2010 Sector CIKR Protection Annual Report

for the Emergency Services Sector

June 2010

Homeland Security

This page intentionally blank

2010 Sector CIKR Protection Annual Report for the
Emergency Services Sector

Released by:

Kory Whalen
Chief, Emergency Services Sector-Specific Agency

This page intentionally blank

Contents

Contents (Cont.)

Executive Summary

Pursuant to Homeland Security Presidential Directive 7 (HSPD-7),[1] the U.S. Department of Homeland Security (DHS) is responsible for managing, coordinating, and promoting activities to enhance security and resiliency across the Emergency Services Sector (ESS). Within DHS, this overarching responsibility is delegated to the National Protection and Programs Directorate's Office of Infrastructure Protection, specifically the Sector-Specific Agency (SSA) Executive Management Office Emergency Services Branch.

Under HSPD-7 and the National Infrastructure Protection Plan, each SSA is required to submit a Sector Critical Infrastructure and Key Resources (CIKR) Protection Annual Report to DHS. These reports communicate how CIKR protection is conducted in each sector, what priorities and requirements drive these efforts, and how such efforts are funded. The 2010 Emergency Services Annual Report describes activities conducted from May 1, 2009, to April 30, 2010.

Because ESS is mostly a non-regulated sector, the majority of these programs are voluntary and depend on the funding and resources of participating stakeholders. The broad diversity within the sector and the desire of owners and operators to strengthen their protective programs are reflected in the breadth of initiatives undertaken by sector partners. These include an array of activities such as developing mutual-aid agreements to share resources, promoting information sharing and developing training programs, initiating active or passive countermeasures, installing security systems, promoting workforce security programs, and implementing cybersecurity measures, among others. In addition, Federal, State, local, and tribal governments have sponsored a broad range of complementary protective programs including vulnerability and risk assessment processes and methodologies.

ESS is defined by the five disciplines that make up the sector: (1) Law Enforcement; (2) Fire and Emergency Services; (3) Emergency Management; (4) Emergency Medical Services; and (5) Public Works. In addition to these disciplines, ESS has the following specialized capabilities: Hazardous Materials, Search and Rescue, Explosive Ordnance Disposal, Special Weapons and Tactics and Tactical Operations, Aviation Units, and Public Safety Answering Points. Each of these disciplines and capabilities contributes to successful performance of ESS's vital functions, which tend to be organized at the State, local, tribal, and territorial levels of government. Moreover, they form the nucleus of a system of response elements that act as the Nation's first line of defense against terrorist attacks or natural hazards.

ESS comprises enthusiastic professionals who have guided the sector, especially in the areas of information sharing, first responder preparedness, sector training and awareness, research and development (R&D), and regional resiliency prevention and protection capabilities. Sector goals have been accomplished through close collaboration among many partners, including many practitioners from the sector, striving to make significant progress in these areas.

Among the sector's primary concerns are biological risks – either from the intentional release of biological substances or a natural contagious human disease. Both could seriously impair the

[1] A list of the acronyms used in this report follows Section 7.

health and response capability of the emergency responder workforce and therefore pose a risk to the sector. The potential short- or long-term health consequences and subsequent absenteeism are of concern for emergency responder agencies. Other threats that continue to be of concern to the sector include concurrent, strategic cyber attacks and complex, coordinated physical attacks, with multiple events affecting a large geographic region or multiple regions. Such attacks could diminish the sector's resiliency, sustainability, and resources.

In the last year, the sector has worked diligently to rewrite its Sector-Specific Plan and reevaluate and update its goals and objectives. Also, the SSA has studied and made adjustments to its CIKR taxonomy, closely aligning it with the Federal Emergency Management Agency (FEMA) National Incident Management System (NIMS) Resource Typing in order to better identify the sector assets.

Great collaborative progress, generally through practitioner-based working groups, has been made in the areas of information sharing. This year, the sector launched a pilot Homeland Security Information Network-Critical Sectors-Emergency Services portal, partnered with the Los Angeles Fire Department to develop a first-responder preparedness pilot program, and established the First Responder Coordinating Council (FRCC) and the First Responder Research, Development, Testing & Evaluation Working Group (FRWG).

The ESS recognizes the enormous efforts of first responders and agencies at all levels of government to identify capability gaps and ensure that CIKR protection and resiliency mission needs that impact the emergency response community are addressed. To achieve a national perspective on R&D needs and activities of the sector, the ESS leverages work done through DHS Science and Technology Directorate (S&T) components; FRCC, FRWG, and First Responder Technologies; Command, Control, and Interoperability; and the Capstone Integrated Product Teams. Additionally, the InterAgency Board is a key component, along with the DHS S&T.

