

Imagine a global
data collection
network that
gathered
information on...

everyone..doing anything



Fusion Centers

or

"I Spy" for the Intelligence Enterprise

Copyright OK-SAFE, Inc. August 2010

Freedom Action National Conference, Valley Forge, PA

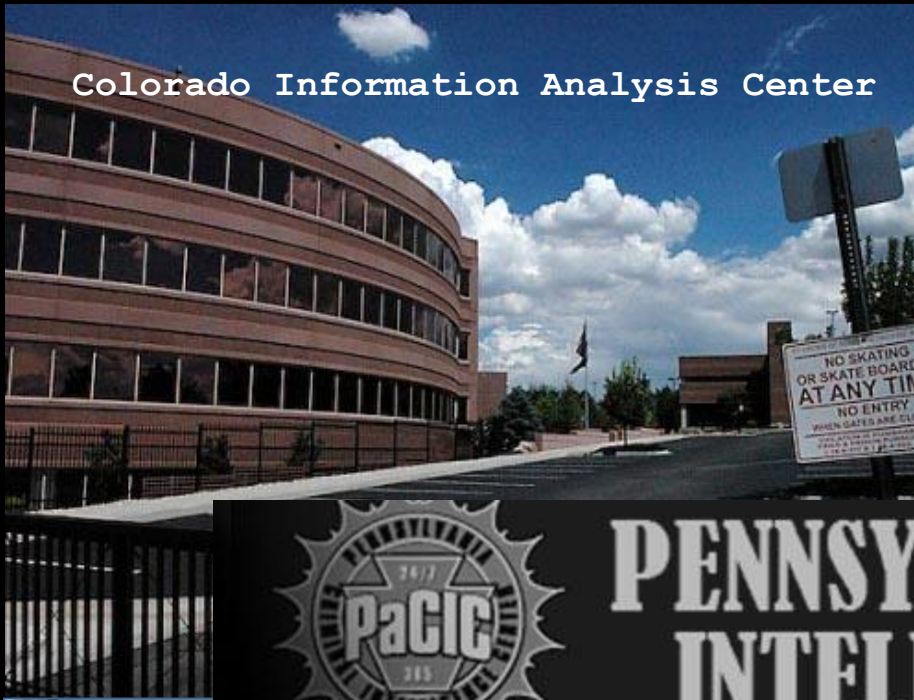
NY Times: "Chicago Links Street Cameras to Its 911 Network" by Karen Ann Cullotta, 2/20/09 Photo: Joshua Lott/Reuters

Intelligence Enterprise

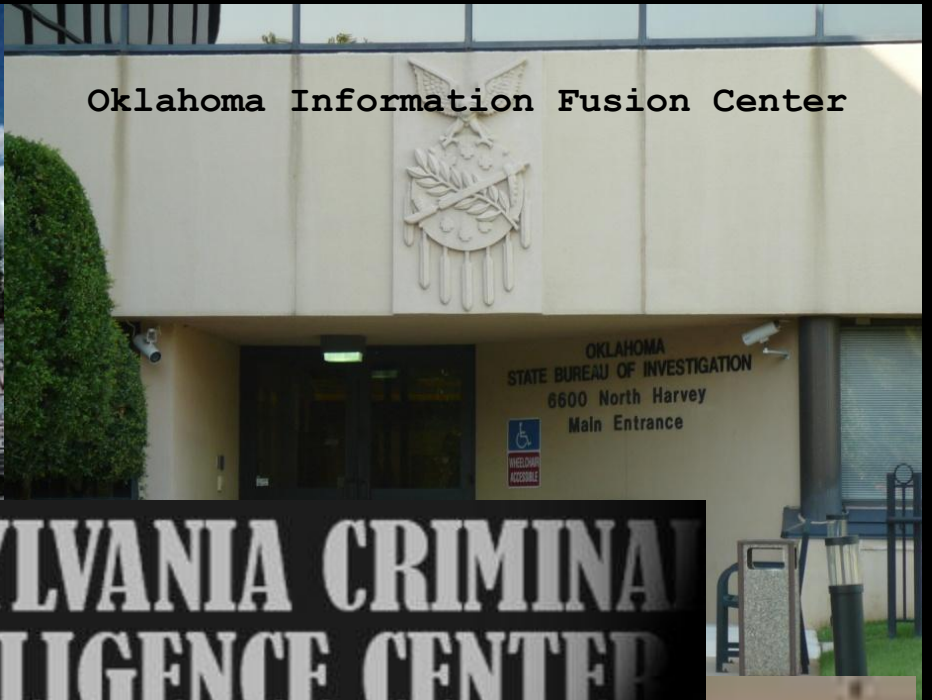
- **Intelligence:** the product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being , or known to be, criminal – and/or ***non-criminal.***
- **Enterprise:** An undertaking, esp. of some scope, complication, and risk. ***A business organization.***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

(Quote source: Vision 2015, p.14)

Colorado Information Analysis Center

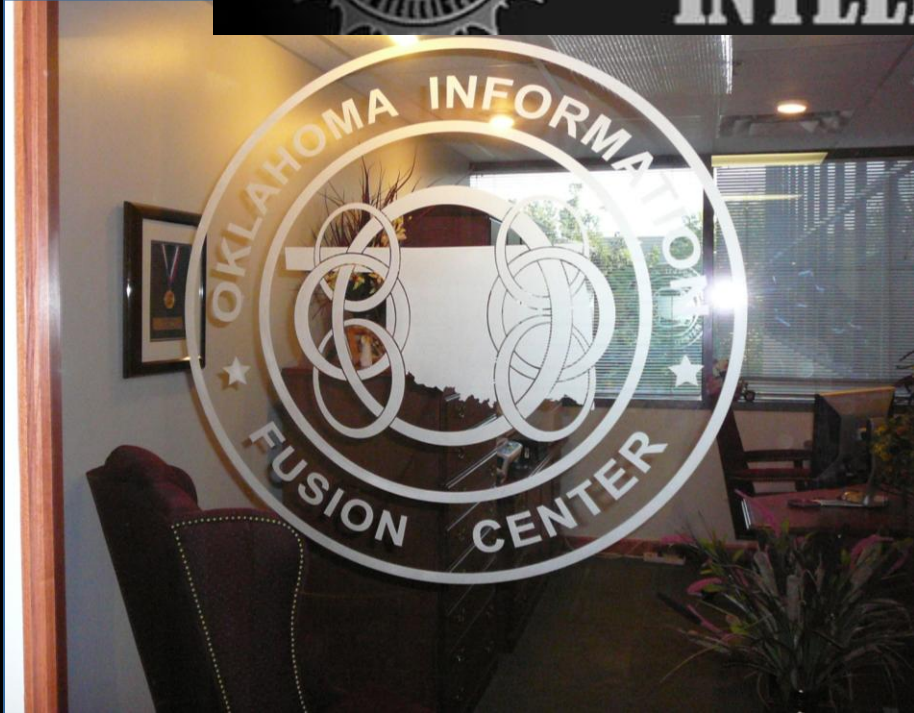


Oklahoma Information Fusion Center



 **PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER**

Chicago's Crime Prevention and Information Center



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

Laying the Groundwork

A Global Economy requires:

- **Global Control of Resources**

Sustainable Development

- **Global Control of Assets**

Assets include People, i.e. Intelligence;

- **Global Transportation System**

Movement of Goods, People and Information

- **Global Supply Chain Management**

Tracking and Control of All Production and Distribution; Interoperable Systems

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

1978-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...*”



