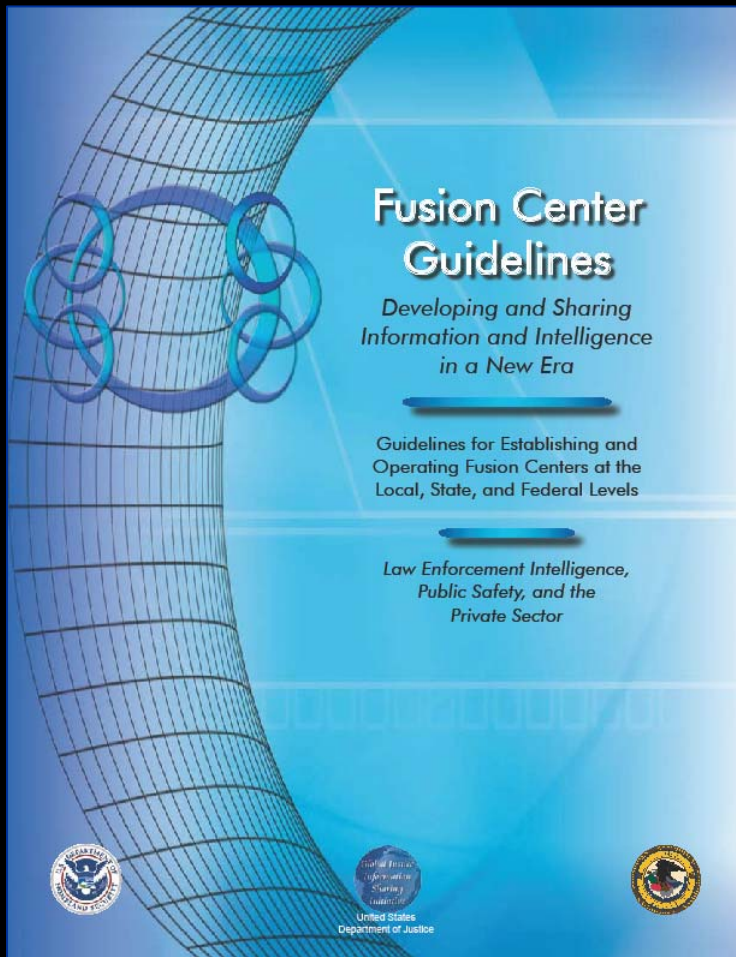
National Strategy for Information Sharing



“Providing *reports* and awareness training to State, local, and tribal authorities regarding strategic goals, operational capabilities, and methods of operation utilized by international and domestic terrorist organizations so that local events and behaviors can be viewed within the context of potential terrorist threats.”

Source: *National Strategy for Information Sharing*, p. A1-6, 2007

Fusion Center Guidelines



- Developing and Sharing Information and Intelligence in a **New Era** (orig. *New World*)
- Remove barriers to information sharing at the Local, State, Tribal and Federal Levels
- Collaboration between Law Enforcement Intelligence, Public Safety, and the **Private Sector**

Fusion Center Guidelines

Introduction— Fusion Concept and Functions

As criminal and terrorist activity threatens the safety of our nation's citizens and visitors, the ability to quickly exchange relevant information and intelligence becomes increasingly critical. Over the last few years, significant progress has been made in breaking down barriers and improving information exchange. Policymakers and leaders have recognized the importance of creating an environment where intelligence can be securely shared among law enforcement, public safety agencies, and the private sector. Although strides have been made, there is still much work ahead. There is still an urgent need to rigorously refine and accommodate our rapidly changing world.

Many obstacles have been encountered that have impacted the ability to share intelligence, such as the lack of trusted partnerships; disparate, incompatible, and antiquated communications, computer systems, and software; the need to query multiple databases or systems; the lack of communication; the lack of standards and policies; and legal and cultural issues.

These barriers have proven to be difficult hurdles. Yet, there are steps that can be taken to overcome these issues and create a proactive environment for the successful exchange of

Information systems contribute to every aspect of homeland security. Although American information technology is the most advanced in the world, our country's information systems have not adequately supported the homeland security mission. Databases used for federal law enforcement, immigration, intelligence, public health, surveillance, and emergency management have not been connected in a way that allows us to comprehend where information gaps and redundancies exist.

We must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy.

The National Strategy for Homeland Security July 2002

We must link the vast amounts of knowledge residing within each government agency while insuring adequate privacy.

National Strategy for Homeland Security July 2002

intelligence component of fusion centers. The focus also tasked with recommending related model police procedures to support this initiative. Group members the need and importance of integrating all public safe private partners.

Concurrently, a parallel effort was under way by the Security Advisory Council (HSAC) Intelligence and Information Sharing Working Group to develop intelligence and information sharing guidelines, based on specific presidential directives local, state, and federal agencies creating fusion center directives provide guidance to local and state entities prevention and response to criminal and terrorist activities. The recommendations and findings resulting from HSAC Intelligence and Information Sharing Working Group support the expansion of the Fusion Center Guidelines safety and private sector entities.

Subsequent to the efforts of the Law Enforcement Intelligence FCFG and HSAC, the Public Safety FCFG was created the purpose of integrating the public safety component the Fusion Center Guidelines. Members of the focus concentrated on the need for information and intelligence between law enforcement and public safety communities. This group endorsed the guidelines developed by the Enforcement Intelligence FCFG and offered suggestions recommendations to successfully incorporate public entities into fusion centers.

The last phase established the Private Sector FCFG mission was to integrate the private sector into the fusion center. With 25 percent of critical infrastructure owned by private entities, their involvement in fusion centers is essential to having a comprehensive all-hazards, all-crimes fusion center. Key points addressed included collaboration between the fusion center and mission-critical private sector entities, as well as identification of private sector capabilities and information needs. In addition, the need for a two-way educational process between the private sector and fusion centers was identified. The purpose of this educational process is to develop an understanding of how each entity operates and how each can enhance operations and functionality with the other.

All levels of government, the private sector, and nongovernmental organizations must work together to prepare for, prevent, respond to, and recover from terrorist and criminal events. Through

8 More information on HSAC can be accessed at www.dhs.gov/hsac.
9 Homeland Security Presidential Directive 8 (HSPD-8) was issued with the purpose of establishing policies to strengthen the preparedness of the United States to prevent and respond to terrorist and criminal

**Fusion:
Turning
Information
and Intelligence
into Actionable
Knowledge**

and their attack methods. This information should serve as a guide for efforts to rapidly identify both immediate and long-term threats; identify persons involved in terrorism-related and criminal activities; and guide the implementation of information-driven and risk-based prevention, response, and consequence-management.

