U.S. DEPARTMENT OF HOMELAND SECURITY

HOMELAND SECURITY ADVISORY COUNCIL

INTELLIGENCE AND INFORMATION SHARING INITIATIVE:

HOMELAND SECURITY INTELLIGENCE & INFORMATION FUSION

APRIL 28, 2005

JOSEPH J. GRANO, JR.
CHAIRMAN
HOMELAND SECURITY ADVISORY COUNCIL

MITT ROMNEY
CHAIRMAN
INTELLIGENCE & INFORMATION SHARING WORKING GROUP

WILLIAM H. WEBSTER
VICE CHAIRMAN
HOMELAND SECURITY ADVISORY COUNCIL

JOHN COHEN
EXECUTIVE DIRECTOR
INTELLIGENCE & INFORMATION SHARING WORKING GROUP

DANIEL J. OSTERGAARD
EXECUTIVE DIRECTOR
HOMELAND SECURITY ADVISORY COUNCIL

MICHAEL J. MIRON
DIRECTOR
INTELLIGENCE & INFORMATION SHARING WORKING GROUP

Background

Effective terrorism-related prevention, protection, preparedness, response, and recovery efforts depend on timely, accurate, and actionable information about who the enemies are,[1] where and how they operate, how they are supported, the targets the enemies intend to attack, and the method of attack they intend to use. This information should serve as a guide for efforts to:

- Identify rapidly both immediate and long-term threats;
- Identify persons involved in terrorism-related activities; and
- Guide the implementation of information-driven and risk-based prevention, response, and consequence management efforts.

Terrorism-related intelligence is derived by collecting, blending, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. There is no single source for terrorism–related information. It can come through the efforts of the intelligence community; Federal, State, tribal, and local law enforcement authorities; other government agencies (e.g., transportation, healthcare, general government), and the private sector (e.g., transportation, healthcare, financial, Internet/information technology).

For the most part, terrorism-related information has traditionally been collected outside of the United States. Typically, the collection of this type of information was viewed as the responsibility of the intelligence community and, therefore, there was little to no involvement by most State and local law enforcement entities. The attacks of September 11, 2001, however, taught us that those wanting to commit acts of terrorism may live in our local communities and be engaged in criminal and/or other suspicious activity as they plan attacks on targets within the United States and its territories. Important intelligence that may forewarn of a future attack may be derived from information collected by State, tribal, and local government personnel through crime control and other routine activities and/or by people living and working in our local communities. Successful counterterrorism efforts require that Federal, State, tribal, local, and private-sector entities have an effective information sharing and collaboration capability to ensure they can seamlessly collect, blend, analyze, disseminate, and use information regarding threats, vulnerabilities, and consequences in support of prevention, response, and consequence management efforts.

The President and the U.S. Congress have directed that an information sharing environment (ISE) be created in the next two years to facilitate information sharing and collaboration activities within the Federal Government (horizontally) and between Federal, State, tribal, local, and private-sector entities (vertically). The concept of intelligence/information fusion has emerged as the fundamental process (or processes) to facilitate the sharing of homeland security-related information and intelligence at a national level, and, therefore, has become a guiding principle in defining the ISE.

[1] Including their capabilities, intentions, strengths, weaknesses.

Homeland Security Intelligence/Information Fusion

Homeland security intelligence/information fusion is the overarching process of managing the flow of information and intelligence across levels and sectors of government and the private sector to support the rapid identification of emerging terrorism-related threats and other circumstances requiring intervention by government and private-sector authorities. It is more than the one-time collection of law enforcement and/or terrorism-related intelligence information and it goes beyond establishing an intelligence center or creating a computer network. Intelligence fusion is a clearly defined, ongoing process that involves the delineation of roles and responsibilities; the creation of requirements; and the collection, blending, analysis, timely dissemination, and reevaluation of critical data, information, and intelligence derived from the following:

- Autonomous intelligence and information management systems (technical and operational) established to support the core missions of individual Federal, State, local, tribal, and government entities;
- General public; and
- Private-sector entities.

The fusion process is a key part of our nation's homeland security efforts. This process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. Simultaneously, it supports efforts to address immediate and/or emerging, threat-related circumstances and events. Although the collection, analysis, and dissemination of terrorism-related intelligence is not the sole goal of the fusion process, one of the principal outcomes should be the identification of terrorism-related leads—that is, any nexus between crime-related and other information collected by State, local, tribal, and private entities and a terrorist organization and/or attack. The fusion process does not replace or replicate mission-specific intelligence and information management processes and systems. It does, however, leverage information and intelligence developed through these processes and systems to support the rapid identification of patterns and trends that may be indicative of an emerging threat condition. Although the primary emphasis of intelligence/information fusion is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to State, tribal and local entities is that it will support ongoing efforts to address nonterrorism related issues by:

- Allowing State and local entities to better identify and forecast emerging crime, public health, and quality-of-life trends;
- Supporting targeted law enforcement and other multidisciplinary, proactive, risk-based and community-focused, problem-solving activities; and
- Improving the delivery of emergency and nonemergency services.

