National TEW
Resource Center

Resource Guide

Book One: TEW Concept and Overview

National TEW Resource Center

Resource Guide

Book One: TEW Concept and Overview

The National TEW Resource Center is funded by the U.S. Department of Homeland Security's Office of Grants and Training through Cooperative Agreement Award Number 2005-GE-T4-0057.

Table of Contents

Acknowledgements: The National TEW Resource Center would like to acknowledge Lt. John P. Sullivan, Director of the National TEW Resource Center, as the primary author of this document, and the support of the Los Angeles County Sheriff's Department, the U.S. Department of Homeland Secuirty, and the TEW Publications Peer Review Panel.

Preface

This resource book is the first in a series of manuals, case studies, and resource materials describing the Terrorism Early Warning Group (TEW) model and concept of operations. Developed by the National TEW Resource Center in Los Angeles in partnership with the U.S Department of Homeland Security (DHS) and TEW practitioners throughout the United States, these materials are designed to assist individual jurisdictions in understanding and applying the TEW concept. This first volume is an overview of the TEW and its application in day-to-day practice. It is designed primarily for command personnel and decision-makers, and provides an introduction to the TEW and the process of implementation, as well as appendices describing various aspects of operations and applicable resources. This resource book will be followed by additional volumes providing detailed templates for operating a functional TEW, as well as case studies on various facets of TEW operations. Subsequent publications will include a more detailed description and discussion of operational processes for actual TEW staff. Together these materials will form a valuable resource for implementing and operating a TEW.

The TEW and National Information Sharing and Intelligence Fusion Processes: A National Perspective

The National Incident Management System (NIMS) establishes a process for gathering, sharing, and managing information and intelligence as a key incident management characteristic. The National Response Plan (NRP) identifies collection, analysis, and application of intelligence and other information as a key component of mission performance. The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of critical infrastructures and key resource (CI/KR) protection efforts. The National Preparedness Goal (the Goal) reflects the consensus of the homeland security community to achieve appropriate levels of proficiency and the required supply of capabilities for these missions and processes.

In order to better align with these pillars of homeland security doctrine, the TEW and related intelligence fusion processes support the *Prevention, Protection,* *Response,* and *Recovery* mission areas. They also significantly improve homeland security efforts directly related to information sharing and fusion-process target capabilities, based upon the Target Capabilities List (TCL), and four of the eight National Priorities identified in the Goal:

- Expanded Regional Collaboration
- Implement the Interim National Infrastructure Protection Plan
- Strengthen Information Sharing and Collaboration Capabilities
- Strengthen CBRNE Detection, Response, and Decontamination Capabilities

Homeland security intelligence/information fusion refers to the process of managing the flow of information and intelligence across multiple disciplines, 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 criminal and/or terrorism-related intelligence information, and it goes beyond establishing an intelligence center or creating a computer network. It 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 re-evaluation of critical data, information and intelligence derived from the following:

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

The fusion process is a key part of our Nation's homeland security efforts because it supports the implementation of risk-based, information-driven prevention, protection, response, and consequence management programs. At the same time, it supports efforts to address immediate and/or emerging threat-related circumstances and events. While the collection, analysis and dissemination of terrorism-related intelligence is not the sole goal of the fusion process, one of the principle outcomes should be the identification of terrorism-related leads—that is, any "nexus" between crime-related and other information collected by State, local, tribal, or 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. In addition, it contributes to achieving the "common operating picture" accessible across jurisdictions and functional agencies that is a principle of NIMS. 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 and local entities is that it adds continuity to the established spectrum of efforts (field-level to Operations Center) to fuse information, and can be used to support ongoing efforts to address non-terrorism related issues.

Fusion is a cyclical process that includes the following stages:

- Management/Governance
- Planning and Requirements Development
- Collection
- Analysis
- Dissemination, Tasking, and Archiving
- Re-evaluation
- Modification of Requirements

The TEW encompasses the above described fusion process and builds toward a "common operating picture" for a national network of sharing terrorist threat- and incident-related information and intelligence. The TEW, as reflected within this Resource Book, supports and implements the recommended standards, baseline processes, and road maps for enhanced law enforcement, public safety and homeland security information/intelligence sharing activities previously described in the fusion process, and that have been produced through the auspices of the U.S. Department of Justice (DOJ), Bureau of Justice Affairs (BJA), GLOBAL initiative. This includes the following documents:

- The *National Criminal Intelligence Sharing Plan* (NCISP), updated as of June 2005.
- Homeland Security Advisory Council (HSAC), *Intelligence and Information Sharing Initiative*, December 2004.
- HSAC, *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*, April 28, 2005.

- Global Justice Information Sharing Initiative, *Fusion Center Guidelines—Developing and Sharing Information and Intelligence in a New World*, July 2005.

Furthermore, the TEW supports objectives set forth in the *National Intelligence Strategy of the United States* (October 2005), which calls for the U.S. to "…integrate the domestic and foreign dimensions of US intelligence." The strategy also states, "U.S. intelligence elements must focus their capabilities to ensure that State, local, and tribal entities and the private sector are connected to our homeland security and intelligence efforts…" and that "…the Intelligence Community must expand the reporting of information of intelligence value from State, local, and tribal law enforcement entities and private sector stakeholders." The TEW provides a mechanism for the State and local community to fully support and augment Federal and national intelligence and information sharing efforts and *strategic objectives* (both *mission* and *enterprise objectives*), as outlined in the *National Intelligence Strategy of the United States*, which will be further enhanced through the national Information Sharing Environment (ISE).

Additionally, while the TEW is a best practice for implementing information sharing and intelligence fusion processes at the State and local level, while supporting national intelligence and information sharing efforts, it also:

- Supports the intelligence fusion and information sharing activities as described in the NRP
- May serve to support a variety of the nodes and functions outlined within the NIMS.
- Meets and supports the strategic objectives outlined in the *National Security Strategy of the United States* (NSS) and the *National Strategy for Homeland Security* (NSHS), specifically the *Intelligence and Warning* critical mission area and the *Information Sharing and Systems* foundation, as well as the initiatives and visions described within the NSHS.

As such, the TEW is flexible and customizable, and may be implemented to accommodate State and/or local jurisdictional capabilities and/or needs (as they may be required by law or policy of specific localities or States), while supporting national information sharing and intelligence fusion process efforts, initiatives and policies.

The TEW model comports with and recommends consultation with all protected information sharing statutes and regulations including, *28 CFR part 23, the Health Insur-*

ance Portability and Accountability Act (HIPAA), the Critical Infrastructure Information Act of 2002, and any other State or local regulations regarding the collection, storage, and/or release of information.

These documents, policies, strategies, and regulations validate the requirement for, and value of, a coordinated ISE and intelligence fusion process in maximizing information sharing activities across multiple jurisdictions, agencies, and disciplines, including law enforcement, public safety, fire, health, and other homeland security communities at all levels of Government and within the private sector. The documents also contain methodologies and requirements for effectively and efficiently sharing information produced by TEWs and fusion centers in a coordinated and collaborative manner across the Nation, including State, regional, and local levels. However, while these standards and guidelines serve as a guide for the development and implementation of TEWs and fusion centers, the manner in which the process is implemented should be based on the management structure and specific needs and capabilities of each jurisdiction.

Executive Summary

The Los Angeles Terrorism Early Warning Group, known as the TEW, was established in 1996 to fill a void in information and knowledge about terrorism. Local law enforcement and public safety agencies—fire service, medical, and public health agencies—all play roles in anticipating, pre-planning for, preventing and responding to potential terrorist attacks. The TEW was formed as a cooperative vehicle to bring these entities together and to develop and exchange the information needed to recognize potential terrorist threats or incidents of national significance, to create an understanding of specific threats or incidents when they materialize, and to enable command staff to determine appropriate preventive and/or protective measures or an effective response, if necessary.

The TEW concept is driven by the recognition that regional and local agencies are producers, as well as users, of intelligence. It bridges the gap between criminal and operational intelligence with a networked approach that integrates law enforcement, fire, health, and emergency management agencies, and allows it to monitor trends and assess potential threats or indicators of a terrorist attack. It relies on pre-planning for possible incidents and the sharing of information across multiple disciplines and levels of government, including criminal leads, investigative information and open source and classified intelligence to identify threats credible enough to warrant a response and to determine what level of response is required. During an actual threat period or attack, the TEW provides information about the possible consequences and identifies potential courses of action. The TEW builds upon intelligence

> The advantage of implementing a TEW is that minimal participation can reap maximum rewards. Not only are individual TEWs able to analyze information from a variety of sources, but they are also able to provide command staff and local officials with timely, accurate answers to questions about potential acts of terrorism. They are part of a nationwide fusion process and information sharing network that taps into expertise from around the country.

sharing operations and capabilities because it actively involves multiple agencies and disciplines in a systematic process of synthesizing information.

The following precepts form a foundation for individual TEWs and support the need to link them into a national fusion process and information sharing network.

- Intelligence for domestic civil protection (homeland security) is both a top-down and bottom-up process.
- Intelligence must move vertically (top-down and bottom-up) and laterally. There is also a need for bilateral information sharing and cooperation among State, regional, and local law enforcement and public safety agencies that is independent of Federal agencies.
- Local law enforcement, public safety, and health agencies may be the first to observe threat or incident indicators.
- Local responsibility is to protect the public and craft response.
- There is a need for accountability, structure, and guidance for access to and the sharing of information and intelligence products deemed nationally important.
- TEW groups and other State, regional, and local fusion centers compose a nationwide network of partners in collecting processing and disseminating intelligence. This precept recognizes the significant value of local knowledge and resources.

The TEW as a Best Practice

The TEW provides a networked approach to intelligence collection, analysis, fusion, sharing and dissemination. This approach includes the management and governance of these processes and activities, the continual evaluation of plans, processes, and requirements, and their modification, as necessary. It integrates Federal, State, and local agencies, enabling them to develop and share information about terrorist threats. This processed information is known as intelligence.

There are many types of intelligence. The most common variety is criminal intelligence, which is used to support investigations. However, a response to terrorism requires more than investigative support, since an attack will require many response activities. The TEW helps fill these needs by developing what is known as "operational intelligence." Operational intelligence is the processed information needed to understand the current and future situation, as well as the capabilities and intentions of an adversary, thus supporting the ability to effectively deter, prevent, protect against, respond to, and/or recover from an incident.

The TEW bridges criminal and operational intelligence, hence the term "all-source/all-phase fusion" is used to describe its operations. It brings together law enforcement, fire, health, emergency management, and other pertinent agencies to address the intelligence needs for terrorism and critical infrastructure protection. It integrates the local-to-Federal echelons and operates pre-, trans-, and post-incident. It utilizes all available sources to scan and monitor indicators of a potential or imminent attack, as well as trends and activities that have the potential to influence training and/or exercise needs and policy development. During an actual threat period or attack, the TEW provides consequence projection (forecasting) to identify potential courses of action for a Unified Command Structure (UCS). Additionally, the TEW provides an intelligence activity meant to directly support the Incident Command System (ICS) and may serve as a node for the NIMS.

The TEW is organized into six interactive cells: The *Officer-in-Charge* cell provides day-to-day direction and supervision. It also approves the dissemination of intelligence products and interacts with command staff at participating agencies and with the Unified Command Structure at a terrorist, or terrorist-related incident or any other incident of national significance. The *Analysis/Synthesis* cell coordinates assessment activities. It tasks the TEW cells with requests for information and develops their results into advisories, alerts, warnings, or issue-specific white papers. The *Consequence Management* cell assesses the law, fire, and health consequences of actual or potential events and provides intelligence support and technical assistance to centers or other entities that coordinate response activities. The *Investigative Liaison* cell coordinates with other criminal investigative entities. The *Epidemiological Intelligence* cell is responsible for obtaining real-time disease surveillance from public health and agricultural/food surety sources. The *Forensic Intelligence Support* cell uses various technologies to understand a situation and contribute to an overall assessment. This includes a Field Assessment Support Team (FAST), which uses specialized detection and sampling equipment to detect the presence of chemical, biological, radiological, nuclear, or explosive (CBRNE) substances. The FAST also uses sensors and detectors, geospatial intelligence, meteorological information, and information technologies to identify cyber threats.

Implementing A TEW

Investigation of potential threats and/or the response to a terrorist incident is best handled as a collaborative effort. It requires the support and participation of the entire law enforcement community and all related disciplines. Obtaining multi-agency, multidisciplinary cooperation requires personnel with leadership skills and the ability to create relationships and build coalitions. This does not, of course, happen overnight. The first TEW was comprised of two deputies from the Los Angeles County Sheriff's Department (LASD) and a handful of representatives from area law enforcement agencies and related disciplines. This group met monthly to share intelligence about possible threats. As the TEW evolved, and particularly after the terrorist attacks of September 11, 2001, more agencies began to contribute resources; funds were directly allocated as the TEW proved its value.

It is important to remember that individual TEWs can range in complexity from small information-sharing forums to full-time multi-agency, multidisciplinary intelligence fusion and analysis centers. The TEW concept is scalable, allowing

The Changing Face of Terrorism

It was August 1996 and Osama bin Laden had issued his first fatwa, urging followers to conduct global terrorist attacks against the U.S. and its citizens. Deputy John P. Sullivan and Deputy Larry Richards were watching as the face of terrorism changed. They knew the small criminal conspiracies that had been the hallmark of most terrorist incidents were probably a thing of the past. The emerging threat appeared to be coming from complex networks, like al-Qaeda, which was not one group but a network of multiple groups. Sullivan and Richards knew the only way to deal with a terrorist network was to create a network of their own, and that information would be the key.

The first TEW meeting was held in October 1996. Representatives of the LASD, FBI, LAPD, the law enforcement branch of California's Office of Emergency Services, and several academic and research institutions attended. The following month the group added representatives from the fire service, public health, public works, and neighboring law enforcement agencies. Initially, the TEW aimed to develop relationships that allowed each agency to share information with one another. Its ultimate goal, however, was to fuse different intelligence disciplines to share information, investigate emerging threats, create sample scenarios of different types of attacks, train to respond to those attacks, and provide tactical support to responding agencies.

each TEW to develop its capabilities based on local threats, needs, and resources. For example, the Los Angeles region is considered a high threat area and therefore is supported by a full-time TEW staff. Rural or remote areas, which may be considered less vulnerable, may not require as many personnel or resources. Yet these TEWs are still considered an important link in the national network and are essential to the nationwide sharing of information and intelligence across multiple disciplines and levels of government.