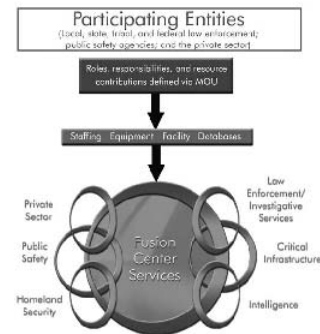
Since September 11, both response and prevention are critical to an overall strategy to secure our homeland and decrease criminal activities. September 11 also confirmed how critical local, state, tribal, and federal law enforcement agencies and public safety and private sector entities are in collecting important information and intelligence that ultimately impacts the nation's overall ability to prevent terrorism-related and criminal activities. In responding



tion in a New Era

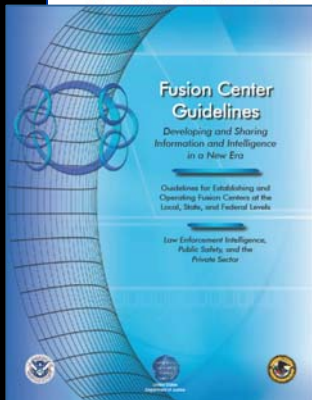
Participating Entities

Figure 2—Fusion Center Components



Fusion centers will act as an analytical hub, processing, evaluating, and disseminating critical information for law enforcement, public safety, and private partners, based on a criminal predicate, threat, or public safety need. They will focus on collaboration and analysis and will become a repository for information that flows through the center, while ensuring state and federal privacy laws and requirements are adhered to. Ultimately, fusion centers will become the center for investigative support, information and intelligence sharing, homeland security, and public safety and private sector partners.

Fusion Center Functions



pile, analyze, and intelligence to threat, public services, and entities, prevent, criminal information assigned to 5) and tactical be meaningful, collection of developing the enforcement it information, on a criminal is to rapidly ary, proactive, and support predictive of emergency and

One of the principal outcomes of the fusion process should be the identification of terrorism-related leads—any nexus between crime-related and other information collected by local, state, and private entities and a terrorist organization and/or attack. Many experts believe that there is a high probability of identifying terrorists through precursor criminal activity, including illegal drug operations, money laundering, fraud, terrorism, and identity theft.¹⁴ The fusion process does not replace or replicate mission-specific intelligence and information management. It does, however, leverage information and intelligence developed through these processes and systems to support the rapid identification of patterns and trends that may reflect an emerging threat. Some of the recommended goals and functions for fusion centers include:

- Serve as the primary point of contact to report criminal/terrorist information to the local Joint Terrorism Task Force (JTTF) and DHS's Homeland Security Operations Center (HSOC).
- Include the capability of blending law enforcement information and intelligence.
- Collect, analyze, and disseminate "all-crimes" information, so as to identify emerging patterns and trends. Evaluate and reevaluate the process, new data, and emerging threats.
- Adopt and adhere to a statewide strategy to examine the information exchanges of the states' law enforcement and homeland security partners, including dissemination of information by the state Homeland Security Advisor to law enforcement.
- Maintain an up-to-date statewide risk assessment.
- Serve as a receipt-and-dissemination hub for law enforcement information provided by federal entities, such as that provided by the Federal Bureau of Investigation's Regional Data Exchange (R-DEX) and National Data Exchange (N-DEX), when operational, and DHS's Homeland Security Information Network (HSIN).

Each of these areas can be expanded to include a number of critical tasks and responsibilities. To successfully achieve these goals, the first responder and private community, along with the public, must be a part of the fusion center concept. The integration of nontraditional consumers of information and intelligence is a key component of a fusion center.

The responsibilities of fusion centers are immense. Guidelines, as well as sample policies and templates, must be developed to assist in establishing and operating fusion centers.

Functional Categories

Every level and sector (discipline) of government and the private sector should be integrated into fusion centers. This may seem like a daunting task, however, functional categories have been developed to assist in integration efforts. These categories are not meant to be exhaustive; rather, they provide governance bodies a starting place to begin collaboration with different components and entities. Each fusion center should evaluate its needs, threats, and constituents to determine what entities should be integrated. Entities that comprise the functional categories can provide fusion centers with both

¹⁴ The Impact of Terrorism on State Law Enforcement, June 2005, p. 34.

- Local, state, tribal, and federal law enforcement
- Public safety agencies
- The private sector
- It must include...law enforcement and intelligence information, such as public health and transportation.

Resolution in Support



Major Cities Chiefs Association RESOLUTION

Fusion Center Guidelines

WHEREAS, the Major Cities Chiefs Association recognizes that in the aftermath of the September 11, 2001, terrorist attacks, there is a need to address the deficiencies that exist in this country in the collection, analysis, and dissemination of criminal intelligence; and

WHEREAS, the Major Cities Chiefs Association recognizes the need to address these deficiencies and to ensure that local, state, and tribal law enforcement are involved in the intelligence process; and

WHEREAS, with the participation of the Major Cities Chiefs Association, the U.S. Department of Justice's Global Justice Information Sharing Initiative convened a working group to develop guidelines for the operation of intelligence fusion centers; and

WHEREAS, the findings of that work group led to the issuance of a report in 2006 entitled *Fusion Center Guidelines—Law Enforcement Intelligence, Public Safety, and the Private Sector*; and

WHEREAS, the *Fusion Center Guidelines—Law Enforcement Intelligence, Public Safety, and the Private Sector* report has recommended 18 guidelines for the proper operation of an intelligence fusion center; now, therefore, be it

RESOLVED, that the Major Cities Chiefs Association supports the *Fusion Center Guidelines—Law Enforcement Intelligence, Public Safety, and the Private Sector* report as a valuable tool to remedy the deficiencies in the existing methods of collecting, analyzing, and disseminating criminal intelligence and that the Major Cities Chiefs Association encourages all law enforcement agencies to utilize these guidelines in the development and operation of intelligence fusion centers.

June 6, 2006

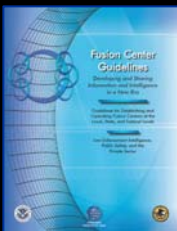
Harold Hurtt
President

...the Major Cities Chiefs Association encourages all law enforcement agencies to utilize these guidelines in the development and operation of intelligence fusion centers.

State Strategy



**“Fusion involves
every level and
sector (discipline)
of government,
private sector
entities, and the
public...”**



Functional Categories

(Sectors in which to gain access)

- **Agriculture, Food, Water and the Environment**
- **Banking and Finance**
- **Chemical Industry & Hazardous Materials**
- **Criminal Justice**
- **Education**
- **Emergency Services**
(non-law enforcement)
- **Energy**
- **Government Health and Public Services**
- **Hospitality and Lodging**
- **Information and Telecommunications**
- **Military Facilities and Defense Industrial Base**
- **Postal and Shipping**
- **Private Security**
- **Public Works**
- **Real Estate**
- **Retail**
- **Social Services**
- **Transportation**

Fusion Center Guideline #1 (of 18)

Guideline 1

Adhere to the *National Criminal Intelligence Sharing Plan* (NCISP) and other sector-specific information sharing guidelines, and perform all steps of the intelligence and fusion processes.

The NCISP and the Intelligence and Fusion Processes

Justification

After the tragic events of September 11, 2001, law enforcement executives and intelligence experts nationwide agreed that law enforcement agencies must work together to develop the capability to gather information, produce intelligence, and share that intelligence with other law enforcement and public safety agencies. The *National Criminal Intelligence Sharing Plan* (NCISP or Plan) was developed in response to this need.