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/

1992-Global Information Infrastructure - trackable

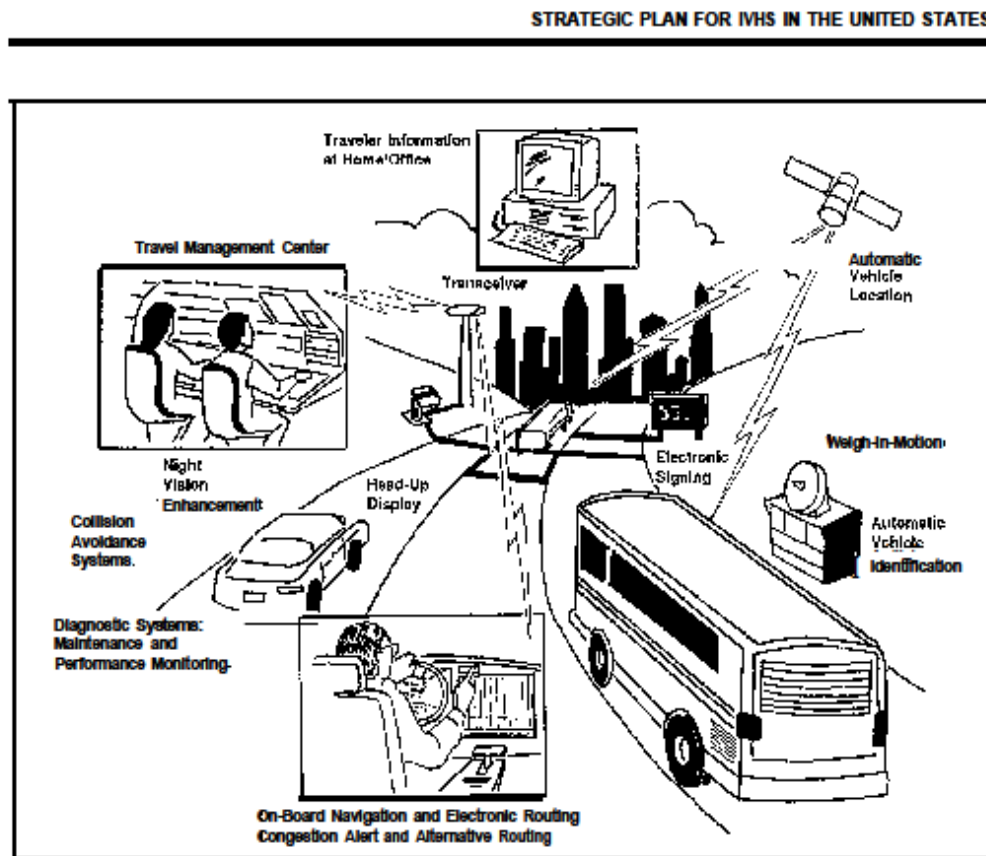


Figure 11-1. Some components of an Intelligent Vehicle-Highway System (Adapted from U.S. Department of Transportation National Transportation Strategic Planning Study, March 1990).

- 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)

1998 – National Crime Prevention and Privacy Compact Act

Pub. Law 105-251 (S. 2022)

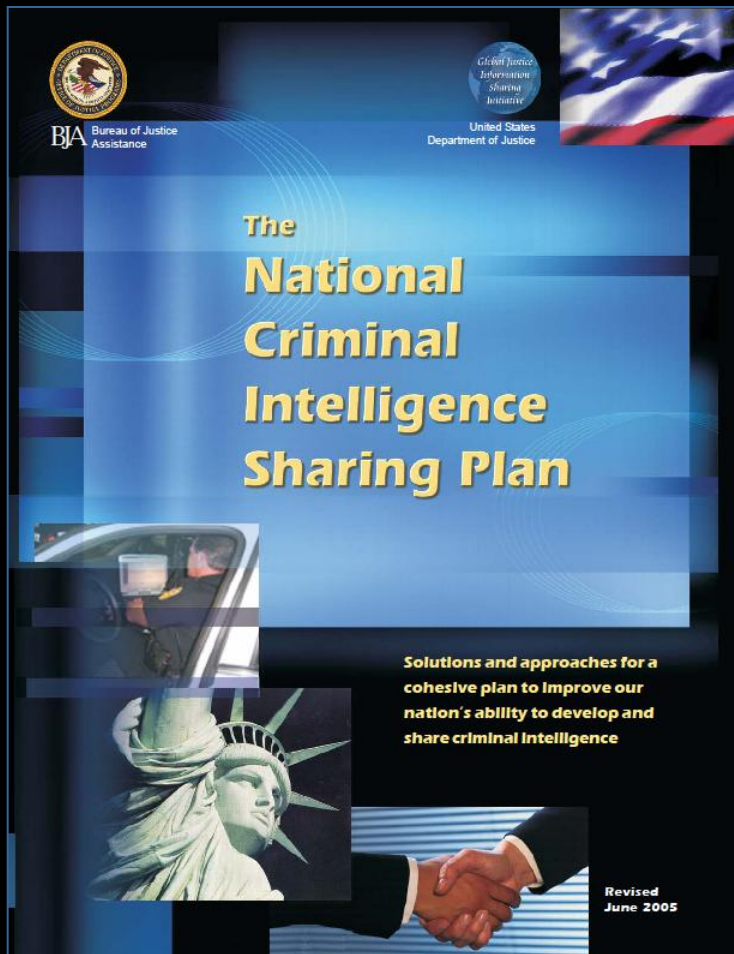
- (a) In General.--**This Compact organizes an electronic information sharing system among the Federal Government and the States** to exchange criminal history records for noncriminal justice purposes authorized by Federal or State law, such as background checks for governmental licensing and employment.
- (b) Obligations of Parties.--Under this Compact, the FBI and the Party States agree to maintain detailed databases of their respective criminal history records, including arrests and dispositions, and to make them available to the Federal Government and to Party States for authorized purposes. The FBI shall also manage the Federal data facilities that provide a significant part of the infrastructure for the system.

2005 -

- **NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL**
28 CFR Part 906, [NCPPC 113]
- **Outsourcing of Noncriminal Justice Administrative Functions**
- **AGENCY:** National Crime Prevention and Privacy Compact Council.
- **ACTION:** Final rule.

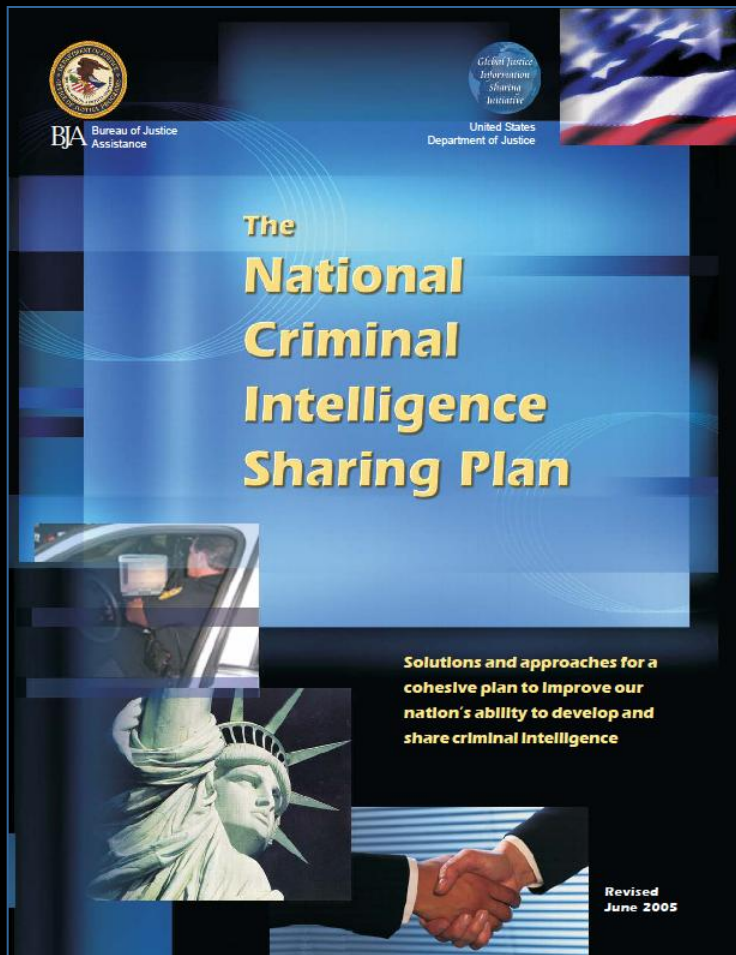
2001...?