The advantage of implementing a TEW is that minimal participation can reap maximum rewards. Not only are individual TEWs able to provide command staff and local officials with timely, accurate answers to questions about potential acts of terrorism, they are part of a nationwide network that taps into expertise from around the country. Ultimately, each individual TEW will link within a nationwide network that processes and shares information laterally (department to department, TEW to TEW, TEW to State/regional/local fusion centers), and vertically (top-down from Federal agencies, and bottom-up from local agencies to the Federal and State levels).

The process of developing and implementing TEWs throughout the Nation and coordinating/linking these TEWs with State, regional, and local fusion centers to create a national network has been supported by the DHS Office of Grants and Training (G&T), formerly the Office for Domestic Preparedness (ODP). The DHS TEW Technical Assistance (TA) Expansion Program provides technical assistance and training, as well as expansion workshops, ongoing subject matter expert (SME) support, and resources for prospective jurisdictions interested in implementing a TEW.

This resource book is intended to provide policy, management and command personnel with an overview of the TEW, which evolved from an *ad hoc* coordinating structure that conducted monthly meetings and worked through committees to conduct assessments. This team evolved into a standing group that was activated for specific threats. It is now a full-time intelligence fusion center. The lessons learned from the experience of establishing and refining the LA TEW is recounted here. It is hoped that it can be used to provide a template to facilitate the development and coordination of TEWs and fusion centers across the Nation.

"TEWs are essential to the nationwide sharing of information and intelligence across multiple disciplines and levels of government."

Chapter One: Introduction

History and Evolution of the Los Angeles TEW

Los Angeles County is home to more than 10 million people. It contains 88 separate cities, including Los Angeles (the largest), Pasadena, and Long Beach. Ranging from the "desert to the sea," Los Angeles County is home to the ports of Los Angeles and Long Beach, several airports including the Los Angeles International Airport (LAX), oil refineries, food distribution hubs, entertainment and cultural facilities, and a complex transportation system including railways, a subway, and freeways. The area is served by 47 law enforcement agencies (including the sheriff's department), 35 fire departments and three public health agencies, as well as numerous utilities, water systems, emergency management and public works agencies, as well as their partners at the Federal and State levels.

Each agency in the region has a specific focus and expertise. Law enforcement patrol neighborhoods. Fire departments provide fire suppression, hazardous materials response, urban search and rescue, and emergency medical services. Public health agencies monitor public health and the progress of

Who is In Charge?

It is important to note that there is no one entity in charge of the LA TEW. Although the LASD implemented the TEW, provides the largest contingent of its staff, and acts as the group's Secretariat, the TEW is an independent function staffed by members of the area's law enforcement agencies and relevant disciplines. This includes members from the fire services, public health, and emergency management. Although the TEW staff is detailed full-time from their respective agencies, they remain in the employ of their agencies. This kind of widespread, multijurisdictional, multidisciplinary participation is evidence of the Los Angeles Operational Area's willingness to dedicate resources to homeland security and the war on terrorism. The LA TEW ultimately will be housed in the Joint Regional Intelligence Center (JRIC) with members of the FBI/JTTF, LASD, LAPD and representatives of other Federal and State intelligence agencies.

disease. Emergency management agencies coordinate major disaster responses to both natural occurrences and intentional attacks; in many ways, a terrorist attack is an intentional disaster. The Federal Bureau of Investigation (FBI) is the lead Federal investigative agency for terrorism. The California Highway Patrol (CHP) protects freeways and bridges. The United States Coast Guard (USCG) protects the seaports. The Transportation Security Administration (TSA) and local and airport police secure the airports. The Postal Inspection Service protects the postal and shipping system. The Bureau of Immigration and Customs Enforcement (ICE) secures the borders and ports.

Each of these agencies has a role in prevention, protection against, response to, and/or recovery from terrorist threats or incidents. In fact, no one agency can do it alone. Comprehensive efforts to prevent, protect against, respond to and recover from attacks require many unique and specialized skills. Law enforcement, fire, and health services, together with government and private entities also have unique information requirements that help them perform their individual and collective tasks in a coordinated and effective manner.

In order to build upon the domain expertise and capabilities of the entire community, the Los Angeles TEW was established. It brings together representatives of the LASD, the Los Angeles Police Department (LAPD), the FBI, the Los Angeles Fire Department, the Los Angeles County Fire Department, the Los Angeles County Department of Health Services, Los Angeles County Police, the CHP, Los Angeles World Airport Police, and individual law enforcement and fire agencies. Together, they form a team that develops the information and intelligence needed to coordinate terrorism prevention, protection, and response activities, and that links with surrounding counties, cities, regions, States, and other similar efforts across the Nation.

The LA TEW currently has a full-time cadre comprised of representatives contributed by participating agencies. The TEW holds monthly meetings to foster coordination and skills development, and coordinates a network of Terrorism Liaison Officers (TLOs), who are members of the county's law enforcement, fire service, and health agencies. TLOs serve as the conduit through which threat information flows to the TEW for assessment, and that carries actionable intelligence from the national level and the TEW to field personnel. TLOs also coordinate with private critical infrastructure and industry partners, such as electric companies, oil refineries, banks or entertainment facilities. Private sector partners are also encouraged to establish Infrastructure Liaison Officers (ILOs), who interact with the TEW and the network of TLOs.

This framework recognizes that law enforcement officers and firefighters are the first link to the public. Their expertise and familiarity with the community can be supported with strategic analysis and intelligence from the TEW. Likewise, the information coming from these first responders helps the TEW understand what is happening on the street and in the community. TEW staff can then alert field personnel, through the TLOs, about potential terrorist activities with intelligence that is based on specific threat information and its monitoring of regional, national, and global trends.

The TEW

The TEW was established to address the challenges of contemporary terrorism. It is based on the premise that intelligence is more than "secret information" about an adversary. Intelligence that addresses contemporary threats must go beyond mere descriptions of the actors. It must also provide a range of users (investigators, emergency responders, strategic, and tactical planners, etc.) with accurate information about the situation they are managing.

This information takes many forms and comes from a variety of sources. Raw information is often ambiguous, frequently inaccurate, and must be placed into context so it can be used to inform sound decision-making. Intelligence is assessed information provided to decision-makers to help them understand the current and evolving situation so they can allocate personnel and resources, and craft a course of action based upon the overall risk. This includes information about threats (terrorists and their organizations), vulnerabilities and potential targets, and consequences or the impact of an actual attack. Criminal investigators, patrol personnel, fire and emergency medical responders, public health personnel, bomb technicians, hazardous materials teams, emergency operations centers (EOCs), the National Guard and military personnel, the USCG, government executives, and private sector interests all have a need for information about terrorist threats. All of these entities are potential users and producers of intelligence. The TEW provides an organization, structure, and process to turn raw information into intelligence for these different, yet inter-related entities. This facilitates the development of a common understanding of a situation (known as a common operating picture) by fusing together disparate pieces of data.

The TEW has two major roles. The first is to identify potential terrorist threats that may affect the jurisdic-

"[The TEW] is based on the premise that intelligence is more than 'secret information' about an adversary."

tion, and then provide pertinent information to the appropriate agencies, decision-makers, or other TEWs and/or State, regional, and local fusion centers. This is known as indications and warning, or I&W. The TEW's second role is to determine the impact of a specific threat or attack and the likely consequences at a given point in time. This is known as operational net assessment, or ONA.

The TEW calls this process "all-source/all-phase fusion." In this approach, information is derived from "all sources" (classified, sensitive but unclassified, and open sources or OSINT) to provide intelligence during "all phases" of a threat or response, *i.e.*, before an actual attack, when an attack is imminent or after it has occurred. These are frequently described as pre-, trans-, and post-incident phases.

The TEW assumes that information germane to an event is available from any number of sources. The immediate precursor for an attack may be in the local area, in another State, in a foreign country, in cyberspace, or in a combination of these areas. Local threats influence global events, and global events in turn influence local threats. Therefore, the TEW looks at local leads and incidents within the global context, and examines global events to anticipate local terrorist threats and/or activities. This is known as assessing trends and potentials.

To achieve this kind of an understanding, and as part of the overall fusion process, the TEW relies on a process known as Intelligence Preparation for Operations (IPO). IPO fuses a number of traditional intelligence processes with unique TEW processes and capabilities, which includes evaluating trends and

Common Operating Picture

Information comes from many sources. Since a high percentage of it is not actionable, a TEW must have a mechanism to vet the information first for credibility. The LASD, for example, uses its TLO program. The LAPD provides a toll-free number for call-in tips, as does the FBI. These agencies then evaluate the information for credibility before passing it along to the TEW for further analysis.

Because the TEW links to other organizations, it has the ability to tie a piece of information from one city or area to a piece of information from another city or area, thereby forming a picture of a potential terrorist threat or the suspicion of criminal activity that may be supporting terrorist activity and therefore warrants further investigation.

potentials, determining the capabilities and intentions of an adversary, conducting pre-incident planning activities, and providing an operational net assessment. IPO also borrows from military concepts that blend the analysis of weather, enemy, and terrain with Urban IPB (Intelligence Preparation of the Battlefield) and a variety of geospatial tools. These are integrated to provide the end users with the strategic and operational intelligence they need to anticipate and understand potential and actual threats.

Decision-making in complex events generally involves a “decision cycle.” First developed by Col. John Boyd, a U.S. Air Force fighter pilot and counterinsurgency specialist, the decision cycle has four elements: *Observe, Orient, Decide, and Act,* which are collectively known as an *OODA* loop. In practice, an actor must *observe* a threat. Next, he/she must place the threat in context—that is, *orient* himself or herself to the threat. The actor then must *decide* upon a course of *action* to counter the threat and, as a final step, take action. Historically, the actor who is able to negotiate this cycle faster than an adversary tends to be the winner. Thus the TEW’s organization and process is designed to move quickly through the decision cycle, thereby forecasting the potential event horizon and crafting meaningful courses of action. The result is that the TEW is able to fuse information into actionable intelligence and bring together a range of operational entities and intelligence disciplines, and effectively and efficiently share the resulting information and intelligence with the appropriate entities.

A Networked Approach

Contemporary terrorist threats come from networks of terrorist organizations that are linked together with modern technology, and that conduct operations around the globe. Examples of terrorist networks include the international *jihadi* network characterized by al-Qaeda and its affiliates; animal and environmental rights extremists willing to use violence; and transnational criminal organizations that finance, cooperate with, and/or support terrorist group activities. Modern technology and criminal networks allow terrorist groups to cooperate across borders in mission planning, communicating their message, moving money and contraband—including weapons, chemical, biological, radiological, nuclear and explosive (CBRNE) agents, people and information—to achieve their objectives.These networked organizations exploit the organizational gaps traditionally found in government hierarchies. Networks communicate faster than hierarchies, giving terrorists and other criminals an advantage unless

“Modern technology and criminal networks allow terrorist groups to cooperate across borders in mission planning, communicating their message, moving money and contraband—including weapons, chemical, biological, radiological, nuclear and explosive (CBRNE) agents, people and information—to achieve their objectives.”

counter-terrorism responders also embrace a networked approach.

The TEW concept is such an approach. It involves the establishment of regional, multi-agency, multidisciplinary mechanisms for sharing, fusing, and assessing information and intelligence. Each individual TEW is an organization based upon collaboration among State, regional, and local law enforcement, fire service, health, and emergency management agencies and organizations. TEW groups build on the core competencies and missions of participating agencies. They bring together the players responsible for addressing terrorist threats and concerns in their area of operation, and to subsequently develop, process, and share the information needed for all phases of counterterrorist operations and with all relevant Federal, State, regional, and local entities.

Individual TEWs can range in complexity from small information-sharing forums to full-time multiagency, multidisciplinary intelligence fusion and analysis centers. Ultimately, each individual TEW must be linked to form a robust national network of information and intelligence sharing entities.

This emerging network of TEWs, fusion centers, and other information/intelligence sharing entities is a valuable starting point for developing a national network capable of sharing information and intelligence laterally (department to department,

A Scalable, Modular Framework

The scalable and modular TEW architecture takes into account a jurisdiction's unique attributes, allowing each one to devote the resources it can afford, and linking the elements of its response community into a common framework that ultimately provides interoperability and a common terminology and process to truly connect the dots and close the gaps in information processing. This kind of an organizational architecture moves away from a standing organization that needs extravagant funding or that requires a large financial outlay to respond to individual threats. A networked architecture allows jurisdictions to plug in the modules required to respond to each threat. For example, if the TEW needs a biological response, it can incorporate the public health community. If it needs a chemical response, it will incorporate the HazMat community. If it needs to provide information in response to a cyber threat, it will reach out to cyber specialists. The TEW then can relay the information from these entities or disciplines directly to decision-makers to support response and mitigation efforts.

TEW to TEW, TEW to State/regional/local fusion centers) and vertically (both top-down, from Federal agencies, and bottom-up from local agencies and TEWs to Federal and State agencies and fusion centers). Together with Federal and State partners, this network will link law enforcement, public safety, and intelligence agencies to facilitate the prevention of terrorist attacks and support the management of response and recovery efforts should an attack occur.

As the Markle Foundation Task Force on National Security in the Information Age noted:

> Participation in such networks can take many forms. Individuals act in a variety of roles, as part of changing organizations. In a national security infrastructure, local police officers, State health officials, and national intelligence analysts are all important actors in the network. Communities of practice—groups of participants in fields like public safety, transportation, agriculture, or energy—can also collectively act in a network. These communities benefit greatly from increased connections to those with similar roles in different organizations or at other levels. In addition, the collective community may come together as *ad hoc* workgroups, mobilized for specific tasks. *Ad hoc* workgroups evolve as they respond to a particular challenge.

The First Markle Report commented on the utility of the TEW concept as it was evolving in Los Angeles and elsewhere in California. Its observations mirror the LA TEW's experience with collaborative analysis.

> These participants are not distinguished by their relationship to a central gatekeeper, but by their relationship to one another. In a distributed, decentralized network, they can, will, and should form unique and utilitarian relationships in order to best support their particular role in national security, whether in prevention, analysis, response, or protection. This peer-to-peer collaboration allows Federal, State, and local participants to draw upon the collective expertise of the community.

The Markle Task Force also validated the TEW's view of the value of distributing counter-terrorist capabilities, noting:

> In an environment of such great risks, empowerment of local actors will lead to better prevention or response management. What we face today is a global, multifaceted problem, and the tools for addressing the challenge may be dispersed among

> thousands of police officers, State public health officials, firefighters, emergency room staff, or soldiers.