The NCISP provides model standards and policies, recommends methodologies for sharing classified reports, and recommends a nationwide sensitive but unclassified (SBU) communications capability for criminal intelligence sharing. The Plan is a living document that provides local, state, tribal, and federal law enforcement agencies the tools and resources necessary for developing, gathering, accessing, receiving, and sharing intelligence. It is the blueprint that law enforcement agencies can employ to support their crime-fighting and public safety efforts. The Plan is based. It is the intelligence. It is the intent in which all

- Target resources.
- Disrupt prolific criminals.
- Articulate a case to the public and in court.

Intelligence-led policing also provides advantages to public safety and private sector components, including trends in criminal activity and increased information sharing with law enforcement to address crime prevention efforts.

Criminal intelligence is the result of a process involving planning and direction, information collection, processing/collation, analysis, dissemination, and reevaluation of information on suspected criminals and/or organizations. This sequential process is commonly referred to as the intelligence process (or cycle). There are various models of the intelligence process in use; however, most models contain the basic steps depicted in the following graphic:

The Intelligence Process

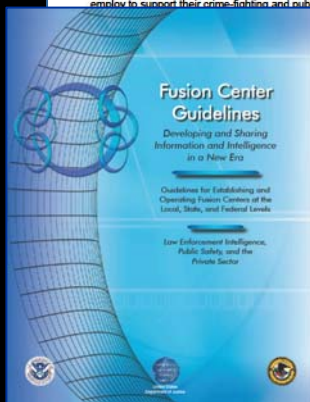


ence-led policing embrace and their efforts policing allows law

and the criminal

Staffing: Excellence
lice College, 2003.

Adhere to the **National Criminal Intelligence Sharing Plan (NCISP)** and other sector specific information sharing guidelines, and perform *all* steps of the intelligence and fusion processes.



Fusion Center Guideline #5

Guideline 5

Utilize Memorandums of Understanding (MOUs), Non-Disclosure Agreements (NDAs), or other types of agency agreements, as appropriate.

Memorandum of Understanding (MOU) and Non-Disclosure Agreement (NDA)

MOU

It is recommended that fusion centers be governed and managed in accordance with an MOU. An MOU, a necessary tool for information sharing, defines the terms, responsibilities, relationships, intentions, and commitments of each participating entity; the agreement also provides an outline of the who, what, where, when, why, and how of the project. Partners should commit to the program policies by signing the MOU. In addition to MOUs, some initiatives utilize agency, individual, and data sharing user agreements.

Issues for Consideration

When negotiating and drafting MOUs, consider:

- Identifying and understanding the legal and practical implications of the MOU.
- Defining the roles and responsibilities of the participating agencies.
- Embracing and encouraging trusted relationships.

- Funding/costs
- Civil liability/indemnification issues
- Policies and procedures
- Privacy guidelines
- Terms
- Integrity control
- Dispute resolution process
- Points of contact
- Effective date/duration/modification/termination
- Services
- Declassification procedure
- Special conditions
- Protocols for communication and information exchange
- Protocols for background checks on fusion center participants

NDA

The fusion center determines risks to the private sector and analyzes suspicious activity information. This function requires the sharing of sensitive information from the private sector to the fusion center. To aid in sharing this sensitive information, a Non-Disclosure Agreement may be used. The NDA provides private sector entities an additional layer of security, ensuring

Utilize Memorandums of Understanding (MOUs), Non-Disclosure Agreements (NDAs)...

- Assignment of personnel (removal/rotation)

Terrorism Task Force (JTF), Field Intelligence Group, the state police, or other appropriate agencies). Information that the

Information shared with outside agencies, i.e. FBI, Joint Terrorism Task Force, Field Intelligence Group, state police, or *appropriate* agencies.

Open records access may change

Fusion Center Guideline #6

Guideline 6

Leverage the databases, systems, and networks available via participating entities to maximize information sharing.

Database Resources

Justification

During the focus group process, participants reviewed a number of information and intelligence sharing initiatives. Most of the initiatives have access to some local, state, and federal databases, as well as other organizations or data sets. Centers may want to evaluate the types of databases that participating agencies have available. Gaps should be identified and researched. Leveraging the databases and systems available via participating entities will help maximize information sharing. This is an opportunity to access previously unavailable information. It is recommended that ownership and control of law enforcement information shared through the center remain with the originating agency. Data owners should be responsible for the quality of data shared. Access to data can be controlled in a variety of

ways, including fusion center leadership controlling who has access or data originators controlling access levels. For more information about the security of data, see Guideline 9 (Security). Another option is for the center to house their information. If a center chooses this option, it is important for the necessary policies and procedures to be in place to govern use and access.

Fusion centers should consult with public safety and private sector personnel to determine if any information sharing databases may be available within their respective jurisdictions. Special consideration should be given to the development of policies and procedures that ensure public safety and private sector information is not combined with federal data that contains personally identifiable information, and when a criminal predicate, threat, or public safety need is identified, access to this information will be virtual through networking and utilizing a search function. Additionally, fusion center participants should ensure compliance with all local, state, and federal privacy and civil liberties laws and statutes.

Issues for Consideration

When accessing databases, consider obtaining access to a variety of databases and systems, such as:

- Driver's license
- Motor vehicle registration
- Location information (411, addresses, and phone numbers)
- Law enforcement databases
- National Crime Information Center (NCIC), Nlets-The International Justice and Public Safety Information Sharing Network, and the Terrorist Screening Center (TSC)



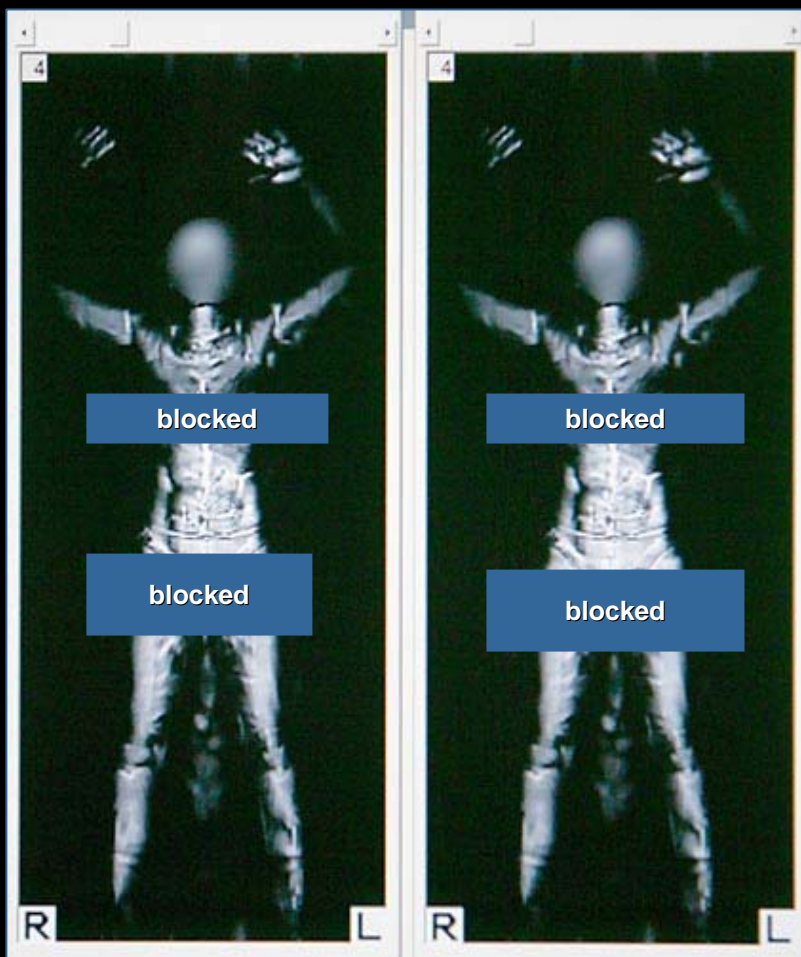
Leverage the databases, systems, and networks available via participating entities to maximize information sharing

