Fiscal Year 2008

HOMELAND SECURITY GRANT PROGRAM

SUPPLEMENTAL RESOURCE: FUSION CAPABILITY PLANNING TOOL

February 2008

U.S. DEPARTMENT OF HOMELAND SECURITY

Fusion Capability Planning Tool

Effective prevention efforts depend on the ability of all levels/sectors of government and private industry to collect, analyze, disseminate, and use homeland security-related intelligence. This capacity, known as the "fusion process," serves as the foundation for all state and urban area fusion centers. Accordingly, the establishment of a network of fusion centers to facilitate effective nationwide homeland security information sharing continues to be a top prevention priority in Fiscal Year (FY) 2008.

Funds from the FY 2008 Homeland Security Grant Program (HSGP) utilized to establish / enhance state and local fusion centers must support the following:

- Development of a statewide fusion process that corresponds with the "Global Justice / Homeland Security Advisory Council (HSAC) Fusion Center Guidelines" and the National Strategy for Information Sharing; and
- Achievement of baseline levels of capability as defined by the *Fusion Capability Planning Tool* below.

The *Fusion Center Planning Tool* has been developed based on the "Global Justice / HSAC Fusion Center Guidelines" and provides a streamlined framework of critical fusion process capabilities - the achievement of which will result in each fusion center meeting baseline operational standards. Grantees are encouraged to use the *Fusion Capability Planning Tool* to determine and prioritize areas of improvement, develop strategies to overcome shortfalls, and prioritize the expenditure of funds to address identified areas of improvement. As noted above, the establishment of a baseline capability level within all state and urban area fusion centers continues to be the primary emphasis of FY 2008 HSGP fusion-related guidance and the information below provides a strategic outline that should be utilized to support this goal. In order to achieve a baseline level of capability, each fusion center must possess and/or prioritize efforts and expenditures to achieve the following capabilities:

Management/Governance

- Defined management structure that governs intelligence activities
- Identification of core (permanent) and ad-hoc stakeholders, including engagement with appropriate federal entities (Joint Terrorism Task Forces (JTTFs), Field Intelligence Groups (FIGs), High Intensity Drug Trafficking Area offices (HIDTAs), DHS field components such as Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE), etc.)
- Governance structure (both multi-disciplinary and multi-level of government) and/or some type of multi-disciplinary advisory committee
- Defined goals and objectives to guide collection, analysis, dissemination, and use of intelligence
- Memorandums of Understanding with all stakeholders
- Processes to add or remove stakeholders/partners as the fusion center matures
- Formal processes to define information and intelligence collection requirements
- Defined Concept of Operations, including Mission Statement

- Defined, agreed upon, and auditable Privacy Policy that covers collection, analysis and dissemination
- Funding strategy that will cover operational costs for the next four years

Planning and Requirements Development

- Completion of a regional (or statewide) risk assessment (threat, vulnerability, and consequence)
- Capacity to identify patterns and trends reflective of emerging threats
- Collection requirements based on results of risk assessments
- Capacity to identify the circumstances or events (crime, public health, etc.) that represent "indicators" and/or "precursors" of threats
- Identification of the sources and/or repositories of data and information regarding "indicators" and "precursors"
- Collection of key information from existing sources
- Conduct public education and other activities necessary to enhance "situational awareness" by the public
- Training of frontline law enforcement and other public safety liaison personnel, including non-traditional partners and the public, so that they can better identify suspicious activities that may represent planning and/or operational activity by a terrorist group
- Mechanism to support reporting of collected information (9-1-1, "Tips-line", internet)
- Identification of regulatory, statutory, privacy, and /or other issues that impede collection and sharing of information, including an oversight mechanism to ensure individual privacy and civil liberties are protected
- Identification of and coordination with appropriate response and recovery personnel and operations centers to ensure fusion center activities are coordinated with and can be leveraged to support emergency operation activities, as appropriate, in the event of an incident
- Processes to obtain detailed knowledge from and provide information to homeland security partners and the private sector, including:
    - Vulnerabilities to possible terrorist attack
    - Assessment of the likelihood of attack
    - Likely methods of attack
    - Equipment and substances to carry out such an attack
    - Identification of planning activities

Collection

- Procedures and protocols to facilitate the communication of collection requirements to relevant local, State, and private sector entities
- Implementation of "situational awareness" activities (training, public education, etc.)
- Mitigating of impediments to collection
- Compilation of classified and unclassified data, information, and intelligence generated by individuals and organizations

- Integration of homeland security information (all-threats, all-hazards, and all-crimes) collection efforts with other reporting systems (9-1-1, 3-1-1, etc.)
- Establishment of process to identify and track reports of suspicious circumstances (e.g. pre-operational surveillance, acquisition of items used in an attack)

Analysis

- Blending of data, information, and intelligence received from multiple sources
- Reconciliation, de-confliction, and validation of the credibility of data, information, and intelligence received from collection sources
- Evaluation and analysis of data and information using subject matter experts
- Identification and prioritization of the "risks" faced by the jurisdiction (State, locality, etc)
- Production of value-added intelligence products that can support the development of performance-driven, risk-based prevention, protection, response, and consequence management programs
- Identification of specific preventive and protective measures to identify and disrupt potential terrorist attacks during the planning and early operational stages
- Appropriate training and certification of analysts in accordance with the Minimum Criminal Intelligence Training Standards.

Dissemination, Tasking, and Archiving

- Identification of those entities and individuals (officials, executives, etc.) responsible for developing and implementing prevention, protection, response, and consequence management (public and private) efforts
- Provision of relevant and actionable intelligence in a timely manner to those entities responsible for implementing prevention, protection, response, and consequence management efforts (public and private sector)
- Archiving of all data, information, and intelligence to support future efforts
- Access to Law Enforcment Online (LEO), the Homeland Security Information Network (HSIN), the Regional Information Sharing Systems (RISS), and/or other key information sharing systems
- Development of performance-based prevention, protection, response, and consequence management measures
- Capacity to track performance metrics associated with prevention, protection, response, and consequence management efforts
- Provision of feedback to collectors of information
- Access to a secret enclave where classified systems and secure rooms are available for use

Re-evaluation

- Tracking of achievement of prevention, protection, response, and consequence management program performance metrics so as to evaluate impact on risk environment
- Update of threat, vulnerability, and consequence assessments so as to update risk environment

Modification of Requirements

- Modification of collection requirements as necessary
- Communication of modifications to key stakeholders in a timely manner