This is not the first national body to recognize the value of networked approaches to combat terrorism. For example, the Second Annual Report of the Gilmore Panel made the following observation:

> **Threat Analysis Needs a Cooperative Vehicle**
> As has been noted elsewhere, threat analysis is critical in the determination of appropriate response. Because of the complexity of terrorism threats in general, and the CBRNE threat in particular, threat analysis is most effectively conducted by multiple agencies, each of which brings its own special skills and strengths to the table. In Los Angeles County, the TEW has filled the previously wanting role of a medium for information transfer, joint analysis and incident net assessment and thus has proven to be an exceptionally useful mechanism.

These reports support what is already known about terrorist threats: There is a need to identify potential threats and to assess imminent and/or occurring situations and their potential outcomes if public safety agencies are going to be successful in their prevention, protection against, response to, and recovery from terrorist threats and/or attacks. It is also clear that:

- The traditional process of intelligence collection, fusion analysis, and dissemination must be more effectively organized and efficiently shared to combat networked transnational threats.
- The elimination of bureaucratic competition and organizational barriers will further enhance and support national preparedness and intelligence sharing.
- The distinction between "global" and "local" is increasingly anachronistic.

The TEW responds to this by recognizing that State, regional, and local agencies are producers as well as users of intelligence, and that:

- Intelligence for homeland security must be shared between multiple disciplines and across all levels of government.
- Intelligence must move vertically (top-down and bottom-up) and laterally. There is a need for bilateral cooperation and information sharing among law enforcement, public safety, and emergency management and response agencies that is independent of, but coordinated with, Federal agencies.

- Local law enforcement, fire, and health agencies may be the first to observe indicators of terrorist activity.
- Local agencies have the responsibility to protect the public and craft a response to a threat or incident. It should be recognized that the State and local homeland security community (law enforcement, public safety, health, fire, emergency management, and other first responders) are the "first line of defense" in preventing and protecting against, and the first "boots on the ground" in responding to and recovering from terrorist threats and/or attacks and other incidents of national significance. This community also plays a vital role in the collection and sharing of information and intelligence within its own State and local levels, as well as serving as a mechanism to share information with the Federal government and other national intelligence community entities.

Therefore, while the TEW may be used as a tool and an organizational concept to implement intelligence fusion processes at the State and local level, it also serves as a mechanism to merge State and local information sharing and intelligence fusion activities with those of DHS and the greater national intelligence community. Thus, the TEW further enables State and local homeland security communities, as both collectors and consumers of available information and resulting intelligence.

TEWs and State Fusion Center Coordination Local, Urban Area, and/or regional TEWs should coordinate and communicate with respective State or regional fusion centers, as well as other relevant Federal entities, to ensure the timely and accurate exchange of information and intelligence. This includes collaborative activities such as:

- Regular meetings and trainings
- Mutual connectivity of information sharing systems and databases
- Exchange/detail of personnel
- Exchange of intelligence products developed (bulletins, advisories, etc)
- Continuous coordination and deconfliction of relevant tips, leads, and any resulting cases, investigations, and/or activities

Chapter Two: TEW Organization

As an intelligence fusion and analysis organization, the TEW brings together subject matter experts from disciplines that have a role in deterring, preventing and responding to terrorist threats or attacks; it also can support response to other incidents of national significance. The TEW staff includes specialty or generalist analysts from law enforcement, the fire service, and health disciplines. They work as a team to develop a comprehensive understanding of current and potential situations and the impact on the Operational Area. Within the TEW, these analysts are divided into six mutually supportive cells.

The *Officer-in-Charge (OIC) (or Unified Command)* cell is a team that provides direction, sets intelligence requirements, and is responsible for interacting with prevention, protection, and response organizations. It approves the dissemination of intelligence products and interacts with command staff at participating agencies and with the Unified Command Structure (UCS) at a terrorist, or terrorist-related incident, or other incident of national significance.

The *Analysis/Synthesis* cell coordinates net assessment activities—determining the impact and consequences of a specific threat or attack. This cell also tasks the various TEW cells with requests for information and develops their results into actionable intelligence products in the form of advisories, alerts, or warnings. This cell is also responsible for the intake of leads and reports.

The *Consequence Management* cell assesses the law, fire and health consequences of an event and provides intelligence support and technical assistance to centers or other entities that coordinate response activities.

The *Investigative Liaison* cell coordinates with criminal investigative entities and the traditional intelligence community.

The *Epidemiological Intelligence* cell is responsible for obtaining real-time disease surveillance from public health, agricultural, and food surety agencies.

The *Forensic Intelligence Support* cell is responsible for technical sup-

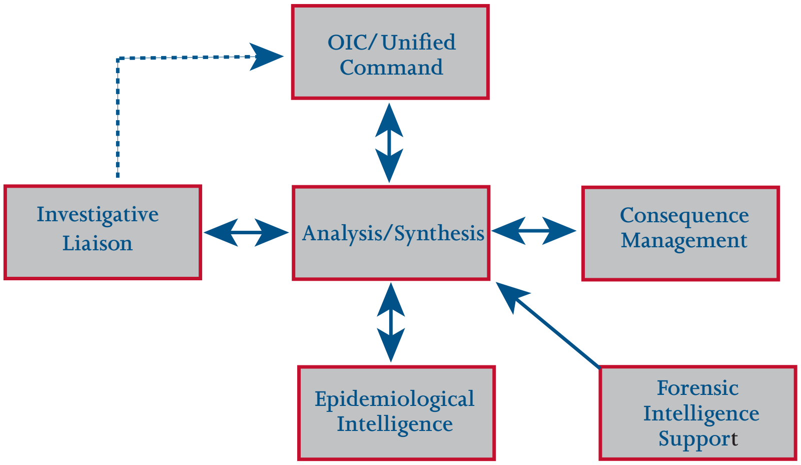
> "[TEW staff members] work as a team to develop a comprehensive understanding of current and potential situations and the impact on the Operational Area."

port, including field assessment and reconnaissance at CBRNE events, and geospatial intelligence activities.

Merging Intelligence Disciplines: All-Source/All-Phase Fusion

"All-source/all-phase fusion" is the process of bringing together information from all sources to develop a complete understanding of all phases of a situation. This includes public information, such as news reports and technical manuals (known as open source intelligence or OSINT), sensitive but unclassified information, such as investigative information, and classified national security information. This is developed by many agencies and by many separate intelligence disciplines. For example, criminal intelligence is derived from criminal investigations and analysis. Operational intelligence informs response activities and includes health intelligence, epidemiological intelligence, and traditional situation and resource status information. Counterintelligence assesses an adversary's intent and capability. Geospatial intelligence describes terrain by exploiting geographic information systems, imagery and mapping products. None of these disciplines can serve all of the intelligence needs for ad-

Figure 1: TEW Organization



dressing terrorist threats. However, together they can effectively support operations. The TEW is a structure for achieving this fusion.

TEW Mission and Concept of Operations

The TEW is designed to develop intelligence that can be used to support local, regional, and national interdisciplinary terrorism prevention and response activities. To accomplish this, the TEW has two major missions: Indications and Warning (I&W) and Operational Net Assessment (ONA).

- *Indications and Warning* includes all the information gathering, intelligence processing fusion, and analysis activities directed toward identifying a terrorist threat and informing those with a need to know. Indicators come from multiple sources and must be correlated and assessed before they are considered actionable intelligence.
- *Operational Net Assessment* is the process of synthesizing all known threat information to determine the impact and consequences of a terrorist act. This includes fusing information gleaned from monitoring local and global trends and potential terrorist activities with what is known about the capabilities and intentions of the adversary.

Within these broad phases, the TEW conducts many separate and related activities.

- *Consequence Consultancies* are individual threat assessments conducted to support field responders. A common example

Operational Intelligence vs. Criminal Intelligence

Operational intelligence is the result of analysis and synthesis of information needed to negotiate the operational environment. It is informed by—and informs—strategic intelligence. Operational intelligence (OPINT) is the actionable, vetted, and validated information that is disseminated to decision-makers, commanders, investigators, and responders. It includes information about the adversary (or opposing force/OPFOR), its composition or network architecture, its capabilities and intentions, as well as the tactics, techniques, and procedures (TTPs) the adversary might employ. Operational intelligence is not criminal intelligence (CRIMINT), which is used for criminal prosecution. Instead, it complements criminal intelligence by providing investigators with the context they need to conduct operations. It also informs operators of the dynamics involved in the criminal investigation along with all other pertinent factors that will influence operations at given points in time.

is the assessment of suspicious powders or "white powder" events, where a field responder or incident commander calls the TEW for technical assistance.

- *Threat Estimates/Assessments* are an analysis of the threat potential for a future event, such as a special event, dignitary visit, or parade. Before a threat is discerned, these are referred to as "estimates." Once a potential threat is identified, they are known as "assessments." Both are predictive tools to guide response and deployment decisions.

Interaction with Other Organizations, Agencies and Disciplines

The TEW is an intelligence fusion and information analysis center with a focus on terrorism. However, to develop a comprehensive threat picture, the TEW must obtain information from (and share information with) a wide range of criminal intelligence entities. These include gang investigators, narcotics investigators, fraud investigators, financial/white collar crime investigators, the FBI's Field Intelligence Groups (FIGs) and a variety of intelligence fusion centers focusing on traditional crimes. The TEW must maintain collaborative relationships with these entities and with State and regional intelligence fusion centers, Federal agencies (including the intelligence community), and with the sector specific Information Sharing and Analysis Centers (ISACs) that have been developed to protect critical infrastructure by facilitating the sharing of information within the private sector.

Investigative Liaison

The TEW does not investigate leads, gather evidence or build cases for prosecution. Although the Investigative Liaison cell is part of the initial vetting/validation process, its members act solely as liaisons to other investigative entities. They pass along leads for investigation and maintain contact with other agencies and disciplines to monitor investigations.

Interaction with Joint Terrorism Task Forces (JTTFs): JTTFs are sponsored by the FBI and have on–staff investigators from local, State and other Federal agencies. They are investigative in nature, pursuing criminal and intelligence investigations related to terrorism. The TEW receives raw reports and potential leads from local law enforcement, fire service, and health agencies, and conducts initial analysis of these leads. It then provides vetted leads to the JTTFs for investigation.

The TEW also assesses potential response needs for specific threat situations. The JTTF and TEW are mutually supportive entities. Additionally, the TEW should interact, communicate and coordinate efforts with any FBI-sponsored entities within the region, such as FIGs and/or Regional Intelligence Centers (RICs), as appropriate.

Interaction with Investigative Entities: The TEW is an intelligence support entity. It assesses and validates raw leads and then passes workable leads to the appropriate investigative entity (such as a JTTF, FIG, RIC, or specialty crime squad). The TEW does not conduct investigations but does provide support to investigative entities. The Investigative Liaison cell is responsible for ensuring the flow of information between the TEW and these investigative entities. It works with investigators to ensure cases, sources, and means are protected, while pertinent threat information is shared in order to develop a comprehensive threat picture or to prepare for response.

Interaction with other TEWs: Since terrorists operate globally to plan and conduct attacks and to gain support for their activities, developing a threat picture requires fusing information from many disparate locations and across jurisdictions and disciplines. Linking individual TEWs and fusion centers at the local, regional, and State level into a national network provides a mechanism for sharing this information and conducting distributed, collaborative fusion and analysis of specific terrorist threats. By embracing complementary organizational structures, terminology, processes, and protocols, TEWs and fusion centers can assist each other during surge periods with course of action development and other analytical tasks. This unity of effort also allows individual TEWs and fusion centers to leverage the experience and capabilities of the entire national network. For example, a TEW in a port city may become expert in port security issues, while a TEW in an agricultural city may become expert in agro-terrorism threats. This knowledge can be shared among the trusted network.

TEW Cells

As previously described, the TEW has two major functions: Indications and Warning (I&W) and Operational Net Assessment (ONA). To fulfill these complex mission areas, the organization is divided into six interactive, multi-agency and interdisciplinary cells that are designed to operate as a network.

Officer-in-Charge (Unified Command Cell): Provides command, direction, and supervision, sets intelligence requirements and interacts with Unified Command Structures (UCS). It is responsible for approving the dissemination of information and TEW intelligence products and ensuring multi-agency coordination with Federal, State, and local agencies.

Analysis/Synthesis Cell (A/S): The A/S Cell is the central integrating hub of the TEW organization. This cell tasks out requests for information to other cells, then collects and integrates their individual products into a cohesive assessment. This process includes capturing investigative information, gathering intelligence from all sources, and analyzing and synthesizing it. The A/S cell also synchronizes information from the Investigative Liaison, Consequence Management, Epidemiological Intelligence, and the Forensic Intelligence Support/ Field Assessment Support Team into a useable product for decision-makers. Products issued by the A/S cell include advisories, alerts, warnings, issue-specific white papers, and mission folders. Mission folders integrate threat-specific playbooks, venue-specific Response Information Folders, intelligence information, archival information on technical dimensions of threat agents, and resource status to support pre-planning activities and develop potential courses of action for incident mitigation and response.

Investigative Liaison Cell (INV-LNO): This cell is responsible for processing, tracking, and collecting

Tips and Leads

Tips and leads are initially logged in by the Analysis/Synthesis (A/S) cell, which vets them first for credibility. The lead may then be sent to one of the TEW cells for further analysis. For example, if a tip comes in about hazardous chemicals stolen from a local manufacturer, the A/S cell would call on the Consequence Management cell, which is staffed primarily with firefighters and hazardous materials specialists. These subject matter experts could provide information about the chemical and the potential effects if it were used in a terrorist attack. The same is true with the Epidemiological Intelligence cell. The A/S cell would turn to this cell, staffed primarily by members of the public health community, for information about threats to the water supply or to area crops.

Tips that need further investigation are passed on to area teams that can follow the lead until it either stalls out, turns into a criminal case, or until investigators identify a “nexus,” or connection, to terrorist activity. Once the nexus is established, the lead is passed on to the FBI, which is the primary lead investigator of terrorist cases.

criminal and national security intelligence and leads related to terrorist threats or activities. It is the primary point of contact with all classified information, national and State databases, and with investigative and intelligence efforts at all levels of government. The INV-LNO is the Operational Area/county link with the FBI and other intelligence and investigative entities, as well as the link to the national network of Joint Terrorism Task Forces, especially the Los Angeles JTTF for the LA TEW. The INV-LNO cell is responsible for vetting and validating leads and assessing specific threats. It is also responsible for working with other specialized investigative entities to develop a complete intelligence picture.