In 2010, the ESS faced challenges similar to those encountered in 2009, including a historic economic crisis, continued governmental change, and global influenza issues. This Sector Annual Report demonstrates that the sector is focused on strengthening homeland security by enhancing information sharing, building capable responders, fostering unity of effort, and encouraging innovative approaches and solutions through leading-edge science and technology.

The priority of ESS is to keep emergency responders safe and to ensure they have the ability to respond and do their jobs. Working in a unified fashion and fostering the strong partnerships that it has created, the sector will continue to gain success. The SSA will serve the sector as a conduit to communicate the sector's priorities to other Federal agencies and ensure that the Sector Coordinating Council and Government Coordinating Council are informed of protective and resiliency activities that impact the sector.

Section 1: Introduction

The Emergency Services (ES) Sector-Specific Agency (SSA) coordinates with sector partners to facilitate the effective implementation of numerous protective programs that manage risk by focusing on the four aspects of the National Infrastructure Protection Plan (NIPP) protective spectrum: deter, detect, devalue, and defend. This approach ensures that risk is managed effectively by deterring threats, mitigating vulnerabilities, and minimizing consequences of all-hazards incidents. The ESS concentrates on protective programs that support sector resiliency by encompassing several areas such as skill proficiency, information sharing, cooperative agreements, and infrastructure resilience.

As a non-regulated sector, the majority of these programs are voluntary and depend on the funding and resources of participating stakeholders. The broad diversity within the sector, and the desire of owners and operators to strengthen their protective programs, are reflected in the breadth of initiatives undertaken by sector partners. They include an array of activities such as developing mutual-aid agreements to share resources, promoting information sharing and developing training programs, initiating active or passive countermeasures, installing security systems, promoting workforce security programs, and implementing cybersecurity measures, among others. In addition, Federal, State, local, and tribal governments have sponsored a broad range of complementary protective programs including vulnerability and risk assessment processes and methodologies.

Highlights of the 2010 ESS Sector Annual Report

- *Established Information Requirements Working Group.*
- *Launched a pilot Homeland Security Information Network-Critical Sectors-Emergency Services Sector (HSIN-CS-ESS) Portal.*
- *Federal Emergency Management Agency (FEMA) and Los Angeles Fire Department partnered with the Office of Infrastructure Protection (IP) to launch a First Responder Preparedness Pilot.*
- *U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate established the First Responder Coordination Council and the First Responder Research, Development, Testing & Evaluation Working Group.*
- *Completed and awaiting publication of 2010 Triennial Sector-Specific Plan (SSP).*

ESS is defined by the five disciplines that make up the sector: (1) Law Enforcement (LE); (2) Fire and Emergency Services; (3) Emergency Management; (4) Emergency Medical Services (EMS); and (5) Public Works. In addition to these disciplines, there are specialized capabilities: Hazardous Materials (HAZMAT), Search and Rescue (S&R), Explosive Ordnance Disposal (EOD), Special Weapons and Tactics and Tactical Operations (SWAT), Aviation Units, and Public Safety Answering Points (PSAPs). Each of these disciplines and capabilities contributes to successful performance of the Emergency Services Sector’s (ESS’s) vital functions, which tend to be organized at the State, local, tribal, and territorial levels of government. Moreover, they form the nucleus of a system of response elements that act as the Nation’s first line of defense against terrorist attacks or natural hazards.

Seven distinguishing characteristics help to define the ESS as a Critical Infrastructure and Key Resources (CIKR) Sector. These characteristics contribute to the sector profile and represent important factors for consideration in addressing sector security:

- The most critical feature of the sector is its large, geographically distributed base of facilities, equipment, and highly skilled personnel who provide services in both paid and volunteer capacities;

- It is largely organized at the State, local, tribal, and territorial levels of government, corresponding to the scales on which emergencies generally occur. The complex and dispersed nature of the sector makes it difficult to disable the entire system, but it also presents challenges in coordinating emergency responses across disciplines, regions, and levels of government;

- It relies heavily on interoperable communication and information technology systems to enable robust communications and appropriate coordination and management of diverse elements during emergency situations;

- It utilizes specialized transportation vehicles and requires secure transportation routes to facilitate sector operations because personnel, equipment, aid, and victims must be moved to and from scenes of emergencies;

- It has dependencies and interdependencies with multiple CIKR Sectors and the National Response Framework's Emergency Support Functions that supply elements for the operation and protection of ESS assets;

- The sector focuses primarily on the protection of other sectors and people, rather than protecting the sector itself, which presents unique challenges in addressing the protection of ES as a CIKR Sector; and

- ES involves primarily the public sector, but also includes private sector holdings, such as industrial fire departments, sworn private security officers, and private EMS providers.