Effective intelligence/information fusion requires the following:

- The use of common terminology, definitions, and lexicon by all stakeholders;
- Up-to-date awareness and understanding of the global and domestic threat environment;
- A clear understanding of the links between terrorism-related intelligence and nonterrorism-related information (e.g., flight school training, drug trafficking) so as to identify those activities that are precursors or indicators of an emerging threat;
- Clearly defined intelligence and information requirements with the Federal intelligence community that prioritize and guide planning, collection, analysis, dissemination, and reevaluation efforts;
- Identifying critical information repositories[2] and establishing the processes, protocols, procedures, and technical capabilities to extract information and/or intelligence from those repositories;
- Reliance on existing information pathways and analytic processes as possible;
- All-hazards and all-crimes approach to defining information collection, analysis, and dissemination;
- Clear delineation of roles, responsibilities, and requirements of each level and sector of government involved in the fusion process;
- Understanding and elimination of impediments to information collection and sharing (i.e., it should be a priority for the Federal Government to provide State, local, and tribal entities unclassified terrorism-related information/intelligence so that it can be integrated into statewide and/or local fusion efforts);
- Capacity to convert information into operational intelligence;
- Extensive and continuous interaction with the private sector and with the public at large;
- Connectivity (technical and/or procedural) with critical intelligence streams, analysis centers, communication centers, and information repositories at all levels of classification as necessary;
- Extensive participation of subject-matter experts (SMEs) in the analytical process; and
- Capacity and commitment to ensure aggressive oversight and accountability so as to protect against the infringement of constitutional protections and civil liberties.

[2] These repositories are not limited to those maintained by law enforcement entities. For example, critical information may be contained in systems supporting medical examiners (unattended death), public health entities, emergency rooms (information similar to the Drug Abuse Warning Network program), environmental regulatory inspectors, transportation entities, housing inspectors, health inspectors, building code inspectors, etc.

Participants in the Fusion Process

To some degree, the fusion process involves every level and sector (discipline) of government, the private-sector, and the public. The level of involvement from these participants will vary based on specific circumstances. Some disciplines, such as law enforcement, represent a core component of the fusion process because of the relationship between crime and because, in many cases, law enforcement authorities are best-suited to coordinate statewide and local fusion efforts. Minimally, the fusion process should be organized and coordinated on a statewide level and each State should establish and maintain an analytic center to facilitate the fusion process. Each major urban area (as defined by the Urban Area Security Initiative [UASI] program) may want to establish a similar capacity ensuring it is interlinked with the fusion process established by the State. Other localities, tribal governments, and even private-sector entities should develop a process to interlink and participate in these statewide (or UASI) fusion efforts. The public should be engaged through public education programs that describe what they should look for and what to do if they observe suspicious activities or circumstances.

Efforts should be organized and managed on a geographic basis and scalable so adjustments can be made based on changes in the operating and/or threat environment. While national standards and guidelines should guide the institutionalization of the process, the actual technological infrastructure and operational protocols used by individual jurisdictions should be based on the management structure, specific needs, and capabilities of each individual jurisdiction.

Stages of the Fusion Process

Fusion is cyclical process that includes the following stages and activities:

- **Management/Governance**
  - Define a management structure (e.g., who is in charge, what entity will manage and coordinate daily activities).
  - Identify core (permanent) and ad hoc stakeholders.
  - Design a governance structure advisory committee (multidisciplinary and multilevel of government).
  - Define goals and objectives.
  - Develop a process to define information and intelligence collection requirements.
  - Develop the process and necessary memorandums of understanding to communicate requirements.
- **Planning and Requirements Development**
  - Conduct (and update frequently) a comprehensive and compatible risk assessment (threat, vulnerability, and consequence).
  - Identify patterns and trends reflective of emerging threats.
  - Define collection requirements based on results of risk assessments.

- Identify the circumstances or events (e.g., crime, public health) that represent indicators and/or precursors of threats.
- Identify the sources and/or repositories of data and information regarding indicators and precursors.
- Identify the existing capacity to collect key information from existing sources.
- Identify collection gaps and mitigate.
- Define public education, and other activities necessary to enhance situational awareness by the public.
- Develop training for front line law enforcement and other personnel so that they can better identify suspicious activities that may represent planning and/or operational activity by terrorist group.
- Ensure a mechanism exists to support reporting of collected information (e.g., 9-1-1, tipline, Internet, connectivity to key information systems).
- Identify regulatory, statutory, privacy, and/or other issues that impede collection and sharing of information.
- Develop (in partnership with private-sector officials) detailed knowledge of vulnerabilities and consequence in the private sector to possible terrorist attacks to assess the likelihood of attack, the likely methods of attack, the likely equipment and substances used to carry out such an attack, and identify planning activities.