Consequence Management Cell (CM): This cell is staffed by members of the fire service, law enforcement, hazardous materials, and medical professionals in order to assess, in the event of a threat or attack, the current and future resource status and to marshal specialized resources when necessary. Its members act as a technical reference and conduct pre-planning activities to develop potential courses of action for response to incidents involving CBRNE and large-scale explosives. It develops tactics and estimates logistical requirements for initiating and sustaining a comprehensive response to a terrorist attack. This cell also has the primary responsibility for developing playbooks and Response Information Folders.

Response Information Folders

One of the jobs typically assigned to the Consequence Management cell is the development of Response Information Folders. These are specific to a location or venue and provide detailed information about the potential impact and response to a terrorist incident. Developing RIFs is generally a team effort, with each discipline—law enforcement, fire, health, public works—looking at the location from their unique perspective. For example, law enforcement might look at an entertainment venue with an eye toward crowd control, setting up a perimeter or choosing evacuation routes; public health may want to identify the quickest way to the nearest hospital; fire might look at managing HazMat and EMS response. The overall goal is to create a comprehensive picture of a location or venue that will ensure an efficient and appropriate response.

Epidemiological Intelligence Cell (Epi-Intel): This cell integrates disease surveillance for all threats (especially biological terrorism). It facilitates the integration of public health, agricultural, food surety, and law enforcement investigations and provides planning estimates on the distribution of casualties and potential decontamination, quarantine, and treatment issues. This cell ensures the accurate and complete flow of information during intentional or suspicious outbreaks and conducts continual monitoring for early recognition and warning of biological threats. This cell is also responsible for food and water surety and agricultural issues (including liaison to the public health community, water districts, U.S. Department of Agriculture (USDA), the Food and Drug Administration (FDA), the U.S. Department of Health and Human Services (DHHS), the Centers for Disease Control (CDC), etc.).

"When al-Qaeda attacked the United States on September 11, 2001, the LA TEW activated the Net Assessment Group to assess the potential impact on the region."

Forensic Intelligence Support (FIS) Cell and Field Assessment Support Team (FAST): This cell is responsible for technical support, including field assessment and reconnaissance activities for CBRNE events. It supports a multi-agency response with specialized detection and sampling equipment and provides technical assistance and specialist advice that enables law enforcement support to the fire services in the event of mass casualty/mass decontamination operations. This cell is responsible for geospatial intelligence (GEOINT), cyberterrorism issues, and "virtual reachback" to specialists at the national laboratories, military, and universities. It uses this information to assess a situation and to help develop tactical courses of action. FIS/FAST uses various technologies for modeling and simulation of the potential consequences of a terrorist event. The FAST is the field component of the FIS cell. It sends information from the field to the TEW for analysis.

Net Assessment Group

During the early years of the TEW's development, its operational model was put into use on an incident-driven basis. What began as an *ad hoc* organization that was brought together to manage the anthrax hoaxes of 1998 was formally assembled for the *Westwind '99* exercise (a FBI-sponsored terrorism exercise with Federal, State, local/civil/military participants), and then again for the Y2K transition and contingency operations for the 2002 Democratic National Convention. The group—by then formally named the Net Assessment Group—was expanded to form the organizational structure of an operational TEW. This structure was developed by analyzing the roles and core competencies of the agencies that would have a part in providing intelligence and decision support in an actual terrorist event. The participants were then organized according to information-processing roles, as opposed to organizational or bureaucratic designation. The result was the current TEW structure minus the Forensic Intelligence Support cell, which was added later.

When al-Qaeda attacked the United States on September 11, 2001, the LA TEW activated the Net Assessment Group to assess the potential impact on the region. Upon activation, the group transitioned into a full-time operational entity based on this organizational structure.

During an actual event, a TEW either activates a Net Assessment Group or uses its standing structure to determine the scope and impact of the event. This is known as a net assessment. The Net Assessment mission follows:

"As directed, the TEW will provide the Unified Command Structure with the impact of an actual attack on the Operational Area, gauge resource needs and shortfalls, continuously monitor and assess situational awareness/status, and act as the point of contact for interagency liaison in order to develop options for courses of actions for incident resolution."

Supporting Committees

A TEW can rely on leadership and guidance from committees comprised of personnel from

TEW Products

Advisories are issued to provide information on potential global or national threats that are non-specific, low credibility, and/or uncorroborated. They are also used to inform recipients about tactics, techniques, and procedures that may be used by terrorists (i.e., modus operandi information). Advisories are designed to raise awareness and support training objectives. They can be issued during all five national Homeland Security Advisory System (HSAS) levels.

Alerts are issued when there is a specific, verified, validated and increased threat to the United States. This includes potential attacks against U.S. interests abroad or within the United States, particularly in California or adjacent states, even though a specific target within the Los Angeles County Operational Area has not been specified. Alerts are generally issued during Elevated (Yellow) or High (Orange) HSAS levels.

*Warning*s are issued when there is a credible, verified, and validated, threat to persons or venues (specific sites, events, or critical infrastructure) within the Los Angeles County Operational Area or an adjacent jurisdiction if Operational Area resources are expected to be involved in a mutual aid response. Warnings will always be accompanied by specific response planning steps and recommended course of action options. Warnings will be issued during High (Orange) or Severe (Red) HSAS level.

participating agencies. These committees can be used during the early phases of implementation in the absence of a full-time standing TEW or to support a full-time TEW by expanding its reach into the response community. As previously stated, the Net Assessment Group comprises the core of an operational TEW. It can be stood up on an *ad hoc* basis or, when sufficient resources exist, operate as a permanent structure. Other committees that have been utilized in Los Angeles and elsewhere include a Playbook Committee, an Emerging Threats Committee and an Intelligence Preparation for Operations Working Group. Other committees have been established on an as-needed basis to support short-term or specialty needs that arise while building the overall capabilities of a TEW.

Playbook Committee: Before evolving into a full-time activity, the LA TEW utilized a committee of part-time law enforcement, fire service, and health personnel to develop Response Information Folders specific to critical infrastructure and public venues. This committee also developed playbooks, or standardized formats, for assessing threats and their impact based upon classes of threat (*i.e.*, chemical, biological, etc.). This function is now primarily conducted by full-time personnel, but part-time personnel are still utilized. This can be a supporting committee to a full-time TEW or a major activity for those that operate on an *ad hoc*, incident-driven basis.

Emerging Threat Committee: The LA TEW established an Emerging Threat Committee to assess potential threats. This committee was initially named the "directed energy weapons" committee because it was assembled specifically to assess a series of laser strikes against aircraft on approach to area airports. Experience dictated that it be renamed to address a wider range of longer-term issues, including new weapons and evolving terrorist organizational structures or tactics—such as suicide bombing—in the 3- to 5-year window. The committee is comprised of full-time TEW staff and subject matter experts.

Intelligence Preparations for Operations (IPO) Working Group: This group was developed to further refine the TEW's IPO process and tools. It is comprised of full-time and adjunct members of the LA TEW from a variety of disciplines: law enforcement, fire, emergency medical services, HazMat, public health, several military services and combat arms, social scientists, and intelligence practitioners from Federal, State, local, and private organizations.

Others: Topical or threat-specific committees or working groups can be established when needed and then stood down when they are no longer required. Examples include training or exercise development committees, task groups for special events, or committees devoted to specific equipment needs.

Terrorism Liaison Officers and Infrastructure Liaison Officers

Terrorism Liaison Officers (TLOs) are designated public sector (law enforcement, fire, health) officials at individual departments or within larger departments at a geographic subdivision (patrol station, precinct, battalion) or at specialty units (bomb squads, HazMat teams, detective squads, gang or narcotic units). These TLOs ensure the two-way flow of information between field personnel and the TEW. They receive training in terrorism basics, terrorist tactics, techniques, and procedures, and in TEW reporting procedures. This allows the TEW to task specific requests for information to field personnel. Additionally, TLOs can be trained to provide surge staffing to the TEW during high activity periods. The Investigative Liaison cell coordinates law enforcement TLOs, the Consequence Management cell coordinates fire and EMS TLOs, while the Epi-Intel cell coordinates public health TLOs. TLOs conduct regular (monthly or bi-monthly) meetings within their own disciplines and participate in periodic (or threat specific) all-discipline TLO meetings and/or training sessions.

The law enforcement, fire, and health TLOs from specific jurisdictions also coordinate joint planning

The TLO Program

The LA TEW TLO program is a robust project that has TEW representatives in more than 200 law enforcement and fire agencies, as well as other organizations and private sector entities. The TLO is often the door through which information flows to the TEW. For example, an officer at an LASD substation may get a tip that a suspicious person is taking pictures of buildings in areas where critical infrastructure is located. The officer may investigate the tip or pass it along to the substation’s TLO. The TLO then gives the tip its first “scrub” by investigating whether it is credible enough to pass along to the TEW for further analysis.

Law enforcement, fire, and health agencies each have their own TLO programs, as do the private sector partners. TLOs meet monthly for training and to exchange information.

and awareness activities and coordinate with private sector representatives in their jurisdictions. Private sector and industry representatives involved in this process are known as Infrastructure Liaison Officers (ILOs). ILOs are usually security or operations managers from specific sectors of critical infrastructure, cultural facilities, or representative associations/organizations. ILOs can serve as subject matter experts for specific or technical TEW analyses to ensure a two-way flow of threat information with the private sector. ILOs meet in a forum known as the Private Sector Terrorism Response Group (PSTRG), as well as regularly with their TLO counterparts.

Chapter Three: Getting Started

Providing staff for a TEW requires a high degree of interagency cooperation. TEW staff comprise a joint, interagency decision-support and intelligence-support capability to all agencies in a region. Staff is provided by participating agencies, with each person assigned to a specific cell to form a task-oriented, multi-agency, interdisciplinary team. Within the TEW framework, all personnel work without regard to their home agency rank or discipline. Leadership functions are designed to facilitate the analytical process and provide mission support. All personnel remain subject to their contributing agency chain of command and agency policies and procedures.

Permanent Cadre

A permanent TEW operates with full-time staff: an Officer-in-Charge, team leaders for each cell, and analysts within each cell. Permanent staff members monitor the threat situation, conduct ongoing analysis, and manage the TLO program. They also process leads, conduct threat estimates and assessments, develop reports, conduct pre-planning (by developing playbooks and Response Information Folders), and provide training to field personnel. Staffing levels are determined by budgetary factors, workload, and threat situation (collectively known as operational tempo), and staff availability. Permanent staff members monitor a "duty desk" during business hours and a duty pager during off-hours, if the TEW does not have 24/7 capabilities.

Surge Staffing

During high activity periods (threat periods or responses), the permanent cadre is augmented by surge staff. Surge staff is drawn from the TLO cadre and from TEW adjunct personnel. Surge staffing can also come from other TEWs or fusion centers in a mutual aid framework. In Los Angeles County, for example, TLOs from area law enforcement and fire agencies have been detailed for two-week tours to the LA TEW during high threat and response periods or for participation in exercises. LA TEW personnel have also worked in neighboring Riverside, San Bernardino, and Orange counties.

“Having trusted and vetted subject matter experts in the science, medical, legal, intelligence, and policy disciplines helps the TEW avoid tunnel vision and achieve a higher quality of assessment.”

Adjuncts and Subject Matter Experts (SMEs)

Adjunct members of the TEW are drawn from academic, scientific, medical, and policy institutions to enhance the TEW’s analytic and assessment capabilities. A broad base of technical expertise is often required to determine the technical capabilities of terrorist groups, the impact of attacks involving weapons of mass destruction, cascading affects of attacks against infrastructure, and emerging threat potentials. Having trusted and vetted subject matter experts in the science, medical, legal, intelligence, and policy disciplines helps the TEW avoid tunnel vision and achieve a higher quality of assessment. Adjuncts and SMEs participate in monthly TEW meetings, exercises, and assessments, both in person and through virtual reachback capabilities.

Agency Participation

It is recommended that representatives from all key law enforcement, public safety, public health, fire, and emergency management agencies in the region participate in the TEW process. This includes representatives from Federal, State, and local agencies, as well as any area military installations. Agencies are encouraged to provide staff resources when they can. Such contributions can be full-time, part-time (several days a week or as part of a duty rotation), or as part of surge staffing during a critical period.

Liaison Officers (LNOs)

During an actual event or incident response it may be desirable to send a TEW liaison officer (LNO) to a field command post, EOC, or to other TEWs or intelligence fusion centers. In Los Angeles, for example, the TEW provides intelligence support to the County Emergency Operations Center (CEOC). During an incident, a designated senior TEW representative is provided to the CEOC management staff to facilitate the flow of sensitive, time-critical information and to provide technical assistance. Similarly, a TEW representative can be provided for the same purpose to the incident commander during major field responses. LNOs can also be deployed to support investigative efforts, although this is generally a function of the Investigative Liaison cell. In addition, the Forensic Intelligence Support cell has the specific responsibility of acting as liaison with the HazMat group and/or Weapons of Mass Destruction Civil Support Team during a field response involving a CBRNE agent.

Tactical Liaison Teams

During a large-scale complex field response or in order to support special events, representatives of each TEW cell can be configured into a tactical liaison team to provide support to a field command post and facilitate reachback to the TEW itself. These teams can be tailored for the specific incident type and with regard to its unique intelligence needs. A tactical liaison team can also provide surge capacity to another TEW during a critical event.

Implementing a TEW

Implementing a TEW is a flexible, scalable process. Each jurisdiction needs to assess its local capabilities; existing local, regional, and State (if applicable) information sharing and intelligence fusion and analysis capabilities; governance structures; organizational and jurisdictional issues, and available resources to develop a blueprint for implementation. In Los Angeles, the TEW started as an integrating structure with monthly meetings held by a TEW Secretariat. The LA TEW then added a committee structure to develop a concept of operations. Once this was established, the LA TEW then moved to activating its Net Assessment Group for special events and exercises. When the 9/11 attacks occurred, the LA TEW stood up its Net Assessment Group, which then transitioned into a full-time structure.

Organizational Issues: Key organizational issues include establishing leadership (which agency will coordinate development, lead the process, and serve as the secretariat), and determining the necessary organizational players and decision-makers (law enforcement, fire service, health agencies, political leaders, State, and/or Urban Area representatives) needed to approve the concept, support its development and implementation, and allocate resources.