The ESS partners have provided input to the report in many aspects, including overall sector improvement recommendations and examples of shared, as well as other program initiatives not driven by the U.S. Department of Homeland Security (DHS). All sector comments have been consolidated, discussed, and appraised for incorporation in the final report. This effort was accomplished through multiple in-person meetings, e-mail correspondence, and teleconferences.

The sector has matured particularly in the areas of information sharing, first-responder preparedness, sector training and awareness, research and development (R&D), and regional resiliency prevention and protection capabilities. The SSA continues to collaborate with its many partners including the National Sheriffs' Association (NSA), the International Association of Fire Chiefs (IAFC), the U.S. Department of Transportation (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA), the DHS Federal Emergency Management Agency (FEMA) and Science and Technology (S&T) Directorate, and many practitioners from the sector to make significant progress in these areas. Some of these programs are briefly introduced below.

The sector's Information-Sharing Working Group (ISWG) was established in 2009 to enhance the sector's information-sharing capabilities within ES and with other CIKR Sectors and Federal, State, and local partners. The Information Requirements Working Group (IRWG), a subcommittee of the ISWG, is a team of highly experienced practitioners charged with identifying ESS information requirements and developing the Homeland Security Information Network-Critical Sectors-ESS (HSIN-CS-ESS) portal. The work of this team has been recognized as an example not only by members of the ESS, but by other sectors as well.

FEMA and ESS have partnered with the Mayor of Los Angeles and Fire Chief of the Los Angeles Fire Department (LAFD) to develop and implement a Responder and Family Preparedness Pilot Project. The pilot program has three phases: education and training; policy assessment; and technical assistance plan. This program is a bottom-up approach to first-responder readiness, sector resiliency, and ultimately community preparedness.

NSA’s Homeland Security Initiative Training and IAFC’s National Hazardous Materials Fusion Center programs are two examples of sector partners’ programs. ESS partners, through these programs, continue to conduct regular training designed to build technical expertise for its members and develop information sharing through its Fusion Center.

The First Responder Coordinating Council (FRCC) serves as the Federal first-responder customer representing the technology, product, service, and standards needs of the 2.4 million first responders in the United States. The FRCC is a vehicle for the coordination of investment, programs, technology, research, development, and delivery of technological tools to first responders at the Federal, State, local, tribal and territorial levels. The Council facilitates effective interactions between S&T, the First Responder Technology Council (FRTC), and the First Responder Research, Development, Testing & Evaluation Working Group (FRWG). The FRWG has representation from four of the ESS disciplines: Emergency Management, EMS, Fire and Emergency Services, and LE.

The Protective Security Coordination Division (PSCD) has several programs, including the Regional Resiliency Assessment Program (RRAP), which is a cooperative interagency assessment. The RRAP resulted in more than $9 million in Buffer Zone Protection Program (BZPP) grant funding, which was allocated to build terrorism prevention and protection capabilities including planning and equipment acquisition by local LE and first responders.

The ISWG intends to develop a cybersecurity working group as a subgroup to identify gaps within the sector relative to cybersecurity. ESS has had discussions with National Cyber Security Division (NCSD) to specifically assess the cybersecurity posture of 9-1-1 Call Centers across the country.

The sector continues to face its challenges to focus on strengthening homeland security for ESS. The following sections of this report highlight some of the key progress made in 2010.

This page intentionally blank

Section 2: Sector Risk Considerations

Communities are highly dependent on first responders in emergencies, which vary from local accidents to large-scale disasters. Society often takes for granted the critical functions and services provided by first responders. Unlike other sectors, the ESS's most critical assets are its highly trained and specialized workforce. Emergency responders view their risk from an all-hazards perspective. Any type of incident, whether manmade or natural, local or regional, poses great risk to the responder. At a national level, due to the sector's structure and composition, there are very specific risks that are of greater concern to the sector itself than others, specifically contagious human diseases and cyber attacks. A widespread biological contaminant or cyber attack has the potential to spread quickly through numerous jurisdictions and/or States and thus impact the health and safety of large numbers of responders.

2.1 Biological Risks

The intentional release of contagious human disease could seriously impair the health and response capability of the emergency responder workforce and therefore poses a risk to the sector. The widespread release of a biological agent would impede the response efforts of local responders and impose burdens on all sectors that are dependent on ESS. Because they are often the first to arrive on the scene, ESS personnel would be among the first, sometimes unknowing, victims of such an attack and would be subjected to potential subsequent short- or long-term health consequences from the exposure as they perform their job duties. In addition, because of the insidious nature of a biological attack, such a release could go unnoticed beyond the contagious stage and continue to infect a significant number of unprotected emergency responders.