The NCIS Plan



- Developed *before* 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**

**A Globally Networked
and Integrated World –**

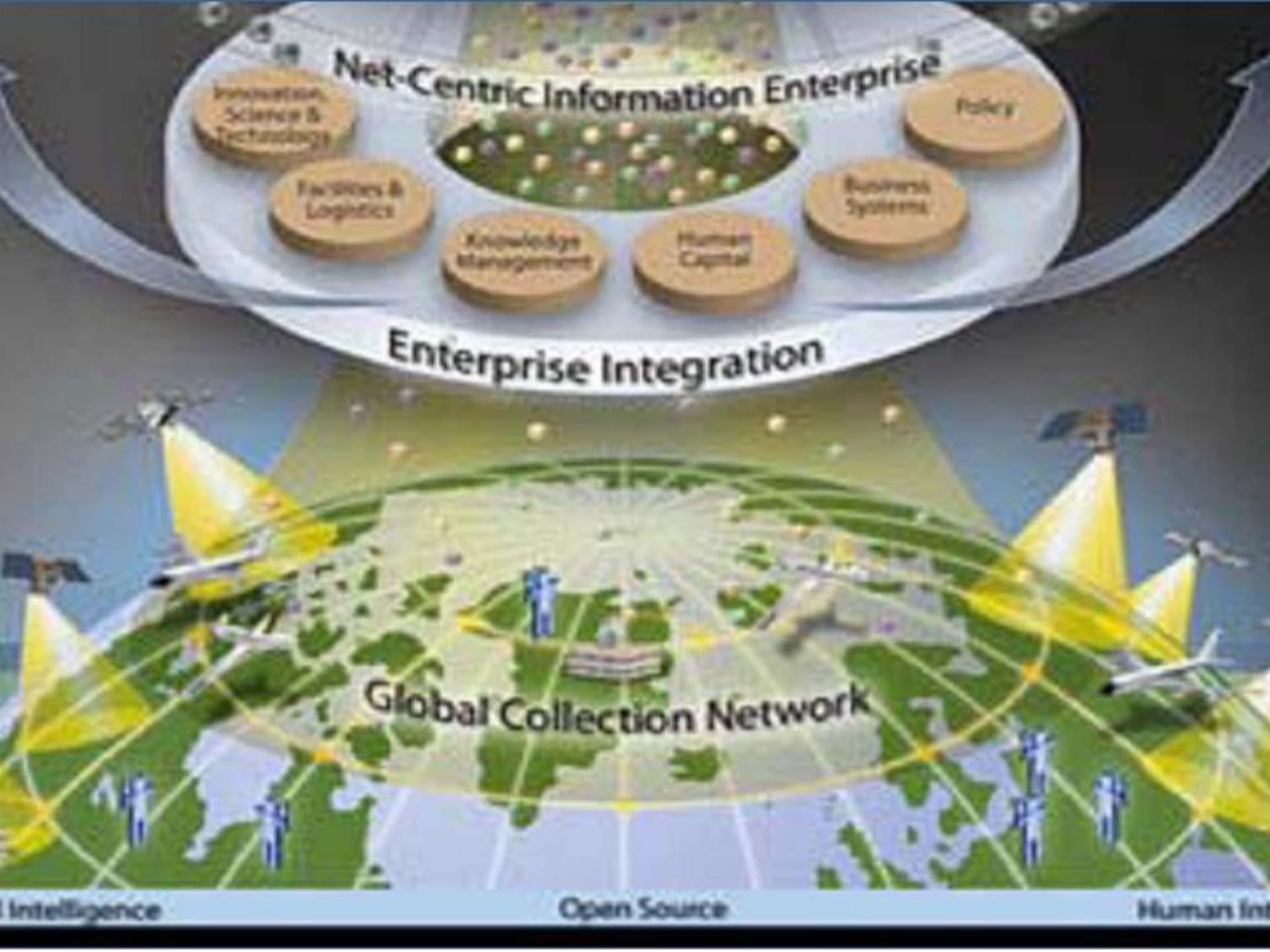
Vision 2015

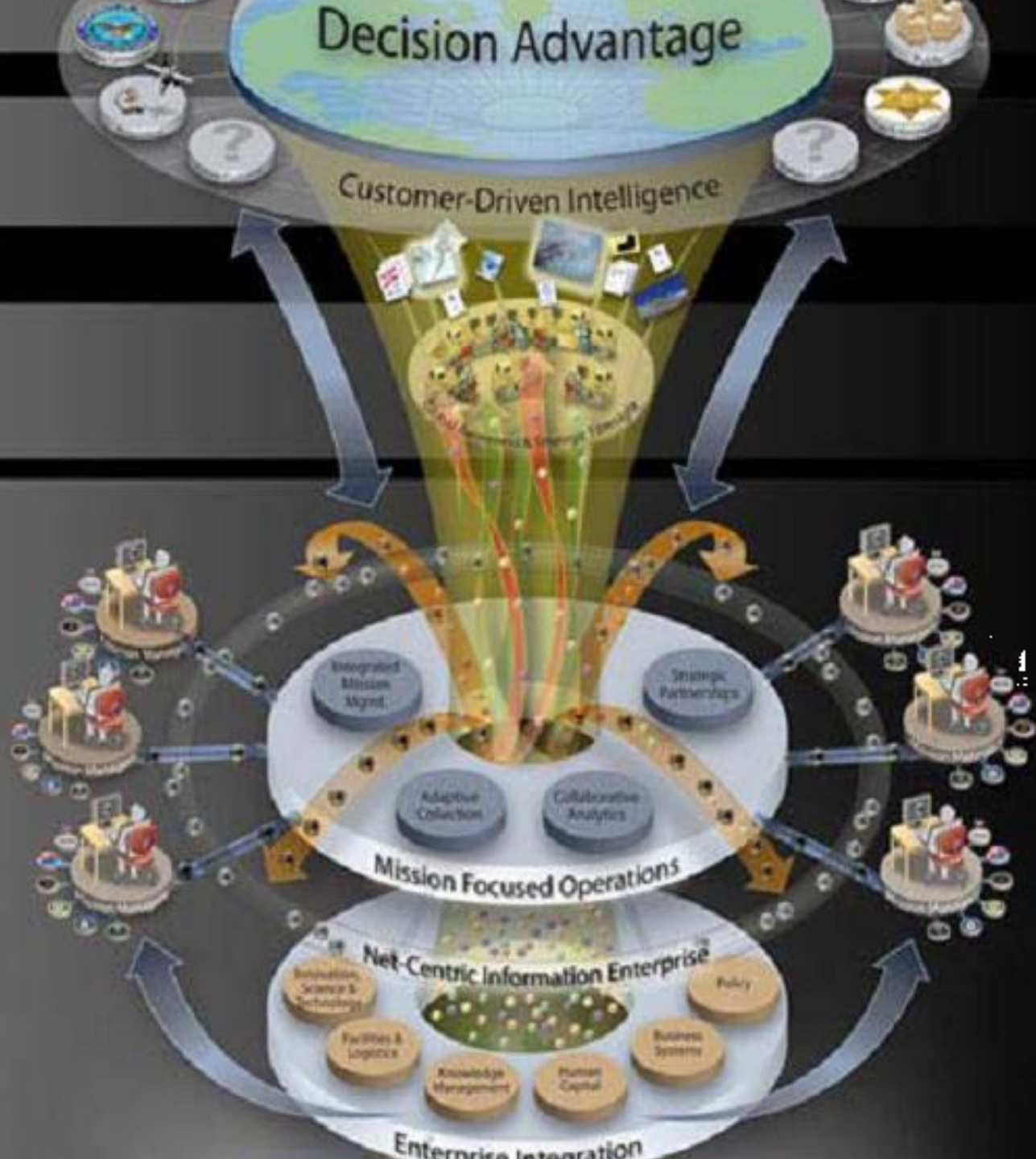


VISION

2015

A Globally Networked and Integrated
Intelligence Enterprise





7. Persistent Threats and Emerging Missions

6. **Decision Advantage**

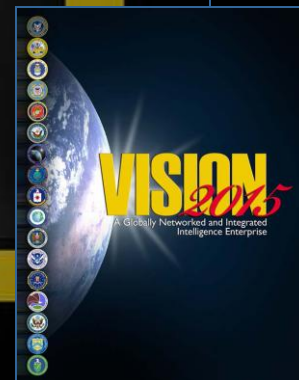
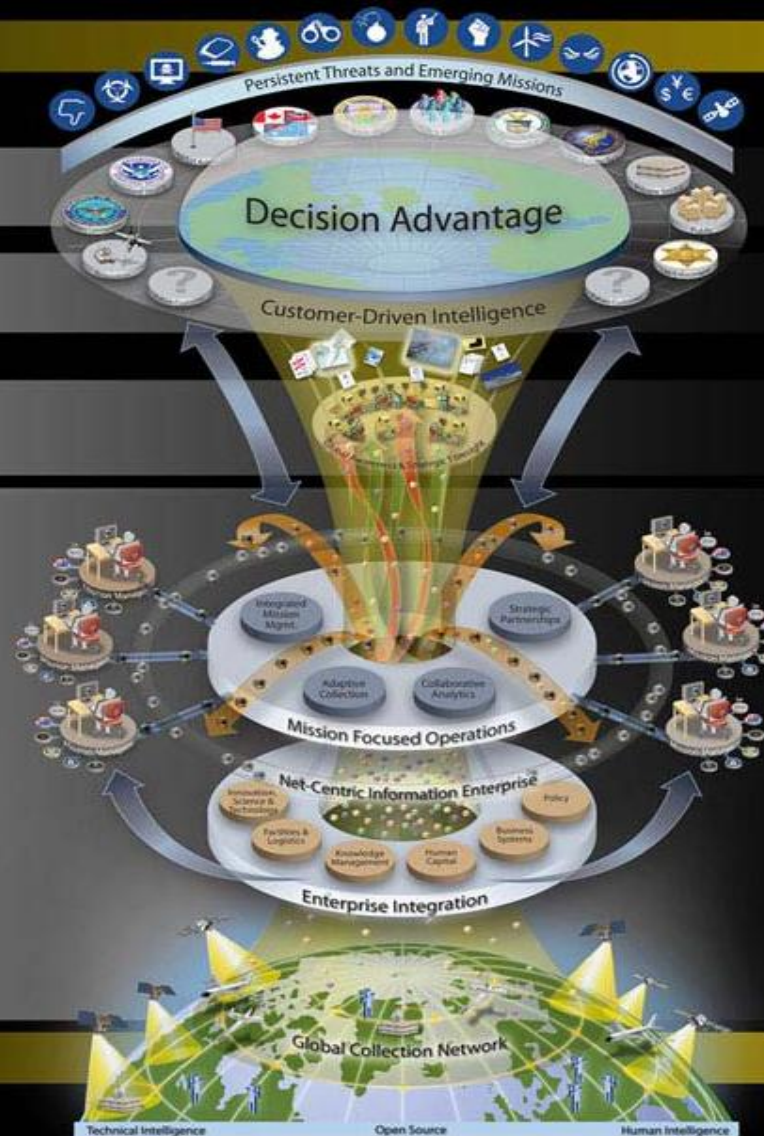
5. Customer-Driven Intelligence

4. Mission Focused Operations

3. Net-centric Information Enterprise

2. Enterprise integration

1. Global Collection Network