- Driver's license
- Motor Vehicle registration
- Location Information (411, addresses, phone numbers)
- National Crime Information Center, Nlets, TSC
- Public & Private sources
- Organizations and associations (i.e. Infragard)



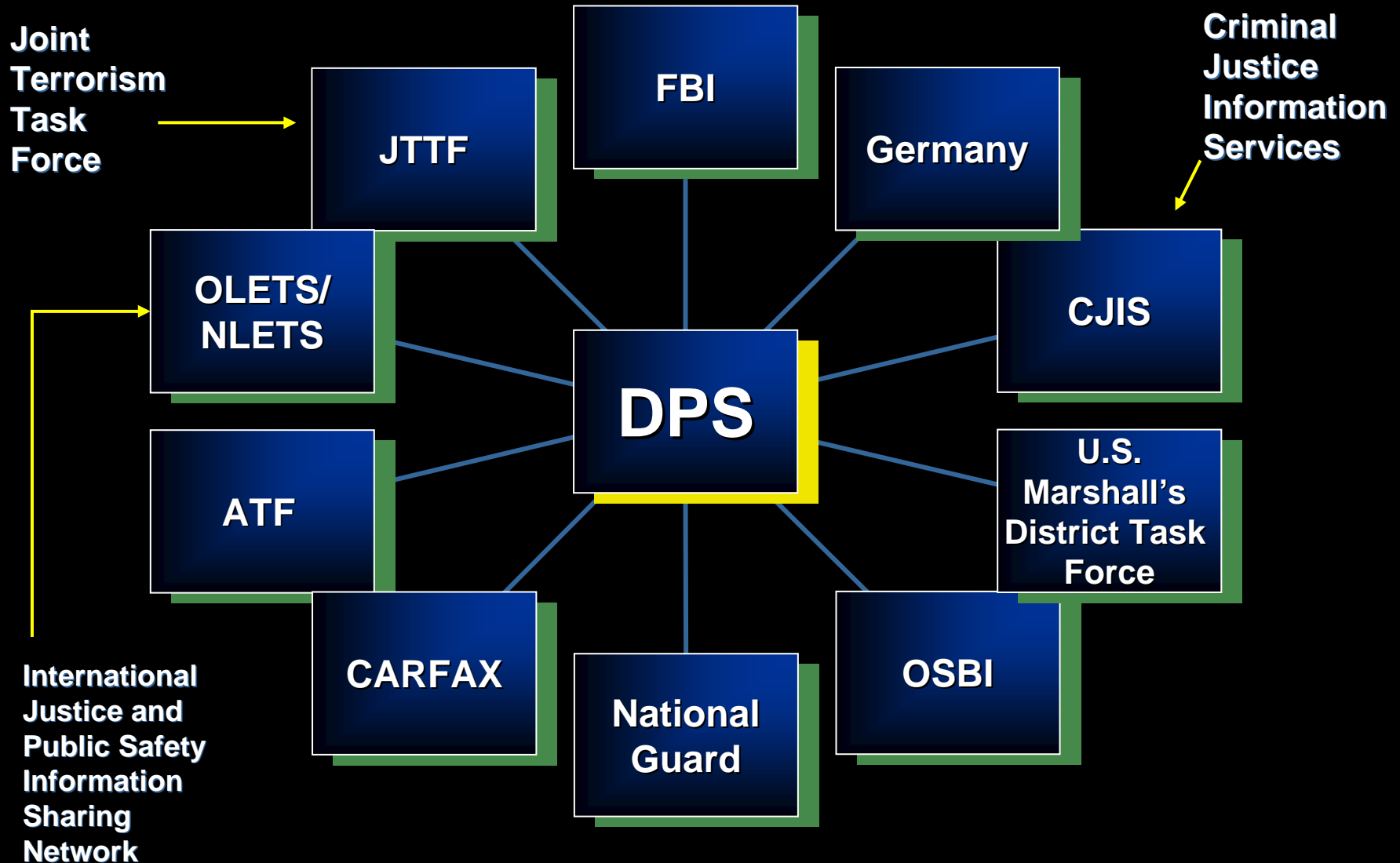
InfraGard®
a collaboration for
infrastructure protection

Fusion Center Guideline #8: Privacy and civil liberties policy



Bars added by presenter – not on original photos

Some of Oklahoma's DPS Agreements & MOUs



Leveraging a database - SB 483:

- **Would allow “direct electronic access” to the computerized photo in the DPS database**
- **For law enforcement purposes**
- **By law enforcement or *by any political subdivision* of the state**