Although Influenza A (H1N1) was a natural, not a manmade, occurrence, it demonstrated the risk to the emergency responders with any disaster involving contagion or contamination. An influenza pandemic has the potential to negatively affect the number of first responders who can or will report for duty. First responder absenteeism is directly influenced by (1) employees' willingness to accept the real or perceived risk of reporting for duty (to themselves and/or to their family members); and (2) the employee's logistical ability to show up for work, which may be complicated due to illness of his or her dependents. To increase the likelihood of emergency responders reporting for duty, local, State, and Federal planning and preparedness efforts could include interventions that would mitigate absenteeism. These interventions would include giving priority or preference to emergency responders for vaccines or post-exposure prophylactic treatments.

2.2 Cyber Risks

The sector also is susceptible to the strategic targeting of cyber attacks on such business systems as the computer-aided dispatch (CAD) systems for the PSAPs and Emergency Communication Centers. The ability of the ESS to react and respond swiftly to incidents is a direct function of its ability to communicate and transmit accurate information. The sector's communication systems are at increased risk as criminals or terrorists could engage in spoofing (concealing caller ID from the actual originating location) or swatting (making emergency prank calls to 9-1-1 in an attempt to trick them to dispatch a SWAT or another emergency response team). Efficient command-and-control structures allow ESS personnel to maneuver and respond to incidents, assess the scene, and relay information to other partners, such as hospitals. The sector has preemptively positioned numerous redundant systems to take over in the event of a degradation of ESS information technology (IT) systems.

The risk associated with a terrorist targeting a single ESS element or asset is low; however, an attack on an ESS entity would adversely impact its emergency response capability for that locality or region. In contrast to the infrastructure composition of other CIKR Sectors, the highly trained workforce of ESS professionals and the electronic systems they use are most susceptible to attack because of the nature of the critical life-saving work performed. ESS assets are most vulnerable as secondary targets following an attack on a primary target.

The ESS is comprised of complex assets, systems, and networks that extend throughout the country. The disruption or loss of any one of these would have minimal consequences on overall ESS operations and therefore would not be elevated to a level of national significance. However, in the event of a complex, coordinated attack, with multiple events affecting a large geographical region or multiple regions, the sector's resiliency, sustainability, and resources would be severely impacted. While the sector is resilient and robust, multiple or widely distributed attacks could exhaust local, regional, and State resources. In an effort to diminish these risks and vulnerabilities, the sector, with the support of local, tribal, State, and Federal governments, has worked diligently toward the establishment of Mutual Aid Agreements (MAAs), Emergency Management Assistance Compacts (EMACs), and similar emerging regional compacts to provide vital mitigation alternatives in response to catastrophic events that could overwhelm the sector and deplete resources.

The sector's R&D capability gaps[2] are varied to address not only the highest threat to the first responder such as biological and cyber incidents, but are also directed at protection of capabilities such as EMS training, alerts and warnings, and interoperable communications. Key risk mitigation activity (RMA) information-sharing activities, such as the HSIN-CS-ESS portal and the Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC), ensures the availability and flow of accurate, timely, and relevant information and or intelligence that serves to enhance the resilience of the sector.

[2] Attachment B is the R&D Activities/FRWG Capability Gap List.

Section 3: Sector Goals and Objectives

Supporting the overarching goal of the NIPP requires a coordinated approach for protective activities across the sector. Sector security goals encompass the goals laid out by Homeland Security Presidential Directive 7 (HSPD-7) for all Federal departments and agencies with regard to infrastructure protection, as well as goals developed specifically for the ESS. The sector vision statement provides the framework to direct its overarching risk management focus and strategy.

3.1 ESS Vision Statement

The ESS vision statement serves as a description of the desired end-state protective posture that contributes to a coordinated direction for protective activities across the sector.

Vision Statement for the Emergency Services Sector

An Emergency Services Sector in which facilities, key support systems, information and coordination systems, and personnel are protected from both ordinary operational risks and from extraordinary risks or attacks; ensuring timely, coordinated all-hazards emergency response and public confidence in the sector.

3.2 Sector Goals

The SSA collaborates with sector partners to create goals that represent the sector’s view of how best to support the overarching goal of the NIPP and to achieve a secure, protected, and resilient ESS. These goals underline the sector’s emphasis on protecting the human as well as physical and cyber assets of the sector. The following goals emphasize collaboration among all the sector partners, including an engaged sector community that is well-informed and takes responsibility for its own safety and sustainability. These goals provide the framework for enduring capabilities that serve the sector’s preparedness and protective needs over the long term, which promotes sustainability and resilience. From these goals and specific objectives, milestones are developed that allow the sector to measure its progress. The CIKR protection goals for the ESS are (1) Partnership Engagement; (2) Situational Awareness; (3) Prevention, Preparedness, and Protection; and (4) Sustainability, Resilience, and Reconstitution.