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

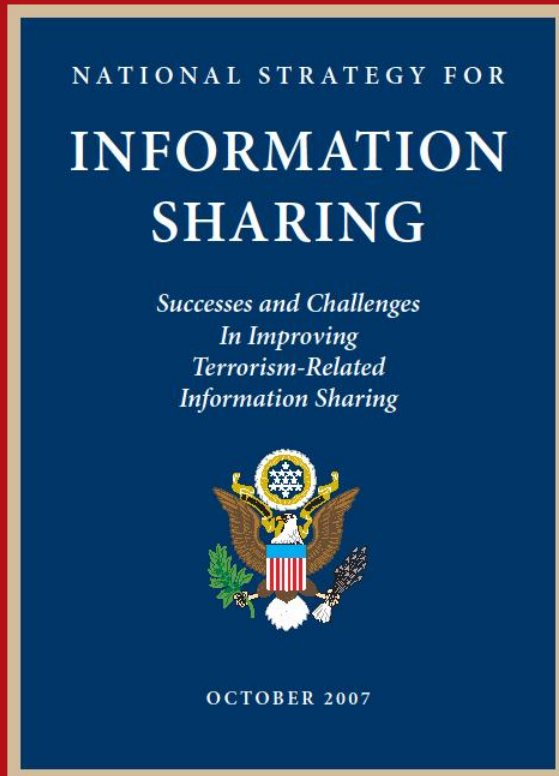
Co-chair

Vladimir Klimov

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



US/EU Agreement

National Strategy for Information Sharing

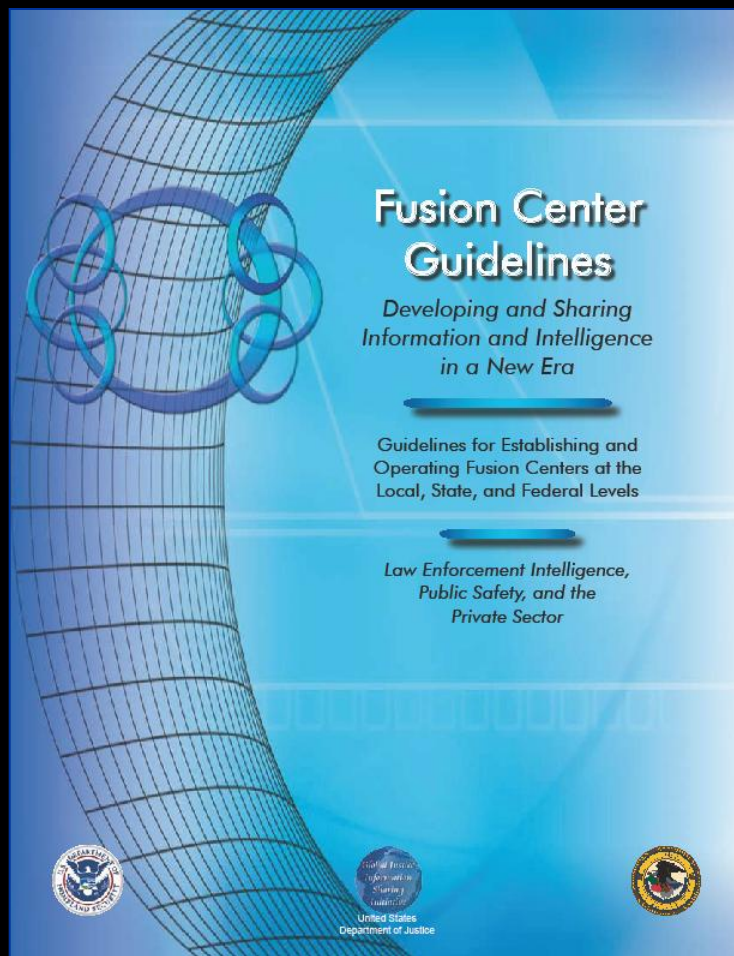


“Providing *reports* and awareness training to State, local, and tribal authorities regarding strategic goals, operational capabilities, and methods of operation utilized by international and domestic terrorist organizations so that local events and behaviors can be viewed within the context of potential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