Development of partnerships is the next essential step. Interagency buy-in is essential and will go a long way toward creating relationships and fostering coordination, as well as facilitating development of the scope of the TEW's area of operations. For example, will the TEW include one city or county? Will it encompass a group of cities and counties? Will it include statewide participation? Will it include Federal participation? In addition to law enforcement, fire, and health agencies, it is also a good idea to include and/or liaison with the local district attorney's office, city prosecutors, city or county counsel, local corrections personnel, and the U.S. Attorney's office (both prosecutors and intelligence liaisons).

Developing a Concept of Operations: Next, the TEW must develop a concept of operations. This should include how the TEW will be started, how it will expand and how it will operate within the region and with other TEWs.

Getting Started: Bringing together the stakeholders and potential participants and forging a mutual agreement that a TEW is needed is the first step. These participants usually include local law enforcement, fire, emergency medical, public health, and emergency management agencies, together with the local FBI field office, State agencies (law enforcement, emergency management, etc.), and any applicable Urban Area Working Group (UAWG) representatives. Federal representation, such as National Guard; USCG; ICE; Customs and Border Protection (CBP); the U.S. Secret Service (USSS); U.S. Marshal Service (USMS); Federal Transportation Administration (FTA); TSA; the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA); and other U.S. Department of Defense (DOD) entities (as applicable); and specialized law enforcement agencies (transit, airport and port police, corrections/prison guards, campus/educational institution resource/security officers and similar agencies), as well as public works or utility agencies, may also be typical participants.

These agencies then designate a planning team and agree upon one agency to serve as the TEW Secretariat. A TEW must be accepted either through interagency agreement (such as a memorandum of agreement), by acknowledgement in operational plans or procedures (administrative recognition), or through codification by a municipal, county, or city ordinance. The TEW should then adopt a logo to ensure recognition within its internal market and broader TEW community. It may now conduct informational briefings for participating agencies and begin developing and disseminating the appropriate products to serve its stakeholders' information and intelligence needs.

Additionally, a TEW should ensure proper connectivity to the appropriate State and local public safety information sharing systems and databases, as well as regional or national homeland security and law enforcement information sharing systems and networks. These include, but are not limited to, the Homeland Security Information Network (HSIN) for direct connectivity to the Homeland Security Operations Center (HSOC), Law Enforcement Online (LEO), the Criminal Information Sharing Alliance Network (CISAnet), the National Law Enforcement Telecommunications System (NLETS), and the Regional Information Sharing Systems Network (RISSNet), as well as appropriate Federal information centers and clearinghouses, such as the National Crime Information Center (NCIC) and the Terrorist Screening Center (TSC).

Funding: Funding is needed to sustain full-time operation. It is needed to obtain work space, procure equipment and information systems, conduct training, and hire permanent or part-time personnel. Agencies can contribute in-kind personnel or resources, seek dedicated funding in their jurisdictional budgets, or seek grant funding from a variety of grant programs. By operating as a multi-agency task force, the TEW shares the burden of these costs and leverages funding and capability development among participating agencies.

Scalable Implementation (Types I-IV evolution)

Developing a TEW is a "work in progress." Few jurisdictions have the funds necessary to stand up a full-scale TEW in one step. Just as the Los Angeles TEW evolved and expanded over time, other TEWs also follow a developmental curve. Four major phases of evolution have been observed.

- *Type I*: An Integrating Concept. Conducts monthly meetings and topical workshops. Establishes committees to coordinate information sharing and development of TEW products.
- *Type II*: Activation for Threats and Special Events. Activates a Net Assessment Group during specific threat periods or special events. Continues work from Type I phase, trains personnel, and develops doctrine/operational policies.
- *Type III*: Standing Full-Time TEW. Serves as a regional all-source/all-phase fusion center with law enforcement, fire, and health participation. Continues work of prior phases. A variation of this phase is Type III+ where the TEW becomes technology enabled.
- *Type IV*: Networked TEW. This is the end-state of the expansion effort. In this phase, a TEW is linked together with other TEWs and fusion centers to perform networked, distributed, and collaborative intelligence fusion, with each one becoming a user and producer of intelligence within the national network.

Monthly Plenary Meetings

As previously mentioned, the TEW started with a monthly meeting. Stakeholder agencies were brought together to share threat information and knowledge of terrorist trends and potentials with an aim toward enhancing prevention, protection, and response capabilities. As the LA TEW matured, it retained this forum as a way to integrate participating agencies and to conduct outreach beyond the full-time staff. Monthly plenary meetings consist of one to three targeted briefings on various terrorism issues—groups, trends, recent attacks, intelligence and counter-terrorism tradecraft, technological, social, and cultural issues—along with a roundtable discussion among all participants about recent threat information and areas of concern. These meetings are held at a set time and usually last about two hours.

Supporting Efforts

As mentioned elsewhere, a TEW can establish a range of committees to further its work. These committees can be permanent or of limited duration; they can be generalized or topic-specific. This allows the TEW to leverage area resources to achieve specific tasks and build capabilities for both the TEW and its participating agencies. A Playbook Committee or Emerging Threat Committee would be an example.

In addition to committee work, monthly meetings and planning efforts, a TEW may conduct topical workshops to build knowledge and expertise. For example, the LA TEW has conducted one-day workshops on suicide bombing and cyberterrorism. This format allows TEW staff and members to obtain in-depth familiarization from recognized subject matter experts on a range of emerging threat issues. The LA TEW typically teams with a co-sponsor(s) with expertise in the area to conduct these topical workshops.

Staffing the TEW Cells

TEW cells can be staffed with full and/or part-time personnel. This section describes the characteristics and specialty skills needed for these positions. All cells require primary assignments, with back-up personnel to cover vacations, training, days off, and/or activation over 24 hours or for extended or multiple shift operations.

- *Officer-in-Charge/Unified Command*: This requires a manager, director, or management team. This position is usually filled by a law enforcement officer with the rank of sergeant or lieutenant. Personnel assigned to this cell or position require an in-depth understanding of terrorist threat issues, intelligence processes, legal investigations, emergency response procedures, local agency dynamics, and the TEW process. A deputy officer-in-charge can be added to this cell to assist with administrative and logistical duties.
- *Analysis/Synthesis*: This cell requires analysts, typically law enforcement and/or counterterrorism intelligence analysts, but can also include fire or emergency management analysts for tasks not related to processing criminal history information. The team leader of this cell needs the same range of skills as the OIC

cell and must be familiar with the capabilities and requirements of the other TEW cells in order to task them and assemble their contributions into finished products. Personnel assigned here require an understanding of lead intake, the use of automated data systems, intelligence analysis and processes, course of action development, and excellent writing and computer skills.

- *Consequence Management*: This cell requires experienced fire, emergency management, medical, and law enforcement tacticians and planners. Typically, the team leader is a battalion-level chief with HazMat and/or arson investigation experience. Other cell members require analytical skills, familiarity with emergency planning and with the local emergency response and recovery infrastructure and capabilities.

- *Forensic Intelligence Support*: Skills required within this team include knowledge of geospatial intelligence, including the use of geographic information systems (GIS), mapping products, overhead imagery, information technology, sensors, and detectors. Familiarity with cyberterrorism and CBRNE threat agents is also required. Personnel assigned to the Field Assessment Support Team require hazardous materials training to at least the HazMat technician level, with specialist training preferred. These personnel also need to be familiar with evidence collection and processing.

- *Epidemiological Intelligence*: Epi-intel cell members must have an in-depth understanding of disease surveillance and reporting systems, disease mechanisms, the local and national public health infrastructure, as well as statistical and epidemiological investigation skills. This includes the use of epi-data systems.

- *Investigative Liaison*: Officers assigned to this cell require an understanding of criminal investigation and criminal intelligence, knowledge of local law enforcement organizational structures, knowledge of Federal law enforcement investigative processes and jurisdictions, detailed knowledge of the TEW process, and detailed knowledge of terrorist tactics, techniques, and procedures, including how terrorist groups finance their activities. Training should include counterintelligence and investigative tasking. The team leader should be a senior investigator or sergeant.

All TEW staff should receive familiarization and/or cross-training with the duties of other TEW cells to the highest degree possible. They should be familiar with the legal requirements related to information collection and intelligence analysis, crisis action planning, and general terrorist trends and threats. In addition, all permanent and recurring surge staff should have clearances to handle classified information. Clearances at the Secret, Top Secret, or higher levels are desirable for all TEW analysts in the Analysis/Synthesis, Consequence Management, Epi-Intel, Investigative Liaison, and Forensic Intelligence Support cells. Team leaders would benefit from Top Secret or higher clearance. Specific allocation of clearances needs to be determined by each TEW based on specific State and local needs and in consultation with the local FBI Field Office/JTTF and/or DHS.

Chapter Four: The TEW Process

Intelligence Preparation for Operations

Intelligence Preparation for Operations (IPO) is a way of conducting current and future preparation for terrorist threats and/or attacks. It provides a standard tool set that enables the recognition of current or future threats and supports course of action development. The process bridges the gap between deliberate planning and crisis action planning for multi-organizational and multi-disciplinary prevention and response activities.

IPO synthesizes several approaches to developing operational intelligence. As a starting point, it combines the traditional military concept of weather, enemy, and terrain (WET) and the emerging concept of Urban Intelligence Preparation of the Battlefield (U-IPB), with the TEW process.

The cornerstone of this IPO tool set is the TEW process, which was developed over eight years of practice. It involves assessing trends and potentials on an ongoing basis (known as scanning), adding an assessment of the adversary's capabilities, especially during a known threat period (known as monitoring), and then developing a net assessment for decision-makers (forecasting). To accomplish these activities the TEW utilizes a number of IPO tools, including Response Information Folders, Playbooks, and Mission Folders.

Note:

The IPO Process

It is important to note that the graphic in Appendix I is a complex visualization of the IPO process in its entirety, the details of which will be fully discussed in a subsequent TEW publication. For the purpose of this volume, we explain the basic steps of the IPO process to introduce the reader to the concept without defining the many terms and acronyms shown on the graphic. It is important to remember, however, that these concepts, terms, and acronyms are the accepted lexicon of the intelligence community and the military, from which much of the TEW fusion process has been adapted. TEW staff should familiarize themselves with these terms to ensure effective communication and consistency among the relevant disciplines, organizations and entities.

IPO has a core and four steps:

- Step 1: Define the Operational Space
- Step 2: Describe the Operational Space Effects
- Step 3: Evaluate the Opposing Force/Potential Threat Elements and Threats
- Step 4: Determine Opposing Force and Friendly Courses of Action

The core of the IPO process is analysis/synthesis, or the process of breaking down information into its constituent parts, processing it into manageable components, providing context and synthesizing the results into actionable intelligence. This includes the entire intelligence cycle of direction, collection, processing, production, and dissemination. These steps are represented by "collection management" (*i.e.*, getting the information) and "situational understanding" (*i.e.*, interpreting the information). This core drives IPO's

Urban Intelligence Preparation for the Battlefield
Intelligence Preparation of the Battlefield (IPB) is an analytic process used to organize and analyze information on terrain, weather, and the threat within a unit's area of operations and interest. It uses a systematic approach to predict how an adversary will act within a certain area of operations given the terrain, weather, and other contextual conditions. Because it is a tool of the mind, IPB can be adapted to any operation for any size force. It is comprehensive enough to manage the seemingly overwhelming amounts of information coming from many sources. It is immediately available and does not require the deployment of sophisticated equipment. To successfully adapt IPB to an urban environment (U-IPB), it must include an analysis of a city's unique attributes—buildings, infrastructure, people, etc. For example, to achieve situational awareness in an urban area, it would be important to include street widths, odd building construction types or building mixes, and unusual street names.

Weather, Enemy, and Terrain (WET)
Weather: Will it be clear, hot, cold, rainy, snowing, storming, or a dense fog? How will the weather affect the officers' ability to operate?

Enemy: Who are the threat actors? Where are they? How well are they equipped and trained? What strategies and tactics do they utilize? What is their likely target? What are their estimated numbers and where are they set up? What movements are they making? How well do they know you and your methods and positions?

Terrain: Terrain dictates how you move and operate. Are your officers trained and equipped appropriately? Can their equipment function properly in the terrain? Are there natural or manmade obstacles to overcome, avoid, or used to your advantage? What are the avenues of approach to the incident site?

four steps by pulsing out requests for information.

Step 1: Define the Operational Space

The first step is defining the operational space, or Opspace. This includes identifying areas or sites that may be targeted by terrorists and that will be covered by intelligence collection assets, and ascertaining exactly what critical infrastructure/key resource (CI/KR) sites exist in the area. This process of defining the Opspace observes factors locally and globally.

Step 2: Describe the Operational Space Effects

In this step, Response Information Folders (RIFs) are developed for key venues, such as CI/KR sites or systems and cultural or entertainment locations where large crowds typically gather. RIFs contain information on what an adversary would

Mission Folders: Playbooks and Response Information Folders (RIFs)
IPO emphasizes Mission Folder development: a package of standardized playbooks, Response Information Folders, and intelligence reports for sharing threat and/or incident information. The IPO process organizes and displays information in a standard format to minimize ambiguity and speed the decision cycle.

Playbooks: Playbooks are developed for classes of threat. They provide preplanned general guidance for assessing a complex situation. The TEW utilizes them as an internal analytical tool. They guide TEW assessment activities before, during, and after an attack. They identify common considerations and typical intelligence requirements that decision-makers are likely to need. The LA TEW has developed playbooks for chemical terrorism, biological terrorism, food surety, water supply surety, suicide bombings, large vehicle bombings, laser threats, radio frequency weapons, and radiological/nuclear terrorist incidents.

Response Information Folders: RIFs are a terrain awareness tool to guide integrated emergency response at a specific, high-profile target within a specific jurisdiction, based upon a specific threat type. A RIF could include site plans, terrain analysis, interior and exterior plume dispersal models, blast analysis, and maps indicating vulnerable points and potential sites for triage, evacuation, and incident support.

Mission Folders: Mission Folders are incident-specific, combining Playbooks and RIFs with time-sensitive threat information. A Mission Folder is designed to provide the unified command structure, field incident commanders, staff at operation centers, and commanders of follow-on resources with the detailed intelligence information that will help them to resolve a complex incident.

consider to be high value or high pay-off targets. They also provide an understanding of how a location would be affected by population, terrain, and weather in a variety of settings or contexts.

Step 3: Evaluate the Opposing Force for Potential Threat Elements
The third step is to identify and evaluate the opposing force (OPFOR) or potential threat elements, such as al-Qaeda or other threat actors, and the threats they may employ by class (*i.e.*, chemical, biological, radiological, nuclear, explosive, suicide bombing). It is in this step that indications and warning are most analyzed. A key component of this analysis process is Adaptive Red Teaming, which uses and develops playbooks or multifaceted intelligence products to shape a response. Playbooks provide preplanned general guidance for use in complex situations, such as a chemical or biological attack. They are threat specific and can be developed for each echelon of response or threat assessment.