3.2.1 Goal 1: Partnership Engagement

To build a partnership model that enables the sector to effectively sustain a collaborative planning and decision-making culture. The objectives for Goal 1 are to:

- Strengthen regional approaches to CIKR protective planning and decision-making;

- Utilize sector-wide processes to identify and close gaps through the development of protective programs;

- Develop and refine processes and mechanisms for ongoing coordination and collaboration, including majority sector participation on councils and working groups that support development and implementation of protective programs;

- Coordinate the identification of R&D priorities for the ESS, and the pursuit of creative, affordable methods and tools for performing sector CIKR protection activities; and

- Provide the platform to reduce redundancy and duplicative efforts by both public and private entities within the sector.

3.2.2 Goal 2: Situational Awareness

To support an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant CIKR information and intelligence about terrorist threats, attacks, natural disasters, or other incidents. The objectives for Goal 2 are to:

- Collaborate, develop, and share appropriate threat and vulnerability information among public and private sector partners;

- Expand strategic analytical capabilities that facilitate public and private sector partner collaboration to identify potential incidents;

- Compile and disseminate best protective practices and lessons learned materials related to development and implementation of protective measures or activities, including cost-benefit analyses;

- Increase awareness of cybersecurity issues impacting ESS infrastructure to encourage sharing and implementation of cybersecurity programs; and

- Report on CIKR protection effectiveness to relevant sector partners throughout the Federal, State, and local governments, as well as the private sector.

3.2.3 Goal 3: Prevention, Preparedness, and Protection

To employ a risk-based approach to developing protective efforts designed to improve the overall posture of the sector through targeted risk management decisions and initiatives. The objectives for Goal 3 are to:

- Update prioritization of assets within the ESS on an ongoing basis as determined by the general threat environment and the associated risk, both of which allow for comparison of risks associated with ESS assets to assets in other CIKR Sectors, to support the prioritization of ESS assets in light of specific threat information;

- Assess and prioritize risks to critical ESS functions, including evaluating emerging threats and vulnerabilities, including cyber, and mapping them against the infrastructure to prioritize efforts;

- Tailor protective measures to mitigate sector consequences, vulnerabilities, and threats, in a manner to accommodate the diversity of the ESS;

- Develop and share ESS model practices and protective measures with sector partners; and

- Develop metrics to measure effectiveness of sector CIKR protection efforts and develop a means of gathering the information needed to measure effectiveness that is not unduly burdensome on asset owners and operators or other sector partners.

3.2.4 Goal 4: Sustainability, Resilience, and Reconstitution

To improve the sustainability and resilience of the sector and increase the speed and efficiency of restoration of normal services, levels of security, and economic activity following an incident. The objectives of Goal 4 are to:

- Strengthen all components of an integrated region-wide response and recovery capability;

- Enhance the ability of Federal, State, local, tribal, and territorial governments and the private sector to respond effectively to emergencies resulting from a terrorist attack, natural disaster, or other incidents; and

- Improve and expand effective resource-sharing systems and standards.

This page intentionally blank

Section 4: Activity Progress

ESS activities are guided by the shared motivation to make progress in achieving the sector goals and objectives listed in Section 3. Sector key RMAs range from an information sharing portal; to education, training, and outreach (ETO) programs; to innovative approaches and solutions through leading-edge S&T. Many of the sector activities described in this section are multiyear efforts that can be applied across the sector, while others are specific to a particular sector partner.

4.1 Overview of Key Risk Mitigation Activities

The ESS key RMAs are those activities that have been a priority in CIKR protection and resilience within ESS during the reporting year. The sector's key RMAs encompass the promotion of an information-sharing culture that functions in a decentralized, distributed, and coordinated manner, leveraging existing information-sharing capabilities, first responder preparedness, sector partner training and awareness programs, and other DHS IP programs and initiatives.

This section briefly describes key RMAs, recent significant accomplishments, and their alignment with the sector's goals and objectives.[3]

Key RMA Accomplishments

- *Established an ESS ISWG.*
- *Developed the HSIN-CS-ESS Portal.*
- *FEMA and the LAFD partnered with the Office of Infrastructure Protection to launch a First Responder Preparedness Pilot.*
- *DHS S&T Directorate established the First Responder Coordinating Council and the First Responder Research, Development, Testing & Evaluation Working Group.*
- *Developed Sector Partner Training and Awareness Programs.*

4.1.1 Information-Sharing Activities

ESS created the ISWG in 2009 to enhance the sector's information-sharing capabilities within ES and with other CIKR Sectors and Federal, State, and local partners. The IRWG, a subcommittee of the ISWG, is a team of highly experienced practitioners charged with identifying ESS information requirements and developing the HSIN-CS-ESS portal.

The IRWG serves to identify the requirements for information sharing that protects and ensures the continuity and resilience of the sector. The group is working toward an HSIN portal design and function that is user-friendly and contains relevant content and collaboration tools. The full launch of the portal is expected in 2010.