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

Fusion Centers - Intelligence Gathering

Fusion Center Guidelines



- Developing and Sharing Information and Intelligence in a **New Era**
- 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 H Security Advisory Council (HSAC) Intelligence and In Sharing Working Group to develop intelligence and in sharing guidelines, based on specific presidential dir local, state, and federal agencies creating fusion cent directives provide guidance to local and state entities prevention and response to criminal and terrorist acti The recommendations and findings resulting from HS Intelligence and Information Sharing Working Group support the expansion of the Fusion Center Guidelin safety and private sector entities.

Subsequent to the efforts of the Law Enforcement Int FCFG and HSAC, the Public Safety FCFG was creat the purpose of integrating the public safety compone the Fusion Center Guidelines. Members of the focus concentrated on the need for information and intellig between law enforcement and public safety commu This group endorsed the guidelines developed by the Enforcement Intelligence FCFG and offered suggest 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 g With 85 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.

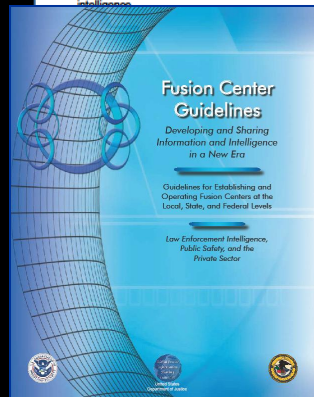
All levels of government, the private sector, and nongovernmental organizations must work together to prepare for, prevent, respond to, and recover from terrorist and criminal events. Through

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 attacks.

**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

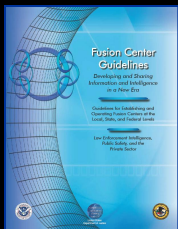


Members (Global) do not justice al Criminal icy and vice Decision information Language represents the country, tards-based ice community oration in a

oip.gov

Fusion Center

tion in a New Era



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.

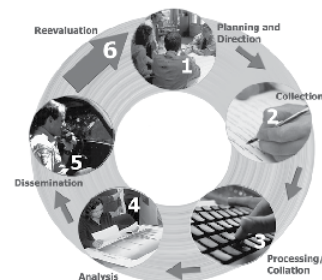
The NCISP provides model standards and policies, recommends methodologies for sharing classified reports, and recommends a nationwide sensitive but unclassified (SBU) communications capability for criminal intelligence sharing. The Plan is a living document that provides local, state, tribal, and federal 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 process in which all agencies work to improve the safety of

- 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

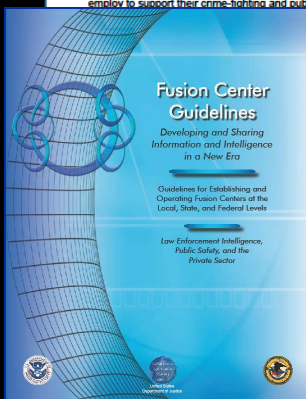


Intelligence-led policing enhances law enforcement and their efforts. Intelligence-led policing allows law

and the criminal

Starting: Excellence
Police 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
- Deconfliction 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 (JTTF), 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)
- Criminal Justice agencies



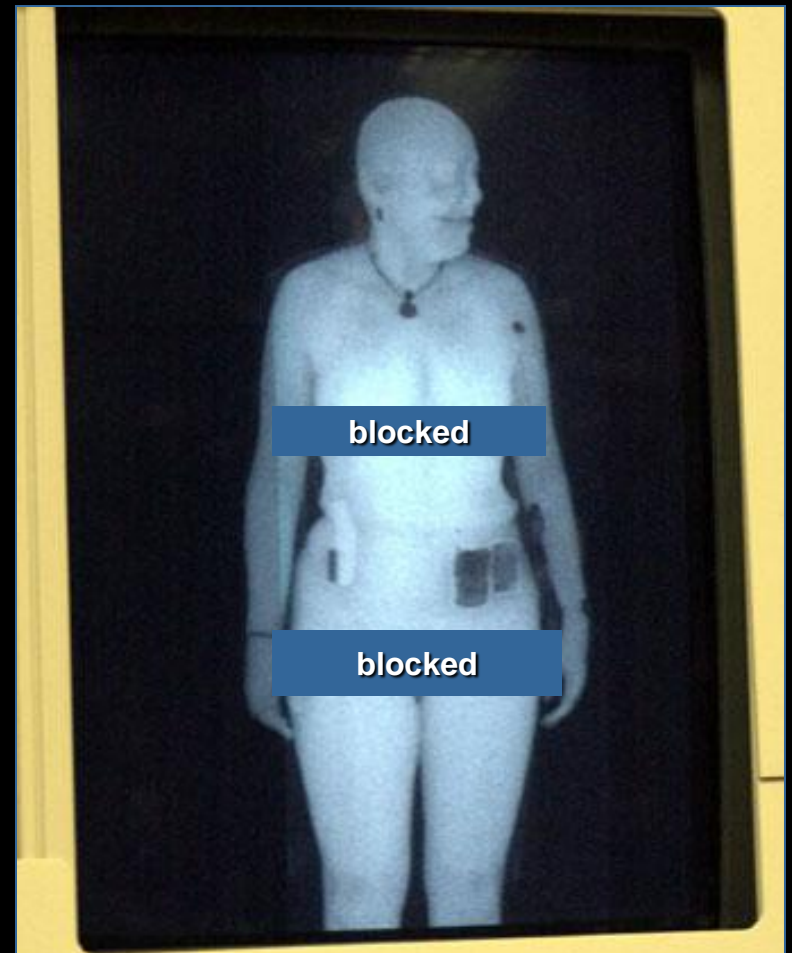
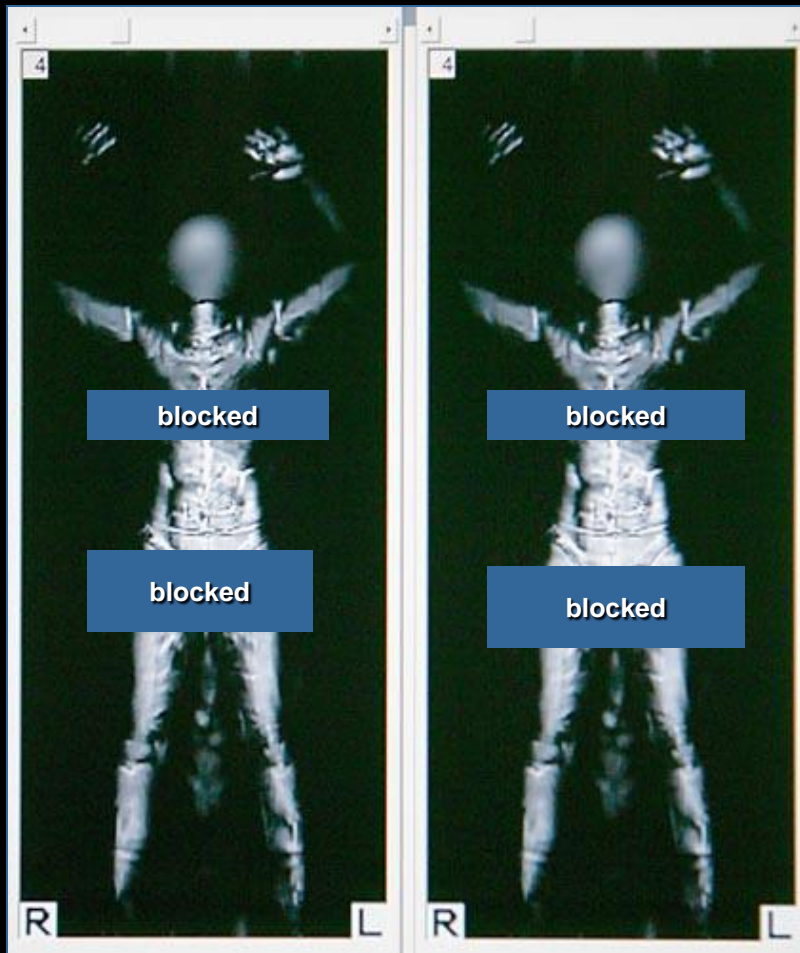
Leverage the databases, systems, and networks available via participating entities to maximize information sharing