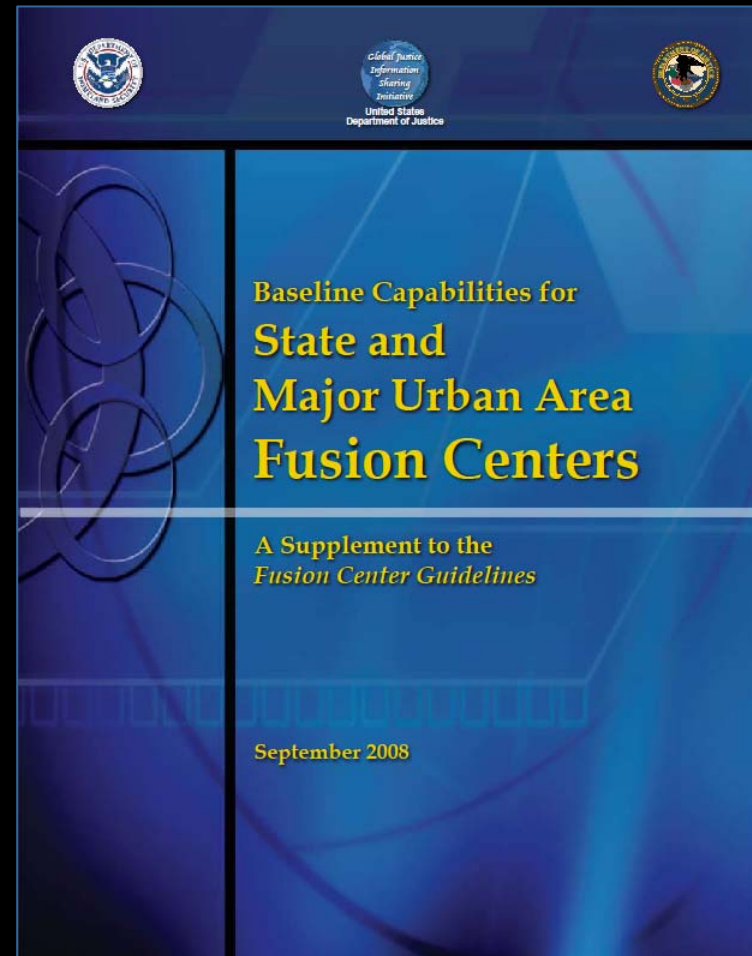


Oklahoma Capitol

Baseline Capabilities

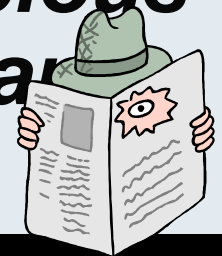
Identifies baseline capabilities for fusion centers and the operational standards for:

“Establishing a National Integrated Network of State and Major Urban Area Fusion Centers.”



SAR – Suspicious Activity

“Fusion Centers shall develop, implement, and maintain a plan to support the establishment of a suspicious activity and incident reporting process for their geographic area of responsibility, in a manner consistent with the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*”



WHY?

Supply Chain Management for a Market Based Economy

- **Resource** – raw material; an available supply that can be drawn on; mineral wealth, *labor force*, and armaments; assets (human resources)
- **Asset** – a thing or *person* that is useful
- **Supply Chain** – or logistics network; system of organizations, *people*, technology, activities, information and resources involved in moving a product or service from supplier to customer; from raw materials to finished product