The ISWG, IRWG, and HSIN-CS-ESS Portal activities support Goal 2, Situational Awareness, to support an information-sharing environment.

[3] Additional information regarding the progress made in the reporting year on these RMAs is provided in Attachment A: RMA Information for the Emergency Services Sector.

4.1.2 Emergency Services Self-Assessment Tool

To facilitate accurate and efficient risk assessment and analysis, sector representatives have identified three general risk assessment layers: (1) facility-specific or fixed assets; (2) specialized ES assets or systems; and (3) multiple systems in a region or multiple regions. As with risk assessment in general, each risk assessment layer has individual aspects of prioritization, yet builds on the other layers, rolling up multiple systems into a regional perspective. Facility risk priorities generally relate to an individual facility (e.g., fire or police stations, 9-1-1 Call Centers, or emergency operations centers). System risk priorities generally relate to the elements that build the system and the entities that rely on and manage the 9-1-1 Call Centers, HAZMAT, or SWAT teams. Regional risk priorities relate to multiple systems and multiple echelons of concern.

An Emergency Services Self-Assessment Tool (ESSAT) enables government and public and private entities to perform risk assessments of fixed assets, systems, regional systems, and critical assets. The tool encourages voluntary and interactive stakeholder involvement and allows for a coordinated effort among sector partners by collecting and sharing common risk gaps, obstacles, and protective measures. The tool benefits individual partners and collective disciplines, and supports sector-wide risk management efforts. An ESSAT Pilot for fixed assets is scheduled to be launched in late 2010.

The ESSAT and RMAs support Goal 3, Prevention, Preparedness, and Protection, to employ a risk-based approach to developing protective efforts designed to improve the overall posture of the sector through targeted risk management decisions and initiatives.

4.1.3 First Responder Readiness Pilot Project

ESS and FEMA National Preparedness Directorate (NPD), working in conjunction with the Center for Homeland Defense and Security (CHDS) Alumni Fellowship Program, seek to improve upon the capability of at-risk public safety organizations such as first responders, emergency management, and public services to better train the individual, family, and organization to prepare themselves and their loved ones in advance of catastrophes. One key component of the initiative includes the development of a Responder and Family Preparedness Technical Assistance Program. The desired result would be an improved ability of first responders to serve their communities following large-scale disasters. A pilot of this project was launched in the spring of 2010.

The project phases include (1) assessment; (2) model development; (3) model implementation; and (4) evaluation. At the writing of this Sector Annual Report, training and outreach are occurring through national conferences, meetings such as the ES Sector Coordinating Council/Government Coordinating Council (SCC/GCC) Joint Meeting, and various individual ESS agencies such as the New York City Fire Department and the Arlington County Fire Department in Arlington, Virginia. The intent is for the ESS to continue to market this program and facilitate ongoing training of all disciplines on this critical aspect of protection and preparedness.

The First Responder Readiness Pilot Project supports Goal 3, Prevention, Preparedness, and Protection, to employ a risk-based approach to developing protective efforts designed to improve the overall posture of the sector through preparedness activities.

4.1.4 DOT/IAFC National Hazardous Materials Fusion Center

The National Hazardous Materials Fusion Center is a joint partnership between the DOT's PHMSA and the IAFC. The purpose of the center is to provide a secure, Web-based network that will facilitate information sharing for emergency responders training for and responding to HAZMAT incidents.

The fusion center provides crucial knowledge for all decision-makers about the transportation and delivery of hazardous materials. It is the first data center of its kind for the first responder community. The Regional Incident Survey Teams (RISTs) are now fully operational in each of five PHMSA regions: southwest, western, central, eastern, and southern. Surveys are currently being conducted nationwide, and information products are being produced.

The fusion center supports Goal, 2 Situational Awareness, to support an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant CIKR information and intelligence about terrorist threats and other hazards, information analysis, and incident reporting.

4.1.5 NSA, Homeland Security Initiatives Training

The NSA, a member of the ES SCC, conducts regular training designed to build technical expertise for its members. Table 4-1 outlines the various DHS-sponsored courses that were presented by the NSA, as well as the number of attendees for each class. In total, the NSA has offered 76 classes with 3,002 total attendees. The total classes and attendance are significantly down from last year due to reduction in budgetary allotments in NSA for these programs.

Table 4-1: NSA Training Courses

Course Title	DHS Course #	Number of Classes	Number of Attendees
Community Awareness	AWR-146	24	1,090
Jail Evacuation	AWR-183	33	1,152
Managing the Event	AWR-184	11	385
First Responder	AWR-198	8	375

The NSA programs support Goal 2, Situational Awareness, to support an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant CIKR information and intelligence about terrorist threats and other hazards, information analysis, and incident reporting.