- 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

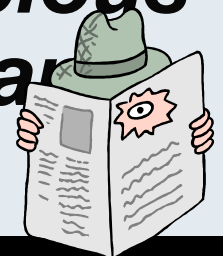
SAR – Suspicious Activity

“Fusion Centers shall develop, implement, and maintain a plan to support the establishment of a

New DHS Initiative for 2010:

“If You See Something, Say Something” Campaign

consistent with the Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project”



Everyone's a Terrorist

2009 MIAC Report

MISSOURI INFORMATION ANALYSIS CENTER
Jeremiah W. (Jay) Nixon Governor
John M. Britt Director, DPS
James F. Keathley Colonel, MSH
Van Godsey Director, MIAC

MISSOURI STATE HIGHWAY PATROL

MIAC STRATEGIC REPORT
02/20/09
The Modern Militia Movement

Modern Militia Movement:

The Militia Movement began in the 1980's and reached its peak in 1996. Several social, economic, and political factors contributed to the surge in militia participation in the 1990's. The primary motivator for the movement was the farm crisis of the 1980's, which caused the destruction of 3/4 of a million small to medium size family farms. Overall, 11 million Americans lost their jobs during this time period.

Academics contend that female and minority empowerment in the 1970s and 1960s caused a blow to white male's sense of empowerment. This, combined with a sense of defeat from the Vietnam War, increased levels of immigration, and unemployment, spawned a paramilitary culture. This caught on in the 1980's with injects such as Tom Clancy novels, Soldier of Fortune Magazine, and movies such as Rambo that glorified combat. This culture glorified white males and portrayed them as morally upright heroes who were mentally and physically tough.

It was during this timeframe that many individuals and organizations began to concoct conspiracy theories to explain their misfortunes. These theories varied but almost always involved a globalist dictatorship the "New World Order (NWO)", which conspired to exploit the working class citizens. United Nations troops were thought to already be operating in the United States in support of the NWO. Much of this rhetoric would become anti-Semitic claiming that the Jews controlled the monetary system and media, and in turn the "Zionist Occupied government (ZOG)". The Militia of Montana (MOM) became a key organization in pushing rightwing rhetoric and informing individuals on how to form militia organizations.

A series of incidents in the early 1990's caused a surge in militia participation. The 1992 standoff between federal authorities and the Weaver family at Ruby Ridge, Idaho became a spark for the movement. On August 14, 1992, a 12 day standoff began that would result in the death of one federal agent and the wife and son of Randy Weaver. The following February, a 51-day siege would occur at the Branch Davidian compound in Waco, Texas, resulting in the death of 82 Davidians and four law enforcement agents. In November of 1993, the enactment of the Brady Handgun Violence Prevention Act of 1992 additionally fueled the movement. The movement reached its peak in 1996 with over 850 groups believed to be operating within the US.

Noteworthy militia activity from 1995 to 1999:

- 11/09/95, Oklahoma Constitutional Militia members are arrested as they plan to bomb the Southern Poverty Law Center (SPLC), news, bars, and abortion clinics.

Info Source: SPLC

ARA was also associated with 22 bank robberies between 1994 and 1996.

UNCLASSIFIED/LAW ENFORCEMENT SENSITIVE (U//LES)

2009 Rightwing Extremism

U.S. DEPARTMENT OF HOMELAND SECURITY

Assessment

(U//FOUO) Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment

VIRGINIA FUSION CENTER
State Federal Local Private
SECURITY LAW ENFORCEMENT

2009 VIRGINIA TERRORISM THREAT ASSESSMENT

COMMONWEALTH OF VIRGINIA
DEPARTMENT OF STATE POLICE
VIRGINIA FUSION CENTER

MARCH 2009

LAW ENFORCEMENT SENSITIVE

Fusion Standards Study 2 - June 2010 RFI (request for information)

- **Decision Fusion**...provides analysts an environment of interoperable services for situation assessment, impact assessment and decision support, based on **information from multiple sensors and databases**, e.g., multi-INT sources. The study includes recent advances such as **social networking for decision fusion**.
- Though the focus of the study is on military intelligence (“INT”), decision fusion is relevant to **business intelligence, urban planning, and many other domains**.

"Multi-INT Examples for an urban situation"

HUMINT	OSINT	SIGINT	GEOINT	MASINT
tips	political climate	intercepted audio, imagery or video	video and imagery	seismic, magnetic, chemical, and other physical signatures
informant reports	population sentiment			
patrol debriefs	culture	signal frequency	vehicle and building locations	event occurrence
links and relationships	TV/radio broadcasts			
coordinates	websites			

Multi-Source Intelligence

Multi-INT information

- Information available to an operations node is not just multi-source, but is from multiple intelligence collection types (multi-INT). Intelligence sources are people, documents, equipment, or technical sensors, and can be grouped according to intelligence disciplines (Table 2).

Table

Otherwise known as

“Living in a Surveillance Society”

- Human intelligence (HUMINT);
- Geospatial intelligence (GEOINT), including imagery intelligence
- Signals intelligence (SIGINT);
- Measurement and signature intelligence (MASINT);
- Open-source intelligence (OSINT);
- Technical intelligence (TECHINT);
- Counterintelligence (CI).

Fighting Terrorism,
Or Something Else?