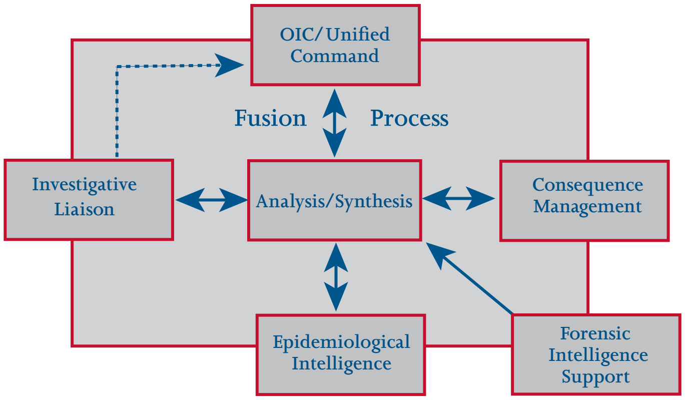
Step 4: Determine OPFOR and Friendly Courses of Action
The fourth step eventually feeds back into the first step, and is the determination of OPFOR and friendly courses of action (COAs). This step builds on all the previous steps and relies upon an accurate assessment of the current situation. This includes an assessment of the response forces that have been deployed or that may be needed. Completed intelligence products are also disseminated to support operations.

Intelligence Fusion and Analysis

To perform intelligence fusion and analysis, the TEW utilizes a number of practices and capabilities to support the intelligence process. This includes the synthesis of a number

Adaptive Red Teaming is the process of looking at our vulnerabilities and actions from the perspective of an adversary. It is based upon military concepts of a “red team” or “red cell” that seeks to attack friendly (or “blue”) forces. In the TEW context, Adaptive Red Teaming involves looking at all phases of operations—pre-, trans-and post-attack—through the eyes of an adversary. The process is adaptive since it is tailored to specific operational needs and analytical requirements. It can be applied to vulnerability assessments, analysis of potential threats, course of action development or as part of anticipating a terrorist operation cycle. It also can help the TEW identify its own operational requirements and prioritize its workload, information collection and analytical efforts.

Figure 2: TEW Organization and the Fusion Process



of intelligence disciplines and approaches. TEW personnel need to understand each of these processes and master the intelligence cycle and the component analytical tools.

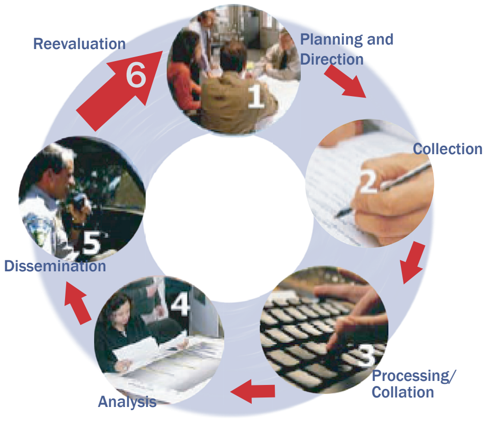
As part of the overall fusion process, the "Intelligence Cycle" is a way of describing the process that converts raw information into intelligence. It is based upon filling the intelligence requirements of a variety of intelligence consumers or users, and has six basic elements:

- Planning and Direction
- Collection
- Processing / Collation
- Analysis / Production
- Dissemination
- Reevaluation

The OIC cell is responsible for direction of the other cells, based on requirements set by executives and operators in the TEW and fusion center stakeholder and national intelligence communities.

Figure 3: Intelligence Cycle

(Source: Global, National Criminal Intelligence Sharing Plan)



Collection includes obtaining information from a number of varied sources and disciplines: investigators, informants, open sources, and technical sources. Fusing all of these together is known as all-source fusion or Multi-INT fusion. Processing includes the analysis of information, while production turns the information into a usable intelligence product for dissemination to the appropriate entities for use before, during, and after operations. All TEW cells participate in these steps at the direction of the OIC cell and in coordination with the Analysis/ Synthesis cell.

"During routine periods, the TEW scans the horizon looking for events or indicators that may pose a threat."

During any span of time, the TEW adjusts its focus to optimize its efforts. Scanning, monitoring, and forecasting are three major segments of this workflow. During routine periods, the TEW scans the horizon looking for events or indicators that may pose a threat. When a specific potential threat is observed, the TEW monitors the situation to develop an assessment. When a threat is expected to mature, the TEW forecasts the impact on the agencies it serves. Thus, the TEW can discern general trends and potentials and match them with a specific group's capabilities and intentions. Before an attack or threat occurs, this is known as indications and warning. Once a threat or attack is anticipated or occurs, the TEW develops an assessment of its impact known as an Operational Net Assessment. A detailed description of these processes and their relationship with the TEW's IPO methodology will be contained in a future TEW publication.

Training and Exercising the TEW

In order to perform proficiently, individual TEW staff members, each TEW cell and the TEW as a whole require training in intelligence concepts, analytical tradecraft, terrorist groups, legal concepts, and a number of specific analytical tools. The TEW then needs to regularly exercise its skills at various phases of counterterrorist operations, *i.e.*, performing indications and warning and operational net assessment at pre-, trans-, and post-incident phases. A TEW should conduct these exercises in conjunction with command staff, emergency operations centers, field personnel, and other TEWs and intelligence fusion centers.

TEW Tools

While skilled and highly trained staff members are a TEW's strongest asset, a number of tools can be employed to enhance the depth and speed of analysis. These tools include databases, access to automated justice systems, information clearinghouses, and access to information about available resources.

Synthesizing information from multiple databases, data warehouses, data sources, and files is enhanced by using automated, or data mining tools. In addition, a number of visualization tools, such as graphic data displays and other imaging and mapping products, help TEW members gain a common operating picture and develop intelligence products. These require hardware, monitors, projectors, wireless communication capabilities, servers, access to internet portals and monitors, such as large format plasma screens and "smart boards," to display and manually manipulate information that can also be captured digitally.

Exercising the TEW:
Operation Talavera and Operation Chimera

The Los Angeles County Operational Area (OA) Three-Year Exercise Plan was developed and is implemented, in accordance with the DHS, G&T, Homeland Security Exercise and Evaluation Program (HSEEP). The exercise plan is focused on providing the OA's public safety and emergency management agencies and their coordination partners with exercise events tailored to emphasize readiness for CBRNE/WMD incidents. The exercise strategy is built on a series of Workshops and Tabletop Exercises (TTX), which progressed to a series of tailored, multidiscipline Functional Exercises (FEX) that culminated in Full-Scale Exercises (FSE) for each CBRNE/WMD area.

Implementation of the current Three-Year Exercise Plan began with the 2004 exercise program—Operation Talavera. Operation Talavera consisted of 24 exercises focused on a radiological dispersal device scenario. This program established a baseline of performance and evaluation against which improvement in the outlying exercise years (2005-2007) will be measured.

The 2005 exercise program, Operation Chimera, sought to build on and incorporate lessons learned and After-Action Report/Improvement Plan recommendations from the previous year to ensure measurable improvement and advancement in the OA's capability to respond to and recover from a terrorist WMD attack. Operation Chimera consisted of 36 progressive exercises based on a biological (aerosolized anthrax) scenario.

Both exercise series focused on the range of activities related to anticipating, identifying, and responding to terrorist threats. To accomplish this goal, the exercises incorporated the Los Angeles TEW in a variety of roles designed to support emergency response agencies, unified command, and EOCs. Both Operation Talavera and Operation Chimera began by exercising the TEW's capacity to provide indications and warning in order to prevent or deter terrorist activity. Additionally, the series included TEW post-attack intelligence support to response entities. The TEW was exercised individually in TTX and FEX, as well as with the entire emergency response and management system during the full-scale exercise.

Secure telephones and faxes that enable access to classified information, as appropriate, software, communications security (COMSEC) applications and equipment, firewall and information security capabilities, and the training to use them are also helpful.

Unlike natural disasters or many types of traditional criminal activities, terrorist activities involve a threat conducted by constantly thinking and adapting adversaries. This opposing force is capable of reading our actions and intentions and adjusting their activities as needed. Operational Security, known as OPSEC, is a risk management tool used to deny the terrorist adversary with detailed information on our intentions, capabilities, response plans, and status of investigations. OPSEC is an essential adjunct to officer safety and investigative integrity. Terrorists are known to conduct reconnaissance (including seeking information about our training, capabilities, equipment and disposition of personnel, response and investigative resources, response and operations plans) that includes surveillance and counterintelligence operations. Maintaining OPSEC helps protect our personnel and our ability to respond effectively. OPSEC is the process that denies terrorists critical information that can be used to compromise our operations.

TEW Products

The TEW produces a number of products to inform a range of users about current and potential threats and their resulting impact. These products are targeted to specific users and are relevant to each user's specific mission and responsibility. In addition to the advisories, alerts or warnings, Response Information Folders, Mission Folders, and Playbooks discussed earlier, these TEW products include reports, net assessments, and issue-specific papers.

Reports: OSINTrep, Weekly Field Report, TEW Executive Weekly
The *OSINTrep* is a monthly product. It contains information collected from open sources that may serve as indicators of global, national, and/or local terrorist trends and potential threats, as well as related legal and policy developments and information on intelligence studies and counterterrorist tradecraft. It is disseminated to participants of the TEW monthly meeting and to analysts and other TEWs and fusion centers, as appropriate.

The Weekly Field Report is targeted toward field personnel. Restricted to one or two pages, it contains an overview of significant leads reported the previous week, information of local or regional relevance, key incidents and specific types of information the TEW would like to have reported back to the TEW.

This request for information, commonly known as an RFI, generally provides focus to the field collection efforts of the law enforcement, fire, and/or the health disciplines.

The TEW Executive Weekly is a more comprehensive report for executives and analysts. It contains analysis of global, domestic, and local trends, reports of key incidents, leads, or events.

Net Assessments

The TEW also produces a number of reports for special needs. These include net assessments and issue papers. Net assessments are produced when a significant event or indicator changes the threat or response posture in the TEW's area of operations. This report is provided to agency executives and the Los Angeles County EOC staff. A net assessment could occur after a major terrorist threat or attack in another area of operations, after a local event or in response to a change in the HSAS level.

Issue-Specific Papers

Issue-specific papers inform decision- or policy-makers of significant strategic issues, such as emerging threats and vulnerability or risk assessments. These are developed on an as-needed basis.

Conclusion

The TEW has successfully adapted since its inception to form a foundation for local and regional intelligence fusion and decision support for all phases of terrorist threat or incident response. Local experts from law enforcement, the fire service, health services, and other pertinent disciplines are able to come together, bringing their individual expertise and sphere of responsibility to develop a comprehensive picture of current and future situations. The TEW

"The TEW has provided a nimble, scalable capability that links Federal, State, and local agencies together in a top-down, bottom-up, multilateral fashion to effectively and efficiently communicate, collaborate, and share information and intelligence as TEWs and fusion centers are emerging across the Nation."

TEW and Critical Infrastructure Protection

The TEW supports critical infrastructure protection efforts, including activities that have resulted in threat assessments of the vulnerability and consequences of an attack on critical infrastructure/key resource (CI/KR) assets or systems. One example is Operation Archangel in Los Angeles. These efforts play a vital role in support of incident pre-planning activities, as well as TEW support of incident response and resource allocation. Completed vulnerability and threat assessments directly support and guide the development of TEW products and tools, including playbooks, RIFs, and mission folders. The TEW may also function as a State, local, Tribal, or regional *Infrastructure Node*, as described in the National Infrastructure Protection Plan (NIPP), which serves to share CI/KR information and/or related intelligence with Federal partners.

has provided a nimble, scalable capability that links Federal, State, and local agencies together in a top-down, bottom-up, multilateral fashion to effectively and efficiently communicate, collaborate, and share information and intelligence as TEWs and fusion centers are emerging across the Nation. National information must be integrated with local capabilities to discern threats before they mature and to effectively marshal response when they do. Within a national information sharing and fusion process network, TEWs provide support to help negotiate the continuing war against terrorism and protect the homeland.

This document provides an overview of the TEW concept, its application in Los Angeles and key issues involved in organizing a TEW and linking with the growing national information sharing network of TEWs and intelligence fusion centers. Detailed discussion of TEW operations, intelligence fusion and analytical concepts, threat assessment, intelligence production, and course of action development for counter-terrorism will be covered in future TEW publications.

Chapter Five: The TEW Expansion Program

The U.S. Department of Homeland Security (DHS) has recognized the Los Angeles County TEW as a best practice for replication throughout the country. It is a practical way of building and integrating information sharing and assessment capabilities, as well as and implementing the intelligence fusion process. DHS recognizes the success of the TEW in gathering, analyzing, and disseminating large quantities of intelligence information from a local or regional, multidisciplinary perspective, while ensuring a flow of intelligence information across all sectors and through all levels of government. It also recognizes that the TEW is scalable, allowing current and emerging TEWs to develop their capabilities based on local threats and available resources, while benefiting from the efficiency found in common operating methods and network protocols.

Therefore, DHS offers the TEW TA Expansion Program to provide support to State, Urban Area (UA), and local jurisdiction sites as they may consider developing and implementing their own TEW. The TEW TA Expansion Program also provides workshops and lessons learned about establishing TEW fusion center operations and how to share resulting information. Included in this approach are strategies to assist in terrorism deterrence, prevention, detection, apprehension, and response efforts.

DHS also encourages support for the development of TEWs and fusion centers through a variety of Federal, State, and UA grant programs and resources, including the State Homeland Security Program (SHSP), Urban Areas Security Initiative (UASI) Program, and the Law Enforcement Terrorism Prevention Program (LETPP), among other grants available across the Federal government, such as those available through the U.S. Department of Justice's Bureau of Justice Assistance (BJA) and the Office of Community Oriented Policing (COPS), as well as the U.S. Department of Health and Human Services. Additional resources through a variety of other grants, TA, training, and exercise programs may also provide assistance to jurisdictions as they build a State, local, and/or regional intelligence fusion process capacity.

National TEW Resource Center

In addition to these familiarization and training opportunities, DHS sponsors the National TEW Resource Center housed at the LA TEW. The resource center is operated by the Los Angeles Sheriff's Department and staffed by LA TEW personnel. It produces reference and resource materials and houses a resource library with information on lessons learned, TEW processes, and intelligence practices. The resource center will also maintain a registry of TEWs and facilitate personnel exchanges, training, and exercise opportunities for the TEW network.