4.1.6 Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC)

The EMR-ISAC, located at the U.S. Fire Academy (USFA), is another critical outreach program that has the responsibility to disseminate critical infrastructure protection (CIP) and resilience information to ESS leaders and first responders throughout the sector. EMR-ISAC delivers information to more than 30,000 ESS stakeholders. EMR-ISAC delivers products that contain emergent, actionable information regarding threats and vulnerabilities to support effective advanced preparedness, protection, and mitigation activities. Due to the dependencies and interdependencies of the ESS with other sectors, the EMR-ISAC continually strives to foster a cross-sector information-sharing environment by participating in monthly Cross-Sector ISAC meetings and daily conference calls. Additionally, the ES SSA holds weekly conference calls with the DHS Information & Analysis, the ES SCC Vice-Chair, and the EMR-ISAC to update the sector on current events.

The EMR-ISAC is a critical partner in disseminating For Official Use Only (FOUO) documents and other information to lower the sector's risk profile. The EMR-ISAC distributes FOUO alerts and advisories to more than 10,000 vetted leaders, owners, and operators of the sector. Additionally, the ISAC has approximately 40,000 direct subscribers to its weekly INFOGRAM, which provides general information and recommendations for improving CIP and resilience in the ESS. Countless sector-related organizations, as well as State and local fusion centers, distribute the INFOGRAM to their members, which significantly increases the information outreach of the EMR-ISAC.

The ES SSA continues to coordinate with the EMR-ISAC in an ongoing concerted effort to align and coordinate initiatives across the sector and to improve information sharing and connectivity. Initiatives include collaboration through the ESS ISWG, HSIN-CS-ESS, and coordination for future exercises and incident response. As an example of its effectiveness, the EMR-ISAC was instrumental in enhancing the information-sharing processes with the SSA and the ES Sector during the 2009 hurricane season.

The EMR-ISAC supports Goal 2, Situational Awareness, to support an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant CIKR information and intelligence about terrorist threats and other hazards, information analysis, and incident reporting.

4.1.7 CIKR Resource Center

The CIKR Resource Center was established to provide a public-facing, Web-based site that has information on the ESS, including the SSP and Sector Annual Report. This site is hosted on the FEMA/Emergency Management Institute (EMI) Web site and connects to a CIKR Learning Series and other training opportunities. The link to the Web site is located at: http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/index.htm.

The CIKR Resource Center supports Goal 2, Situational Awareness, to support an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant CIKR information and intelligence about terrorist threats and other hazards, information analysis, and incident reporting.

4.1.8 DHS S&T Directorate Virtual USA Project

Virtual USA (vUSA) is a DHS S&T Directorate-funded project to create a cost-effective, nationwide capability to significantly improve real-time information sharing and decision-making during emergencies. Building on the momentum created through Virtual Alabama, emergency management and homeland security representatives from the states of Alabama, Alaska, Florida, Georgia, Idaho, Louisiana, Mississippi, Montana, North Carolina, Oregon, South Carolina, Tennessee, Texas, Virginia, and Washington; FEMA Regions I, IV, VI, and X; and FEMA Headquarters are participating at some level in a vUSA regional interoperable information-sharing pilot throughout the United States.

In 2009, only two States had developed information-sharing platforms, and as a result of vUSA-led efforts, nine stakeholders are engaged in the development of platforms. Some of the practitioners at the State level have begun the process of institutionalizing vUSA through a regional memorandum of agreement, which has been adopted by five States (Alabama, Florida, Mississippi, South Carolina, and Virginia). The White House Open Government Initiative recognized vUSA as a DHS flagship initiative that enables better access to information and collaboration. Developed in partnership with the emergency response community, vUSA improves multijurisdictional interoperability and supports emergency response efforts by ensuring that stakeholders at all levels have immediate access to the information they need to make critical decisions.

ESS has engaged the S&T Directorate in a collaborative effort to integrate the interoperability focus of the vUSA real-time information-sharing platform with the collaborative platform of HSIN-CS-ESS. Working together will ensure that the stakeholders within the sector are informed and have access to information-sharing solutions that meet their needs during both incidents and steady-state operations. The S&T Directorate’s Strategic Resource Group will serve as the national body of subject matter experts that will guide national policy development in support of vUSA.

The vUSA project supports Goal 2, Situational Awareness, to support an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant CIKR information and intelligence about terrorist threats and other hazards, information analysis, and incident reporting.

4.1.9 DHS S&T Directorate First Responder Coordinating Council and First Responders Research, Development, Testing & Evaluation Working Group

The DHS S&T Directorate sponsors the First Responder Integrated Product Team (FR/IPT), FRCC, and the FRWG. They are a forum and advisory group that meet to discuss, analyze, and serve as a mechanism for the coordination of investment, programs technology, research, development, and delivery of technological tools to first responders at the Federal, State, local, tribal and territorial levels.