Identify Stovepipes

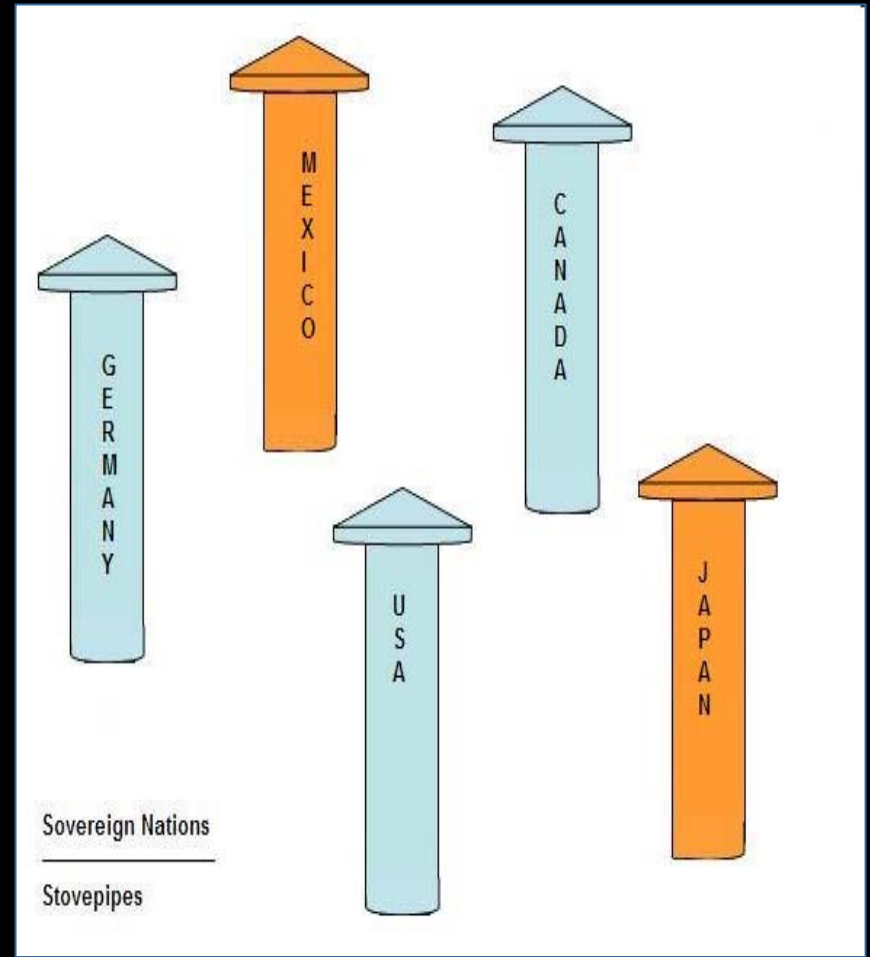


Diagram courtesy V.L. Davis, researcher

Eliminate Stovepipes

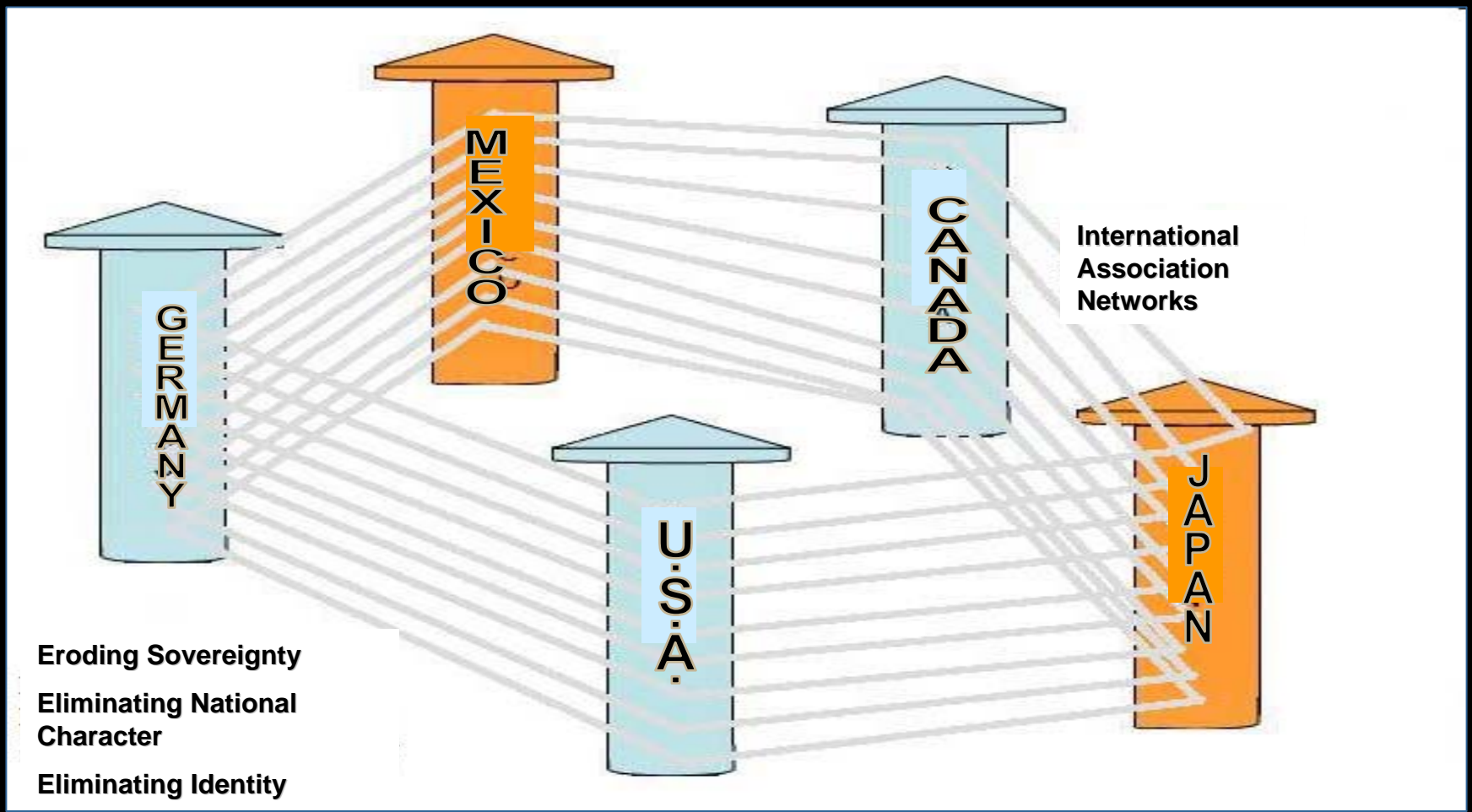
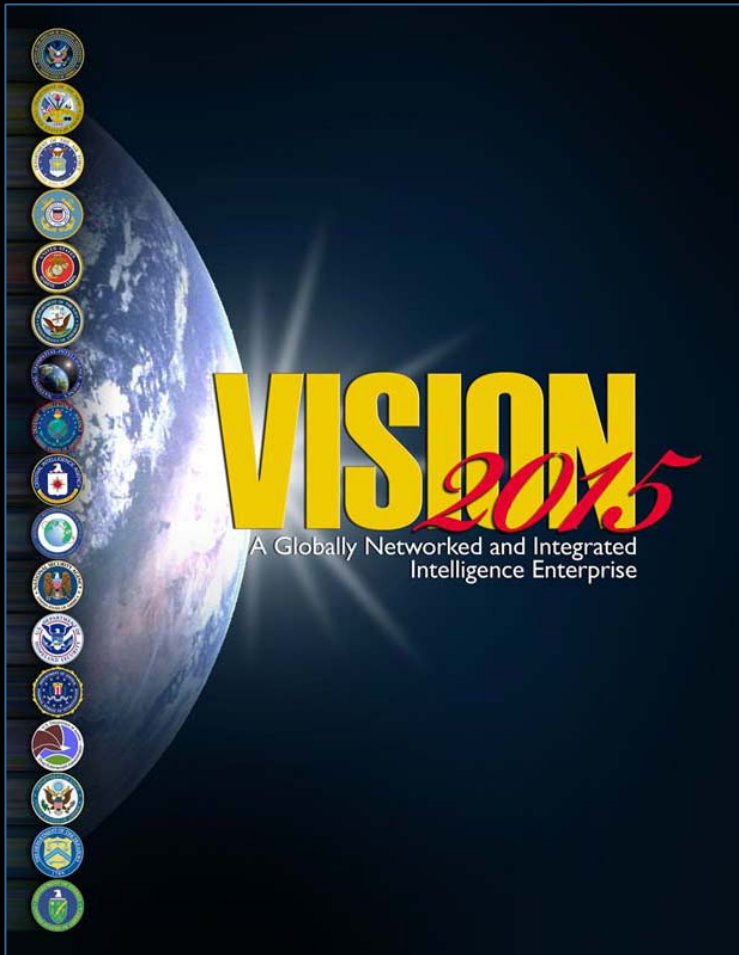


Diagram courtesy V.L. Davis, researcher

VISION *2015*



- **17 Intelligence Agencies, including DoD, DHS, CIA, FBI**
- **A Globally Networked and Integrated Intelligence Enterprise**

Customers: Policy Makers, military commanders, law enforcement and homeland security officials

Create Decision Advantage

Mission

Create Decision Advantage

Vision

A Globally Networked and Integrated Intelligence Enterprise

Strategy

Integrate foreign, military, and domestic intelligence capabilities through policy, personnel and technology actions to provide decision advantage to policy makers, warfighters, homeland security officials and law enforcement personnel