Joint Regional Intelligence Center

The LA TEW plans (as of Winter 2005-2006) to move from its original headquarters at the Los Angeles County Emergency Operations Center into the Los Angeles Joint Regional Intelligence Center (JRIC). This groundbreaking cooperative initiative will fully integrate intelligence intake, vetting, analysis/fusion, and synthesis. It will disseminate developed intelligence, provide analytical case support, analyze trends, and provide tailored analytical products to end users.

The JRIC, with the infusion of increased personnel, will operate 24 hours a day, seven days a week. Although initially focused exclusively on terrorism, it is envisioned that someday the JRIC will expand to support the analysis needs of the law enforcement community across all programs, *i.e.*, crime types. As a foundational concept, the new JRIC will enhance and strengthen the partnerships among the participating local agencies while increasing the number of Federal and State-level participants, exploiting existing and new agencies' unique processes and best practices, while integrating those enhancements into a bigger, better supported and connected initiative. The JRIC could therefore be described as a larger TEW augmented by additions to the TEW membership. The TEW will continue its mission, *i.e.*, intelligence support by gathering, vetting, and analyzing tips and leads, open-source reporting, and national source exploitation, and document production. Terrorism investigations will continue to be referred to the FBI's JTTF.

"Although initially focused exclusively on terrorism, it is envisioned that someday the JRIC will expand to support the analysis needs of the law enforcement community across all programs, i.e., crime types."

The JRIC will be a multi-agency cooperative initiative—the first of its kind in the area. The founding agencies include the FBI, U.S. Attorney's Office for the Central District of California, the California Department of Justice, LASD, and the LAPD. Other agencies are encouraged to provide analysts to staff the JRIC; the JRIC's services will be available to all law enforcement agencies throughout the seven county region. Those counties include Riverside, San Bernardino, Orange, Los Angeles, Ventura, Santa Barbara, and San Luis Obispo.

Related initiatives, including the FBI's Los Angeles Terrorism Threat Squad, will also be housed at the JRIC, which is located adjacent to the existing Joint Drug Intelligence Group (JDIG). The JRIC is working with the State of California to serve as one of its Regional Terrorism Threat Assessment Centers (RTTACs). Arrangements are also being made to allow analysts access to the FBI, State, LASD, and LAPD databases, as well as other government databases and classified intelligence through the JDIG.

The partnerships formed in the JRIC will allow it to become the central contact point for law enforcement and homeland security intelligence, thereby enabling a smoother flow of leads and intelligence to prevent duplication, fragmentation, and circular reporting.

DHS Fusion Process Initiatives Overview

The following information pertains to fusion-related TA services designed, developed, and delivered through the DHS TA program. The goal of the overarching fusion-related TA program is to facilitate a process by which States, major metropolitan areas, local jurisdictions, and regions develop fusion centers that are tailored to their exact needs, goals, and objectives. However, it is vital that all fusion centers are developed based on a common process to ensure the establishment of a national network of information sharing and intelligence fusion capabilities. Currently, the primary component of the fusion process effort includes Pilot Fusion Process Orientation Technical Assistance.

The Fusion Process Orientation TA program assists States and local jurisdictions in the establishment of a common understanding of the *fusion process* and its implementation nationwide. The curriculum has been developed based on the findings of the HSAC's Final Report, "Homeland Security Intelligence and Information Fusion;" the Global Justice Information Sharing Initiative's "Guidelines for Establishing and Operating Fusion Centers at the Federal, State, Local, and Tribal Level;" and DHS fusion-related target capabilities, based upon the Target Capabilities List (TCL). The TCL is designed to assist jurisdictions and agencies in understanding and defining their respective roles in a major event, the capabilities required to perform a specified set of tasks, and where to obtain additional resources if needed.

Fusion process experts from across the State and local community assisted in organizing the information from the HSAC and Global efforts and in the development of a Fusion Process Orientation TA program. Additionally, participants in the HSAC and Global efforts served as the primary subject matter experts conducting TA service deliveries with support from the DHS TA program staff and other Federal agency representatives, as well as associated contractor support. The service delivery consists of three main components:

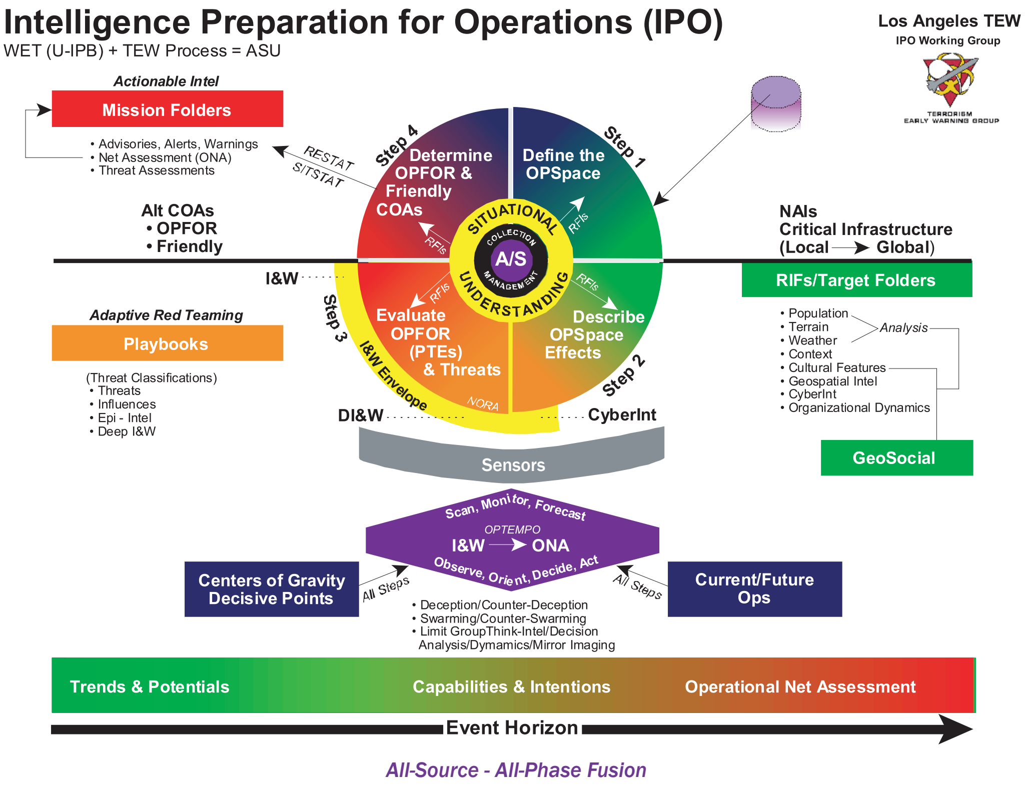
- Detailed assessment of the as-is fusion process environment
- Overview of the seven stages of the fusion process
- Collaborative development of a blueprint for developing/enhancing the fusion process based on the as-is environment

The Fusion Process Orientation TA will ensure that States, local jurisdictions, and regional fusion process capabilities are accurately assessed and strengths/weaknesses are leveraged to develop an actionable blueprint for the establishment or enhancement of the fusion process based on current capabilities and a common understanding of the operational environment. Future additional TA services may be developed to correspond with the four fusion-related TCLs:

- Information Gathering and Recognition of Indicators and Warnings
- Intelligence Analysis and Production
- Intelligence/Information Sharing and Dissemination
- Law Enforcement Investigation and Operations

These services, along with the TEW TA Expansion Program, which is a best practice for implementing the fusion process, will assist in the design, development, and/or enhancement of State, local, or regional fusion process capabilities, and will also ensure that the State and local grantees have direct access to the appropriate fusion process subject matter experts.

Appendix I: Intelligence Preparation for Operations



Intelligence Preparation for Operations (IPO)

WET (U-IPB) + TEW Process = ASU

Los Angeles TEW

IPO Working Group

TERRORISM EARLY WARNING GROUP

Actionable Intel

Mission Folders

- Advisories, Alerts, Warnings
- Net Assessment (ONA)
- Threat Assessments

RESTAT

SITSTAT

Alt COAs
- OPFOR
- Friendly

I&W

Adaptive Red Teaming

Playbooks

(Threat Classifications)
- Threats
- Influences
- Epi - Intel
- Deep I&W

Step 4 — Determine OPFOR & Friendly COAs

Step 1 — Define the OPSpace

Step 2 — Describe OPSpace Effects

Step 3 — Evaluate OPFOR (PTEs) & Threats

RFIs

SITUATIONAL UNDERSTANDING

COLLECTION MANAGEMENT

A/S

I&W Envelope

NORA

DI&W

CyberInt

NAIs

Critical Infrastructure

(Local ⟶ Global)

RIFs/Target Folders

- Population
- Terrain
- Weather
- Context
- Cultural Features
- Geospatial Intel
- CyberInt
- Organizational Dynamics

Analysis

GeoSocial

Sensors

Scan, Monitor, Forecast

OPTEMPO

I&W ⟶ ONA

Observe, Orient, Decide, Act

Centers of Gravity Decisive Points

All Steps

Current/Future Ops

All Steps

- Deception/Counter-Deception
- Swarming/Counter-Swarming
- Limit GroupThink-Intel/Decision Analysis/Dymamics/Mirror Imaging

Trends & Potentials

Capabilities & Intentions

Operational Net Assessment

Event Horizon

All-Source - All-Phase Fusion

Appendix II: References and Additional Reading

Articles and Papers

John P. Sullivan. “A Cooperative Vehicle for Threat Assessment, A Case Study: Los Angeles County Terrorism Early Warning Group.” *The InterAgency Board for Equipment Standardization and Interoperability, Annual Report*, 2000.

John P. Sullivan. “Intelligence Preparation for Operations: Developing Tools to Support Decision Making in Specific Incidents.” *The InterAgency Board for Equipment Standardization and Interoperability, Annual Report,* 2000.

Matt Begert and Dan Lindsay. “Intelligence Preparation for Operations.” *Non-State Threats and Future Wars*, 2003.

John P. Sullivan and Robert J. Bunker, Ph.D. “Multilateral Counter-Insurgency Networks.” *Low Intensity Conflict and Law Enforcement,* Vol. 11, 2002.

Michael Grossman. “Perception or Fact: Measuring the Effectiveness of the Terrorism Early Warning (TEW) Group.” Masters Thesis, Naval Postgraduate School, 2005.

John P. Sullivan. “Networked Force Structure and C4I.” *Small Wars and Insurgencies,* Vol. 13, No. 2. 2002, and *Non-State Threats and Future Wars*, 2003.

Lois Pilant. “Strategic Modeling.” *Police Magazine, 2004.*

John P. Sullivan, “Terrorism Early Warning Groups: Regional Intelligence to Combat Terrorism,” in Russell Howard, James Forest, and Joanne Moore (Eds.), *Homeland Security and Terrorism: Readings and Interpretations.* New York: McGraw-Hill, 2005.

Books

John Sullivan, Robert J. Bunker, Ph.D., Ernest Lorelli, Howard Sequine, and Matt Begert. *Unconventional Weapons Response Handbook, First Edition.* Jane's Information Group, 2002.

Executive Orders

President George W. Bush, Executive Office of the President of the United States. "Executive Order 13354: National Counterterrorism Center," 2004.

President George W. Bush, Executive Office of the President of the United States. "Executive Order 13355: Strengthened Management of the Intelligence Community," 2004.

President George W. Bush, Executive Office of the President of the United States. "Executive Order 13356: Strengthening the Sharing of Terrorism Information to Protect Americans," 2004.

President George W. Bush, Executive Office of the President of the United States. "Information Systems Council in response to EO 13356: Initial Plan for the Interoperable Terrorism Information Sharing Environment," 2004.

Fact Sheets

United States Department of Homeland Security. "Homeland Security Operations Center (HSOC)," 2004.

President George W. Bush, the Executive Office of the President of the United States. "President Issues New Orders To Reform Intelligence," 2004.

Homeland Security Presidential Directives

President George W. Bush, Executive Office of the President of the United States. "Homeland Security Presidential Directive 3: Homeland Security Advisory System," 2002.

President George W. Bush, Executive Office of the President of the United States. "Homeland Security Presidential Directive 5: Management of Domestic Incidents," 2003.

President George W. Bush, Executive Office of the President of the United States. "Homeland Security Presidential Directive 8: National Preparedness," 2003.

Legal Considerations

"Intelligence Reform and Terrorism Prevention Act of 2004," Public Law 108-458, 2004.

"Robert T. Stafford. Disaster Relief and Emergency Assistance Act," as amended by Public Law 106-390, October 30, 2000. United States Code, Title 42.

Reports

Thomas H. Kean, Chair, and Lee H. Hamilton, Vice Chair. "The Final Report of the National Commission on Terrorist Attacks Upon the United States." *The 9/11 Commission Report*, 2004.

United States Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, and Global Justice Information Sharing Initiative. "Fusion Center Guidelines–Developing and Sharing Information and Intelligence in a New World," 2005.

United States Department of Homeland Security, Homeland Security Advisory Council, Intelligence and Information Sharing Initiative. "Homeland Security Intelligence and Information Fusion," 2005.

Co-Chairmen: The Honorable Laurence H. Silberman and The Honorable Charles S. Robb. "The Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction." *Comission Report to the President of the United States*, 2005.

United States Department of Homeland Security, Homeland Security Advisory Council, Intelligence and Information Sharing Initiative. "Intelligence and Information Sharing Initiative Final Report," 2004.

Global Justice Information Sharing Initiative, International Association of Law Enforcement Intelligence Analysts, Inc. "Law Enforcement Analytic Standards," 2004.

David Carter, Michigan State University. Funded by the Office of Community Oriented Policing, Department of Justice. "Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies," 2004.

United States Department of Justice, Global Justice Information Sharing Initiative, Counter-Terrorism Training Working Group. "Minimum Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies Report, Findings and Recommendations," 2004.

United States Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, Global Justice Information Sharing Initiative (NCISP). "National Criminal Intelligence Sharing Plan," 2005.

United States Department of Homeland Security. "National Incident Management System," 2004.

United States Department of Homeland Security, Office of Homeland Security. "National Strategy for Homeland Security," 2002.

Markle Foundation Task Force on National Security in the Information Age. "Protecting America's Freedom in the Information Age," 2002.