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

Henry Kissinger, May 31, 2007 Conference, Istanbul



Eliminate Stovepipes

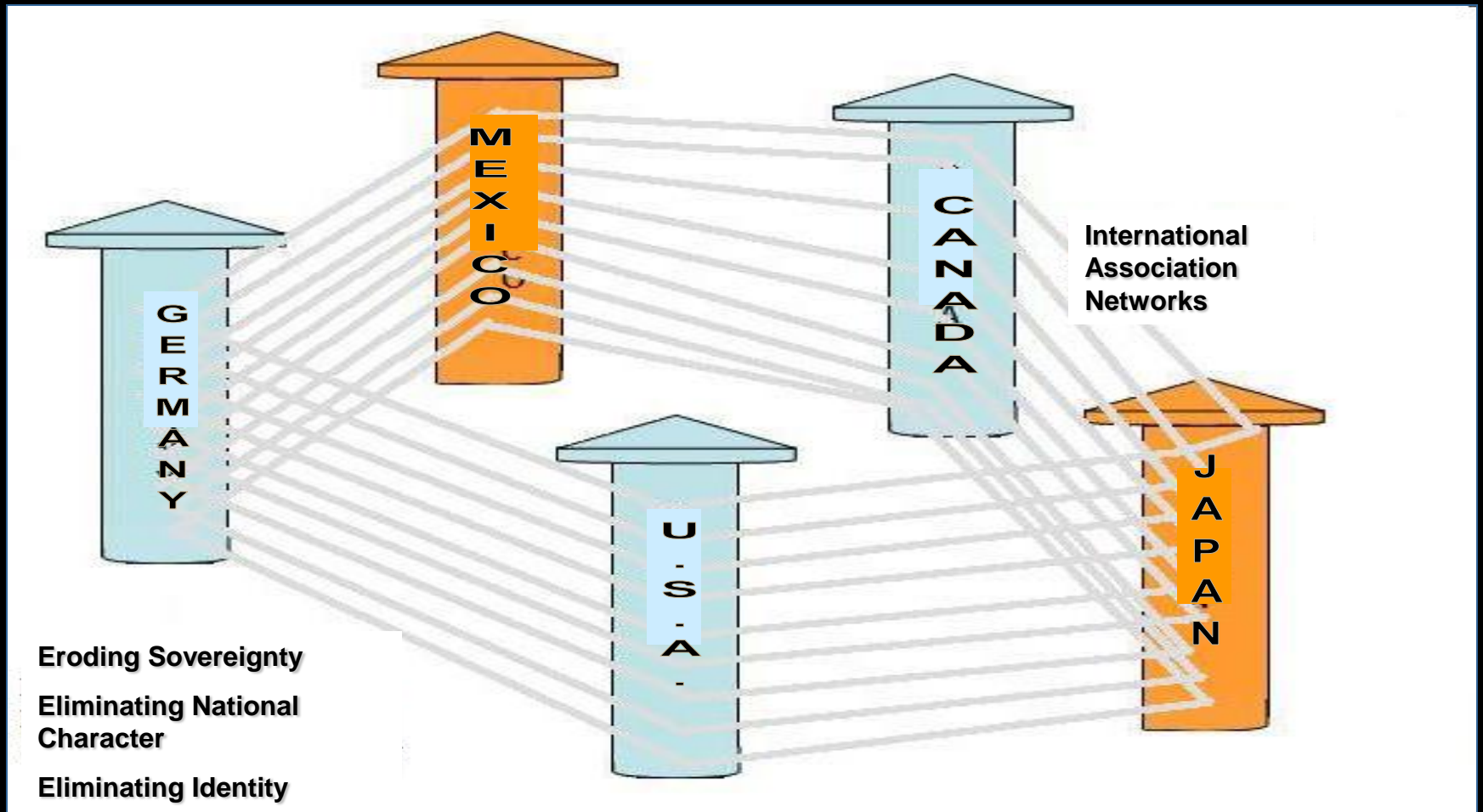
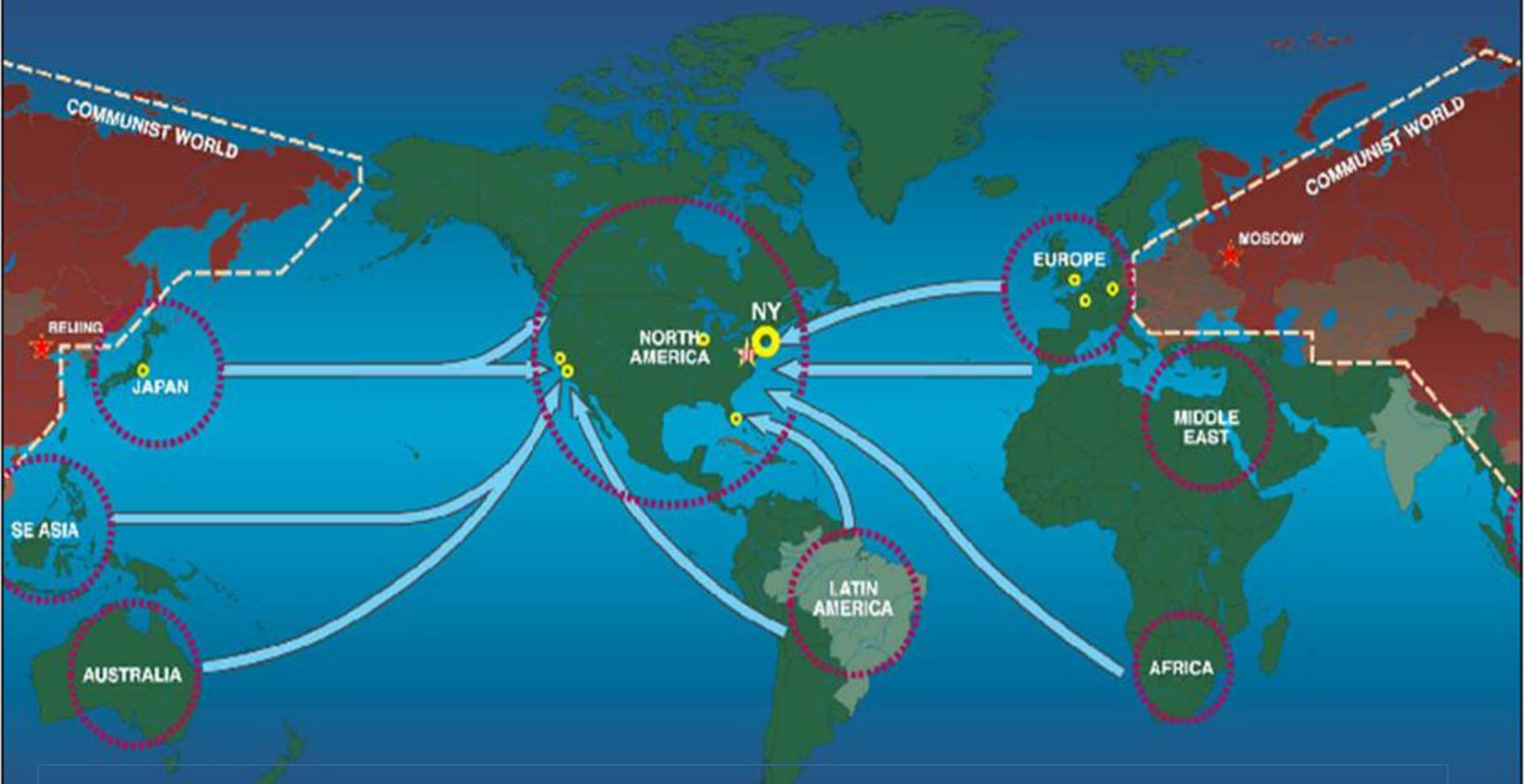