Values

Commitment • Courage • Collaboration



7. Persistent Threats and Emerging Missions

6. Decision Advantage

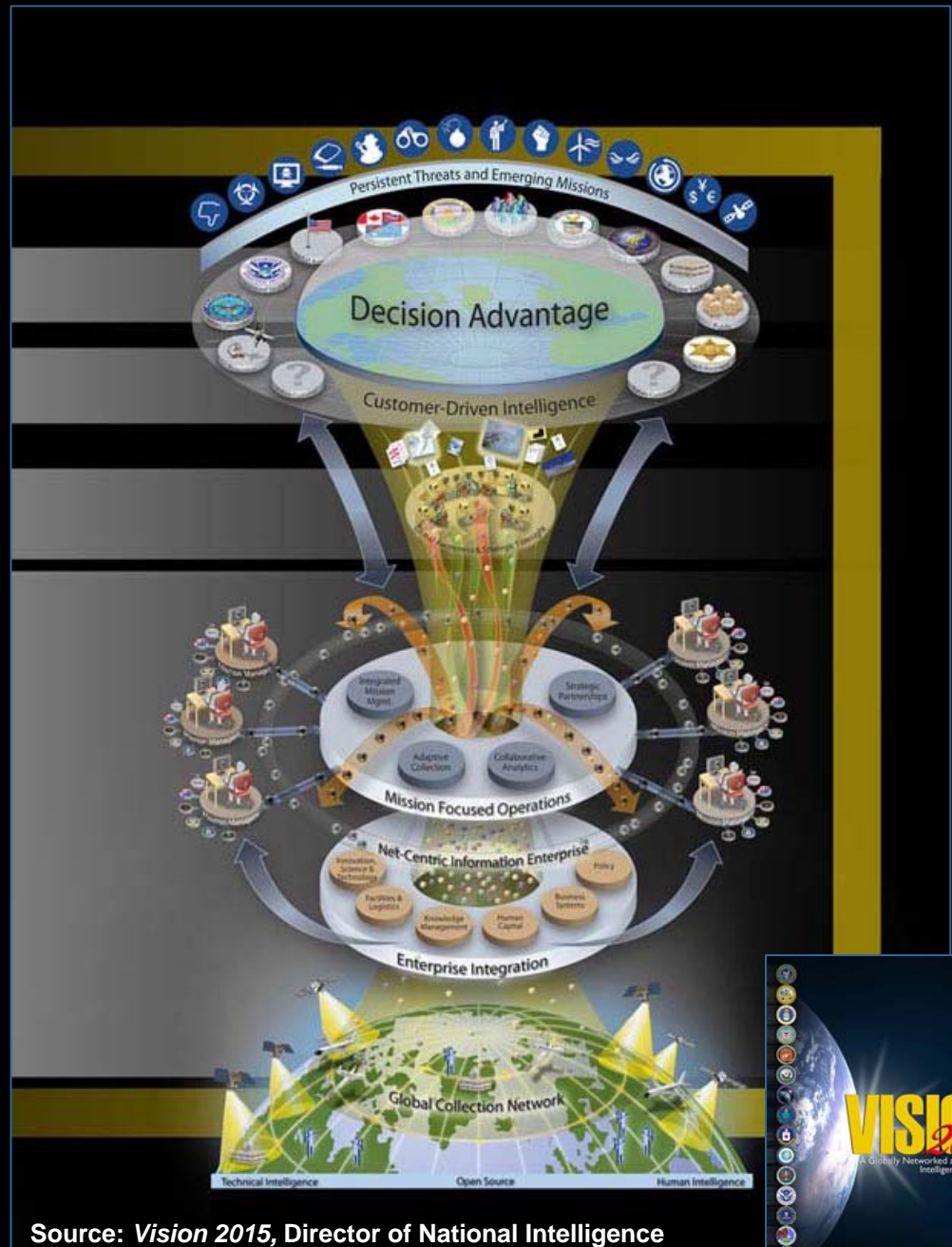
5. Customer-Driven Intelligence

4. Mission Focused Operations

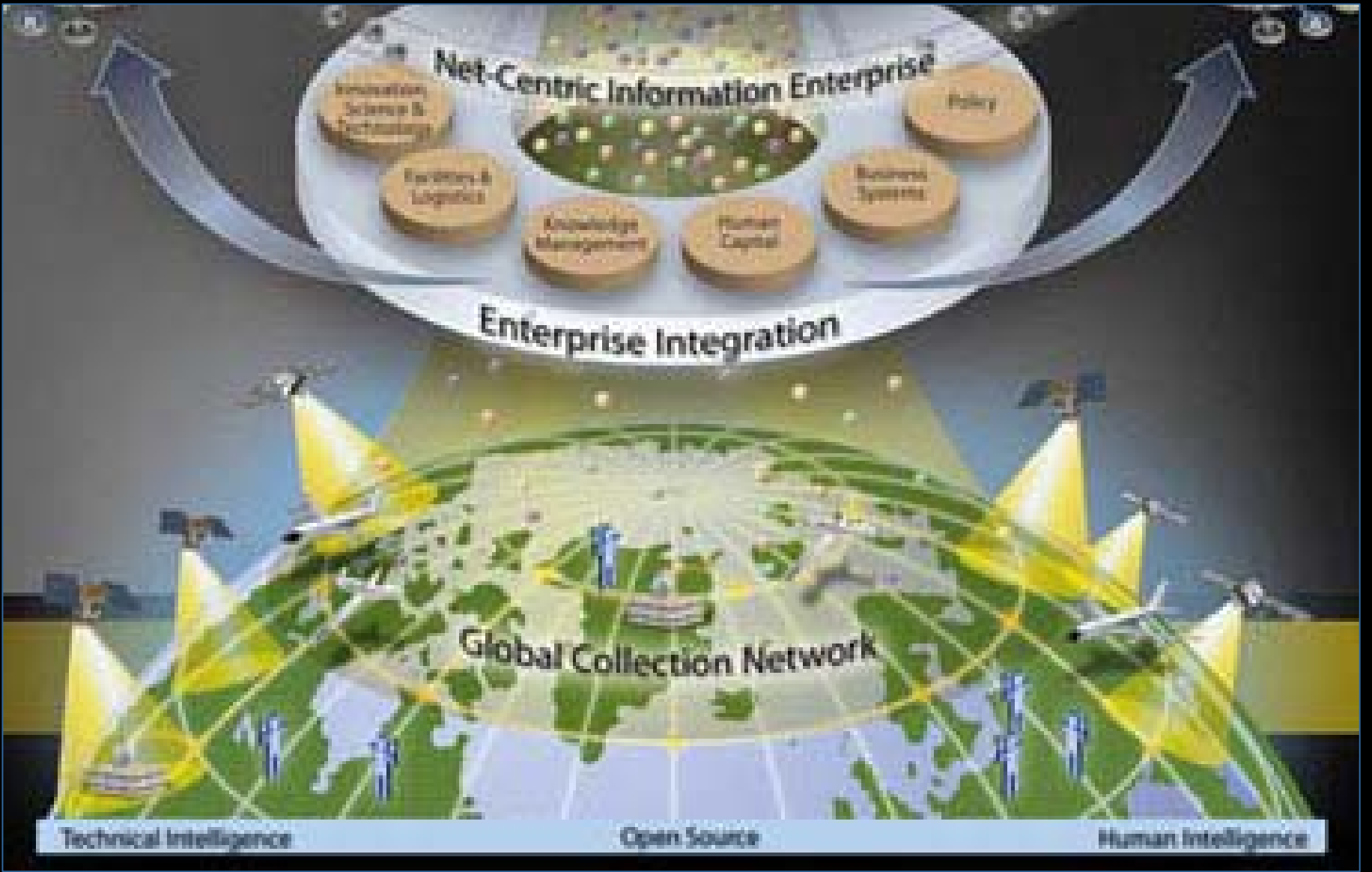
3. Net-centric Information Enterprise

2. Enterprise integration

1. Global Collection Network



Source: *Vision 2015*, Director of National Intelligence



Laying the Groundwork

Global Positioning System (GPS)

“The Global Positioning System (GPS) was designed as a dual-use system with the primary purpose of enhancing the effectiveness of U.S. and allied military forces.

GPS is rapidly becoming an integral component of the emerging

Global Information Infrastructure...”