- **Collection**

  - Communicate collection requirements to relevant State, tribal, local, and private-sector entities.
  - Implement situational awareness activities (e.g., training, public education).
  - Mitigate impediments to collection.
  - Compile classified and unclassified data, information and intelligence generated by people and organizations.
  - Serve as the 24/7/365 initial point of contact for information provided by the U.S. Department of Homeland Security, Department of Defense, Department of Justice, Federal Bureau of Investigation, and other Federal entities (via telephone calls, Homeland Security Information Network/Joint Regional Information Exchange System, LEO, e-mail bulletins, VTC, fax) for the receipt of the following:

    - Immediate threat-specific information (classified and unclassified)
    - Long-term threat information (classified and unclassified)
    - Tactics and methods used by terrorists (classified and unclassified)

  - Integrate with other reporting systems (e.g., 9-1-1, 3-1-1), and establish and maintain further, easy-to-use capability for the public reporting of suspicious activity in conjunction with the Joint Terrorism Task Force (e.g., internet, toll-free tipline).

  - Establish a process to identify and track reports of suspicious circumstances (e.g., pre-operational surveillance, acquisition of items used in an attack).

- **Analysis**

  - Blend data, information, and intelligence received from multiple sources.
  - Reconcile, deconflict data, and validate as to credibility of data, information and intelligence received from collection sources.
  - Evaluate and analyze data and information using SMEs.
  - Identify and prioritize the risks faced by the jurisdiction (e.g., State, local).
  - Produce value-added intelligence products that can support the development of performance-driven, risk-based prevention, response, and consequence management programs.
  - Identify specific protective measures to identify and disrupt potential terrorist attacks during the planning and early operational stages.

- **Dissemination, Tasking, and Archiving**

  - Identify those entities and people (e.g., officials, executives) responsible for developing and implementing prevention, response, and consequence management (public and private) efforts.
  - Provide relevant and actionable intelligence in a timely manner to those entities responsible for implementing prevention, response, and consequence management efforts (public and private sector).
  - Archive all data, information, and intelligence to support future efforts.
  - Support the development of performance-based prevention, response, and consequence management measures.
  - Establish the capacity to track performance metrics associated with prevention, response, and consequence management efforts.
  - Provide feedback to information collectors.

- **Reevaluation**

  - Track the achievement of prevention, response, and consequence management program performance metrics so as to evaluate impact on the risk environment.
  - Update threat, vulnerability, and consequence assessments so as to update the risk environment.
  - Assess effectiveness of national (i.e., Federal, State, tribal, and local) intelligence and information collection requirements process.

- **Modification of Requirements**

- Modify collection requirements as necessary.
- Communicate modifications in a timely manner.

Intelligence and Information Sharing Working Group Members

Chair, Governor Mitt Romney (Homeland Security Advisory Council (HSAC))
Chuck Canterbury (HSAC)
Frank Cilluffo (HSAC)
Maj. General Bruce Lawlor (Ret.) (HSAC)
Mayor Patrick McCrory (HSAC)
Lydia Thomas (HSAC)
Mayor Karen Anderson (State and Local Senior Advisory Committee (SLSAC))
James Dunlap (SLSAC)
Don Knabe (SLSAC)
Peggy Merriss (SLSAC)
Karen Miller (SLSAC)
Mayor Donald Plusquellic (SLSAC)
Michael Carona (Emergency Response Senior Advisory Committee (ERSAC))
Frank Cruthers (ERSAC)
Ellen Gordon (ERSAC)
Phillip Keith (ERSAC)
Paul Maniscalco (ERSAC)
Dr. Allan Zenowitz (Academe, Policy and Research Senior Advisory Committee)
George Vradenburg (Private Sector Senior Advisory Committee)
John Cohen (Office of the Governor, Massachusetts)
Cindy Gillespie (Office of the Governor, Massachusetts)

Fusion Group Subject-Matter Experts

Kenneth Bouche, Colonel State Police, Illinois
Dan Cooney, Captain State Police, New York
George Foresman, Homeland Security Advisor, Virginia
Bart Johnson, Lieutenant Colonel State Police, New York
Fred LaMontagne, Fire Chief, Maine
Pete Modafferi, Chief of Detectives, Rockland County, New York
Steve McGraw, Homeland Security Advisor, Texas
Jim Mcmahon, Homeland Security Advisor, New York
Tom O'Reilly, Office of the Attorney General, New Jersey
Russ Porter, Assistant Director, Department of Public Safety, Iowa
Mark Zadra, Chief of Investigations, Office of Statewide Intelligence, Florida

Homeland Security Advisory Council Staff

Dan Ostergaard, Executive Director, Homeland Security Advisory Council
Rich Davis, Director, Academe and Policy Research Senior Advisory Committee
Jeff Gaynor, Director, Emergency Response Senior Advisory Committee
Katie Knapp, Special Assistant to the Homeland Security Advisory Council
Mike Miron, Director, State and Local Officials Senior Advisory Committee
Candace Stoltz, Director, Private Sector Senior Advisory Committee