United States Department of Homeland Security, U.S. Department of Justice, and Federal Bureau of Investigation. "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," 2005.

Appendix III: Glossary

28 CFR part 23: A guideline for law enforcement agencies that operate federally funded, multi-jurisdictional criminal intelligence systems, specifically providing guidance, submission, and intelligence of criminal intelligence information, security, inquiry, dissemination, review, and purge processes.

Access: The authority, ability, and opportunity to be admitted into a controlled environment or retrieve controlled data or information.

Administrative Analysis: The provision of economic, geographic, or social information to administrators. The analysis of economic, geographic, demographic, census, or behavioral data to identify trends and conditions useful to aid administrators in making policy and/or resource allocation decisions.

Analysis: The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment. That activity whereby meaning, actual, or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment.

Coordination: The process of interrelating work functions, responsibilities, duties, resources, and initiatives directed toward goal attainment.

Classified Information/ Intelligence: A uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism, to ensure certain information be maintained in confidence in order to protect citizens, U.S. democratic institutions, U.S. homeland security, and U.S. interactions with foreign nations and entities.

Top Secret Classification: Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

Secret Classification: Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Confidential Classification: Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Law Enforcement Sensitive: Information that is only supposed to be released to law enforcement groups. Because the information is unclassified, however, it is often released to the public as well.

For Official Use Only: Information which is unclassified, but which the government does not believe should be subject to Freedom of Information Act requests is often classified as U//FOUO.

Classified National Security Information ("Classified Information"): Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Collaboration: A wide range of activities aimed at coordinating the capabilities, resources, and information possessed by various governmental and private-sector entities.

Communications Security (COMSEC): The communications security systems, services, and concepts that constitute protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of any/such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

Compromise: An unauthorized disclosure of classified information.

Criminal Investigation Analysis: The use of components of a crime and/or the physical and psychological attributes of a criminal to ascertain the identity of the criminal. An analytical process that studies serial offenders, victims, and crime scenes in order to assess characteristics and behaviors of offender(s) with the intent to identify or aid in the identification of the offender(s).

Deconfliction: The process or system used to determine whether multiple law enforcement agencies are investigating the same person or crime and which provides notification to each agency involved of the shared interest in the case, as well as providing contact information. This is an information and intelligence sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of an investigation.

Dissemination (of Intelligence): The release of information, usually under certain protocols. The process of effectively distributing analyzed intelligence using certain protocols in the most appropriate format to those in need of the information to facilitate their accomplishment of organizational goals.

Emergency Operations Center (EOC): The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place. An EOC may be organized by major functional disciplines such as fire, law enforcement, or medical services, by jurisdiction such as Federal, State, regional, county, city, tribal, or by some combination thereof.

Freedom of Information Act (FOIA): The Freedom of Information Act, 5 U.S.C. 552, enacted in 1966, statutorily provides that any person has a right, enforceable in court, to access Federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

Fusion: The process of managing and merging the flow of data, information and intelligence, with the end goal of deriving additional information and intelligence from the disparate sources that could have not been determined prior to the fusion

Fusion Center: A collaborative effort of two of more agencies who 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 by applying the concepts of fusion.

Homeland Security Advisory Council (HSAC): The Homeland Security Advisory Council (HSAC) provides advice and recommendations to the Secretary of Homeland Security on matters related to homeland security. The Council is comprised of leaders from State and local governments, first responder communities, the private sector, and academia.

Information Security: As used in this directive, information security is the system of policies, procedures and requirements established under the authority of EO 12958, as amended, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Information Sharing: A multi-jurisdictional, multidisciplinary exchange and dissemination of information and intelligence among the Federal, State, and local layers of government, the private sector, and citizens. The goal of information sharing is to facilitate the distribution of useful, relevant, and timely information and/or intelligence to the entities that need it.

Information Sharing and Analysis Centers (ISAC): Information Sharing and Analysis Centers (ISAC) were established by Presidential Decision Directive-63 to allow critical sectors to share information and work together in an effort to protect our critical infrastructures and minimize vulnerabilities

Intelligence Analysis: The process of examining raw data with the intent of identifying any number of forming threat pictures, recognizing potentially harmful patterns, or connecting suspicious links to discern potential indications or warnings. The analysis may focus on the raw data's relevance to a suspected or known potential threat element, target, attack methodology; other related terrorist activity, or any combination of these aspects.

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 in nature. Intelligence is information that has been analyzed to determine its meaning and relevance. Information is compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. The product of the analysis of raw information related to crimes or crime patterns with respect to an identifiable person or group of persons in an effort to anticipate, prevent, or monitor possible criminal activity.

Intelligence Fusion: The merger of data and information for the purpose of analyzing, linking, and disseminating timely and actionable intelligence. It is focused on maintaining the larger-threat picture and consolidating analytical products among the various intelligence analysis units at the Federal, State, and local levels for tactical, operational, and strategic use.

Intelligence Process (Cycle): Planning and direction, collection, processing and collating, analysis and productions, dissemination. An organized process by which information is gathered, assessed and distributed in order to fulfill the goals of the intelligence function—it is a method of performing analytic activities and placing the analysis in a useable form.

Jurisdiction: A range, or sphere, of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authorities. Jurisdictional authority at an incident can be political or geographical (*e.g.*, city, county, tribal, State, or Federal boundary lines), or functional (*e.g.*, law enforcement, public health).

National Criminal Intelligence Sharing Plan (NCISP): A formal intelligence sharing initiative, supported by the U.S. Department of Justice, Office of Justice Programs, that securely links local, State, tribal, and Federal law enforcement agencies, facilitating the exchange of critical intelligence. The plan contains model policies and standards and is a blueprint for law enforcement administrators to follow when enhancing or building an intelligence function. It describes a nationwide communications capability that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives.

National Incident Management System (NIMS): Homeland Security Presidential Directive 5 directed the Secretary of Homeland Security to develop and administer a National Incident Management System. NIMS provides a consistent nationwide template to enable all government, private-sector, and nongovernmental organizations to work together during domestic incidents. NIMS is a comprehensive, national approach to incident management that is applicable at all jurisdictional levels and across functional disciplines. The intent of NIMS is to be applicable across a full spectrum of potential incidents and hazard scenarios, regardless of size, or complexity, and to improve coordination and cooperation between public and private entities in a variety of domestic incident management activities.

Need-to-Know: As a result of jurisdictional, organizational, or operational necessities, intelligence or information is disseminated to further an investigation.

National Response Plan (NRP): The NRP, using the NIMS, is an all-hazards plan that provides the structure and mechanisms for national-level policy and operational coordination for domestic incident management. Its purpose is to establish a comprehensive, national, all-hazards approach to domestic incident management across a spectrum of activities including prevention, preparedness, response, and recovery.

National Preparedness Goal: The goal aims for Federal, State, local, and tribal entities to achieve and sustain nationally accepted risk-based target levels of capability for prevention, preparedness, response, and recovery for major events, especially terrorism.

Open Storage Area: A room or area constructed and operated pursuant to this directive, for the purpose of safeguarding national security information that, because of its size or nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

Preparedness: The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private-sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources.

Prevention: Actions taken to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions taken to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Privacy (of Information): The assurance that legal and constitutional restrictions on the collection, maintenance, use and disclosure of personally identifiable information will be adhered to by criminal justice agencies, with use of such information to be strictly limited to circumstances where legal process permits use of the personally identifiable information.

Private Sector: Organizations and entities that are not part of any governmental structure. Private sectors include for-profit and not-for-profit organizations, formal and informal structures, commerce and industry, private emergency response organizations, and private voluntary organizations.

Requirement: A validated intelligence information need submitted to address an intelligence gap. Requirements can be “standing” (normally valid for months or years) or “*ad hoc*” (processed as they are identified, normally outside of planned, periodic requirements development and prioritization cycles).

Response: Activities that address the short-term, direct effects of an incident. Response includes the execution of emergency operations plans and incident mitigation activities designed to limit loss of life, personal injury, property damage, and other unfavorable outcomes.

Right-to-Know: Based on having legal authority, one's official position, legal mandates, or official agreements, allowing the individual to receive intelligence reports.

Risk Management: The decision-making process inherent in determining which critical infrastructure assets to secure, the assessment methods and resources used to address the security, and the cost-benefit calculus associated with those decisions.

SCI (Sensitive Compartmented Information): Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the director of the Central Intelligence Agency (CIA).

SCIF (Sensitive Compartmented Information Facility): An accredited area, room, group of rooms, buildings, or an installation where SCI may be stored, used, discussed, and/or processed.

Sensitive But Unclassified (SBU) Information: Information that has not been classified by a Federal law enforcement agency which pertains to significant law enforcement cases under investigation and criminal intelligence reports that require dissemination criteria to only those persons necessary to further the investigation or to prevent a crime or terrorist act.

Strategic Intelligence: Most often related to the structure and movement of organized criminal elements, patterns of criminal activity, criminal trend projections, or projective planning. An assessment of targeted crime patterns, crime trends, criminal organizations, and/or unlawful commodity transactions for purposes of planning, decision making, and resource allocation; the focused examination of unique, pervasive, and/or complex crime problems.

Tactical Intelligence: Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety. Evaluated information on which immediate enforcement action can be based; intelligence activity focused specifically on developing an active case.

Target Capabilities List (TCL): The TCL is designed to assist jurisdictions and agencies in understanding and defining their respective roles in a major event, the capabilities required to perform a specified set of tasks, and where to obtain additional resources if needed. Section II of the TCL contains capability descriptions and Section III provides an initial assignment of capabilities to levels of government.

Technical Assistance (TA): A process whereby help is provided to resolve problems and/or create innovative approaches to the prevention of, response to, and recovery from acts of terrorism and other hazards. TA provides services that identify and address problems, address items in an improvement plan from a completed exercise, fills in the gaps between equipment, training, and exercise programs, and assists in the development and/or execution of projects.

Terrorism: Any activity that (1) involves an act that (a) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and (b) is a violation of the criminal laws of the United States, or of any State or other subdivision of the United States; and (2) appears to be intended (a) to intimidate, or coerce, a civilian population; (b) to influence the policy of a government by intimidation or coercion; or (c) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

Threat Assessment: A strategic document which looks at a group's propensity for violence or criminality or the possible occurrence of a criminal activity in a certain time or place. An assessment of a criminal or terrorist presence within a jurisdiction integrated with an assessment of potential targets of that presence and a statement of probability that the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal's or terrorist's opportunity, capability, and willingness to fulfill the threat.

Universal Task List (UTL): The UTL is a tool that defines the tasks that need to be performed by someone in response to an incident of national significance, but no single jurisdiction or agency, would be expected to perform every task listed. The UTL provides a common language and common reference for homeland security professionals at all levels of government and the private sector. It describes what tasks are to be performed in terms common to incident management agencies across the country.

Violation: Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of EO 12958, as amended or its implementing directives; or any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of EO 12958, as amended.

Vulnerability Assessment: A strategic document which views the weaknesses in a system that might be exploited by a criminal endeavor. An assessment of possible criminal or terrorist group targets within a jurisdiction integrated with an assessment of the target's weaknesses, likelihood of being attacked, and ability to withstand an attack.

Appendix IV: Acronyms

A/S: Analysis/Synthesis Cell

ADNET: Anti-Drug Network

BJA: Bureau of Justice Assistance

CBP: Customs and Border Protection

CBRNE: Chemical, Biological, Radiological and Nuclear and Explosives

CI/KR: Critical Infrastructure and Key Resources

CIS: Critical Infrastructure Sensitive

CISAnet: Criminal Information Sharing Alliance Network

CJIS: Criminal Justice Information Services

CM: Consequence Management (Cell)

COA: Course of Action

COMSEC: Communications Security

CRIMINT: Criminal Intelligence

DHS: U.S. Department of Homeland Security

DIA: Defense Intelligence Agency

DOJ: U.S. Department of Justice

EEI: Essential Element of Information

EOC: Emergency Operations Center

EPI-INTEL: Epidemiological Intelligence (Cell)

FAST: Field Assessment Support Team

FBI: Federal Bureau of Investigations

FIG: Field Intelligence Group

FIS: Forensic Intelligence Support (Cell)

FGDC: Federal Geospatial Data Committee

FinCEN: Financial Crimes Enforcement Network

FOIA: Freedom of Information Act

G&T: Office of Grants and Training

GEOINT: Geospatial Intelligence

GIS: Geographic Information System

Global: Global Justice Information Sharing Initiative

HIDTA: High Intensity Drug Trafficking Areas

HSIN: Homeland Security Information Network

HSOC: Homeland Security Operation Center

HUMINT: Human Intelligence

IACA: International Association of Crime Analysts

IALEIA: International Association of Law Enforcement Intelligence Analysts

IC: Intelligence Community

ICE: Immigration and Customs Enforcement

ILO: Infrastructure Liaison Officer

IPO: Intelligence Preparation for Operations

INV-LNO: Investigative Liaison

ISAC: Information Sharing and Analysis Center

ISE: Information Sharing Environment

I&W: Indications and Warning

JTTF: Joint Terrorism Task Force

LEO: Law Enforcement Online

LES: Law Enforcement Sensitive

LNO: Liaison Officer

MOE: Measure of Effectiveness

NIMS: National Incident Management System

NLETS: National Law Enforcement Telecommunications System

NPG: National Preparedness Goal

NORA: Non-Obvious Relationship Awareness (or Analysis)

NRP: National Response Plan

OIC: Officer-in-Charge (Cell)

OIR: Other Intelligence Requirement

ONA: Operational Net Assessment

OODA: Observe-Orient-Decide-Act (Boyd's Decision Cycle)

OPFOR: Opposing Force

OPINT: Operational Intelligence

OPSEC: Operational Security

OPSPACE: Operational Space

OSINT: Open Source Intelligence

OSIS: Open Source Information System

PIR: Priority Intelligence Requirement

POC: Point of Contact

PSS: Public Safety Sensitive

RESTAT: Resource Status

RIC: Regional Intelligence Center

RIF: Response Information Folder (Target Folder)

RISSNet: Regional Information Sharing System Network

RFI: Request for Information

ROE: Rules of Engagement

SBU: Sensitive But Unclassified

SCI: Sensitive Compartmented Information

SCIF:Sensitive Compartmented Information Facility

SIR: Specific Intelligence Requirement

SITSTAT: Situation Status

SNA: Social Network Analysis

TEW: Terrorism Early Warning Group

TLO: Terrorism Liaison Officer

UAWG: Urban Area Working Group

USCG: United States Coast Guard

WET: Weather-Enemy-Terrain