Global Information Infrastructure = trackable

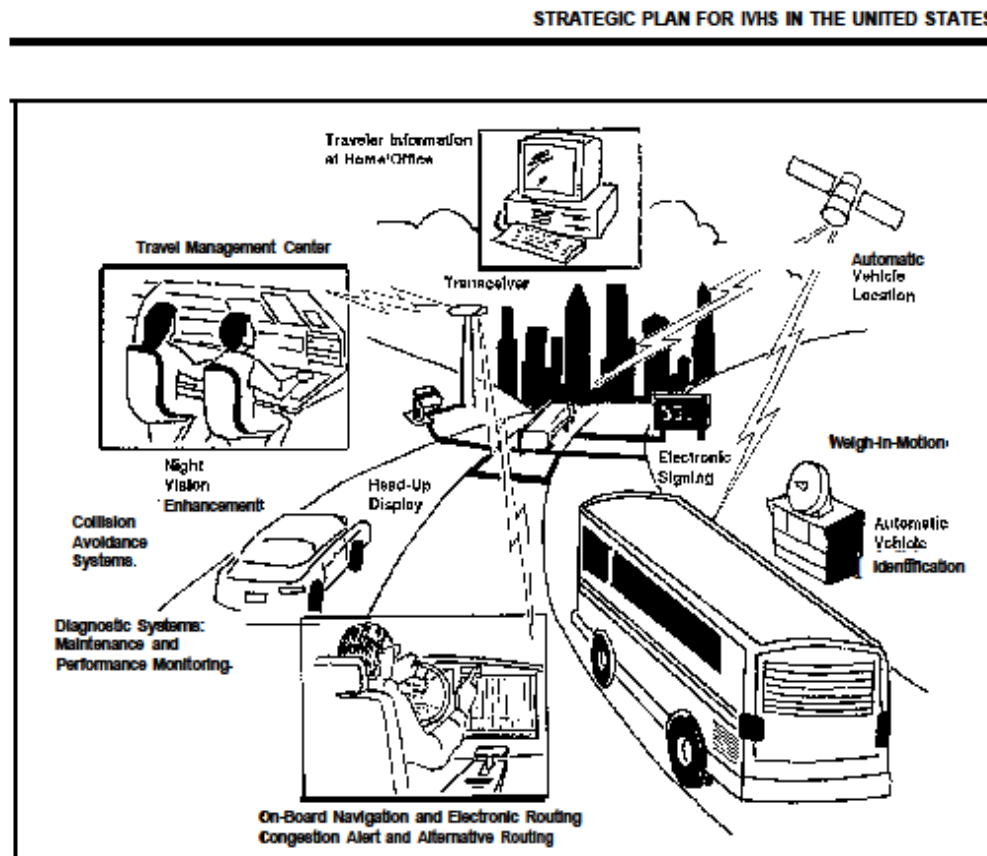


Figure 11-1. Some components of an Intelligent Vehicle-Highway System (Adapted from U.S. Department of Transportation National Transportation Strategic Planning Study, March 1990).

- Anything that emits an electronic RFID signal
- People
- Cars
- Buses
- Animals
- Cell Phones
- Etc.

MOU DoD & DOJ – Joint Technology



1994

The DoD and the DOJ entered into an agreement for the joint development of technology

(Date: 4/20/94, by A.G. Janet Reno, John Deutch, Deputy Secretary of State; later CIA Director)

1996

Presidential Decision Directive (PDD/NSTC6) – GPS for civil and commercial use.

(Jointly chaired by DOD and Dept. of Transportation)

GPS Policy: Cooperation

Dept. of Defense:

- With the Director of Central Intelligence, the Department of State and other departments and agencies

Dept. of Transportation:

- With the Departments of Commerce, Defense, and State.

Department of State:

- With foreign governments and other international organizations.



Communications Accord – US and Australia 7/08

Defense Dept photo by U.S. Air Force Tech Sgt
Jerry Morrison. www.defenselink.mil/

GPS Interoperability Agreements with EU, Russia, Australia, Japan

United States – Russian Federation
GPS/GLONASS Interoperability and Compatibility Working Group (WG-1)

Yaroslavl, Ring Premier Hotel, 14 December, 2006


Joint Statement

Working Group 1 met on December 13-14, 2006, in Yaroslavl, Russia, and discussed a range of issues. This was the third meeting of the working group. The meeting was highly successful and resolving many questions regarding interoperability and compatibility between the GPS and GLONASS systems. Both sides noted that concerning the question of the use FDMA and CDMA significant progress was made in understanding the benefit to the user community of using a common approach. The Russian side noted that a decision in this regard would be made by the end of 2007.

Both sides agreed that the planned International Satellite Forum 2007 to be held April 9-10, 2007, in Moscow will be a unique opportunity to demonstrate the benefits of GLONASS and GPS interoperability in the Russian Federation for civil applications.

Co-chair

Mark Crews

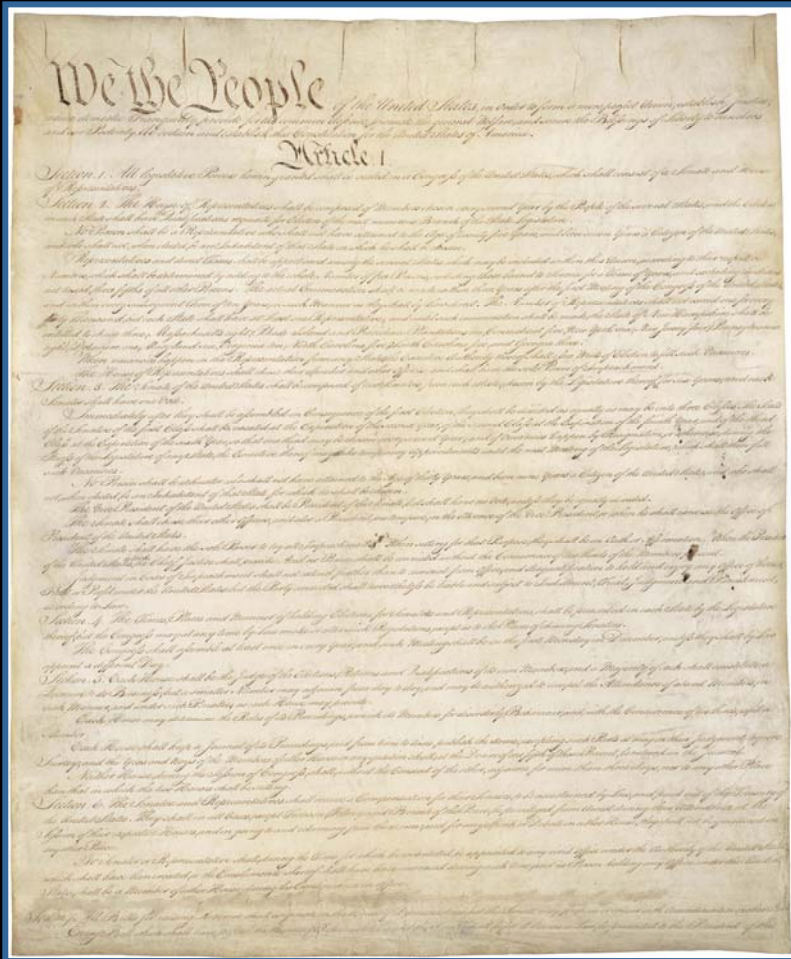
Co-chair

Vladimir Klimov

**US/Russian Federation
GPS/GLONASS
Interoperability**



US/EU Agreement

Constitutional vs. Corporate Considerations



Tower of Babel



Action

- **Identify the Fusion Center in your State**
- **Contact your Legislators and notify him/her of your concerns**
- **Open Records Request for all MOUs between the state Dept. of Homeland Security, OSBI, and DPS and any other entity.**
- **Do not allow “direct electronic access” to the DPS database**

Primary Sources