Diagram courtesy V.L. Davis, researcher

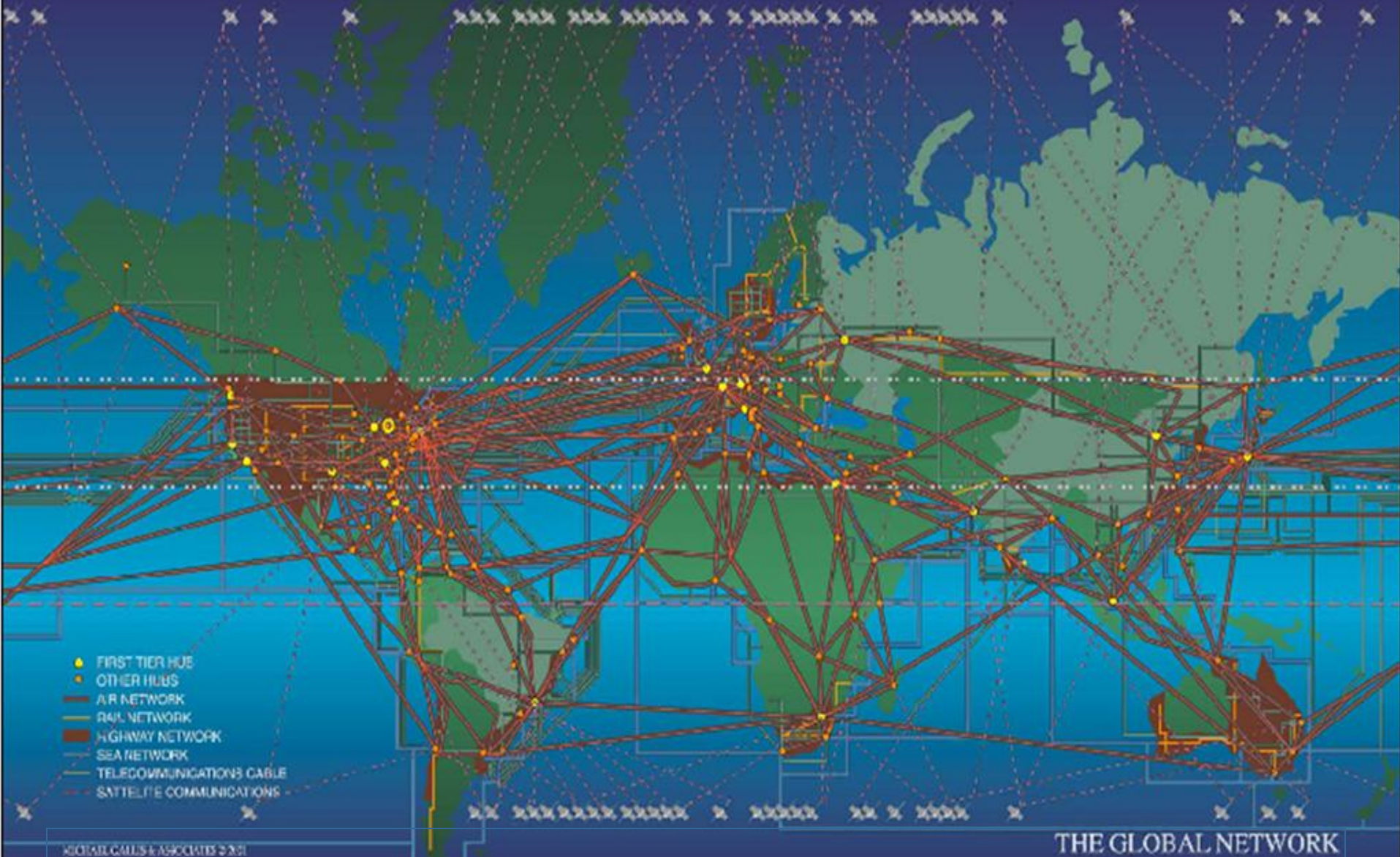
FREE WORLD



Slide Source: Michael Gallis Presentation at a 2008 NASCO Conference.

DIVIDED WORLD (BEFORE 1990)

A Globalist's World: 5 Trading Blocks

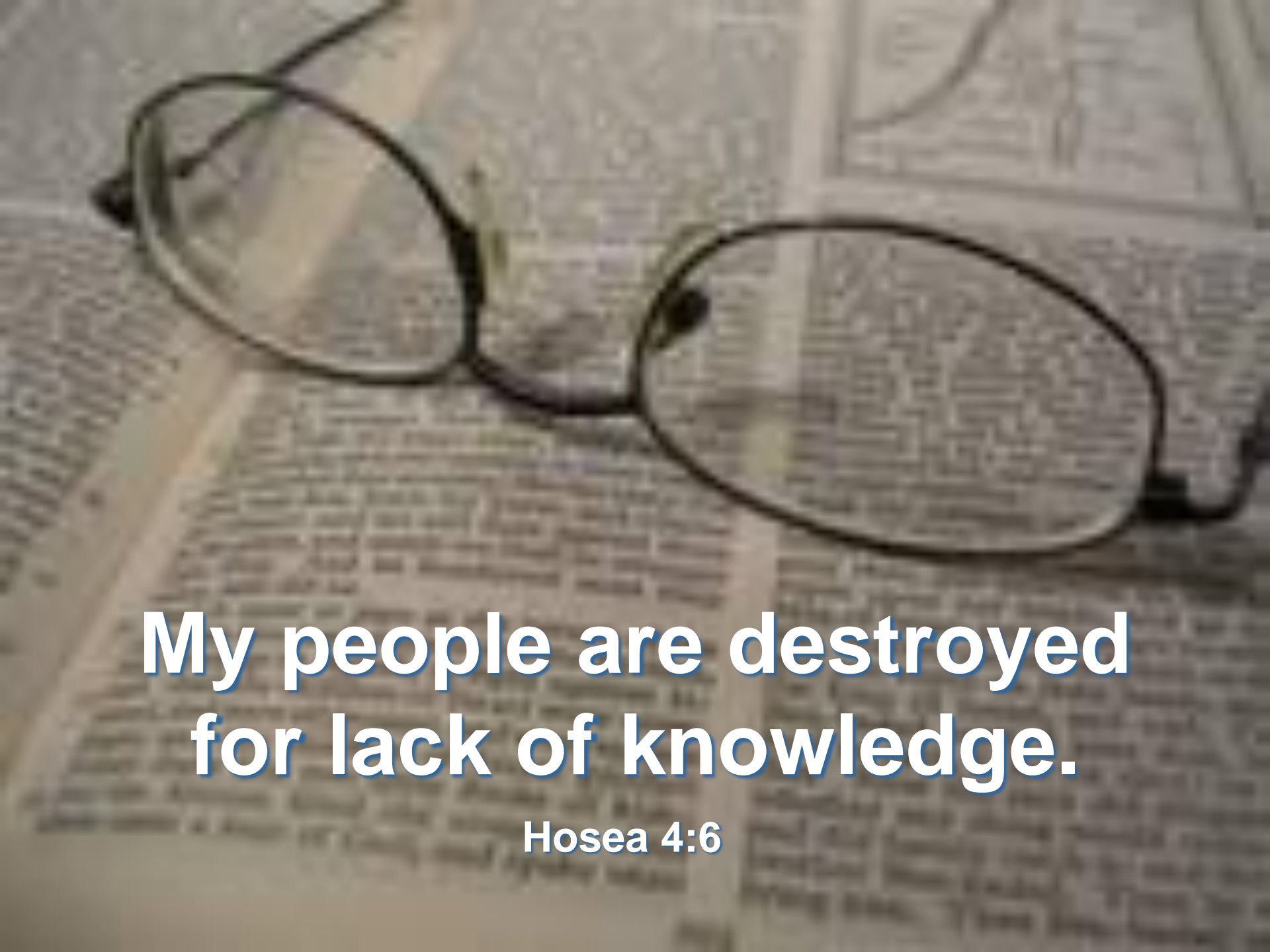


Slide Source: Michael Gallis Presentation at a 2008 NASCO Conference.

Corporate Considerations vs. Constitutional Sovereignty



Conclusion

A pair of black-rimmed glasses with oval lenses is resting on an open newspaper. The newspaper's text is visible but blurred in the background. The glasses are positioned horizontally across the upper half of the frame.

**My people are destroyed
for lack of knowledge.**

Hosea 4:6

Action

- **Get your own house in order**
- **Minimize electronic data exposure – i.e. use of social networking, online medical information, and online financial transactions**
- **Stop using Credit Cards - Pay cash**
- **Try ‘low-tech’ methods of communication**
- **Lobby your state legislatures against the further collection of personal information, i.e. biometric samples**
- **Join OK-SAFE, or a local grassroots group**
- **Pay attention to what is happening**

Primary Sources