The FR/IPT, the newest Capstone IPT, was established in early 2009. This Capstone IPT coordinates the identification and prioritization of capability gaps, and the creation of detailed operational requirements of Federal, State, local, tribal and territorial first responders in keeping with an ESS “customer drive, customer focus” process. Identified technology solutions will be designed, tested, and assessed for effectiveness and reliability before they are produced for the first responder community. The FR/IPT managed a portfolio of six projects in 2009 with a budget of nearly $10 million.

The FRCC reviewed S&T’s TechSolutions Program portfolio. The projects on the portfolio are selected to field technologies that meet 80 percent of the operational requirement, in a 12- to 15-month time frame, at a cost commensurate with the project proposal but less than $1 million per project. Goals will be accomplished through rapid prototyping or the identification of existing technologies that satisfy identified requirements.

The FRWG met in March 2010 to address capability gaps for the ESS and made recommendations to the FRCC for the 2010 portfolio. Participants assisted in the vetting of the operational requirements of ongoing first responder S&T projects. The working group assessed capability gaps from four ESS disciplines: Fire and Emergency Services, LE, Emergency Management, and EMS.

The S&T First Responder Coordinating Council and R&D Working Group supports Goal 1, Partnership Engagement, to build a partnership model that enables the sector to effectively sustain a collaborative planning and decision-making culture.

4.1.10 Other DHS IP Protective Programs

DHS PSCD, RRAP led interagency assessment of specific CIKR and regional analysis of the surrounding infrastructure. In 2009, RRAPs conducted in Chicago, New Jersey, New York, North Carolina, and Tennessee resulted in more than $9 million in BZPP grant funding for those areas. The grants are allocated to build terrorism prevention and protection capabilities including planning and equipment acquisition by local first responders.

RRAP supports Goal 4, Sustainability, Resilience, and Reconstitution, to improve the sustainability and resilience of the sector and increase the speed and efficiency of restoration of normal services, levels of security, and economic activity following an incident.

Table 4-2 compares metrics information from 2009 to that of 2010.

Table 4-2: Comparison of Metrics Information, 2009–2010

2009 Metrics Information	2010 Metrics Information
ESS ISWG Developed the ISWG charter and established the working group. This RMA evolved into a key RMA for 2010.	**Information-Sharing Activities** Launched the IRWG as a sub-committee of the ISWG in 2009. The IRWG identified requirements for the HSIN portal design and function that are user-friendly and contain relevant content and collaboration tools to be used across all ESS disciplines. The ESS HSIN portal will go live in September 2010.
ESS Risk Assessment Working Group Developed after last year's workshop with selected practitioners representing four of the five sector disciplines (Public Works was not represented). This RMA evolved into a key RMA (ESSAT) for 2010.	**ESSAT** Initiated the development of the ESSAT that enables government, public and private entities to perform risk assessments of fixed assets, systems, regional systems, and critical assets. This tool is a product of the Risk Assessment Working Group workshop. An ESSAT Pilot for fixed assets is scheduled to be launched in late 2010.
N/A	**First Responder Readiness Pilot Project** Worked in collaboration with FEMA, CHDS, and LAFD to improve the capabilities of first responders through the promotion and implementation of a Responder and Family Preparedness Technical Assistance Program. The implementation phase is projected for September 2010.
National Hazardous Materials Fusion Center Developed through a partnership between PHMSA and IAFC in order to provide a secure, Web-based network to facilitate information sharing for emergency responders training for and responding to HAZMAT incidents.	**DOT/IAFC's National Hazardous Materials Fusion Center** Promoted the use of the Fusion Center throughout the first responder community. This Web-based network facilitates information sharing for emergency responders training for and responding to HAZMAT incidents. RISTs were deployed in 2009; surveys are currently being conducted nationwide.
NSA Homeland Security Initiatives Training Collaborated with the NSA to promote the DHS-sponsored curriculum designed to support the capability and capacity of first responders to prevent, plan for, and response to all-hazards events. This RMA evolved into a key RMA for 2010.	**NSA Homeland Security Initiatives Training** Collaborated with the NSA to promote the DHS-sponsored curriculum designed to support the capability and capacity of first responders to prevent, plan for, and respond to all-hazards events. The training attendance went significantly down from last year due to reduction in budgetary allotments in NSA for these programs.

Table 4-2: (Cont.)

2009 Metrics Information	2010 Metrics Information
N/A	**EMR-ISAC** Coordinated with the EMR-ISAC initiatives across the sector through the ESS ISWG and HSIN-CS-ESS for future exercises and incident response. This partnership was instrumental in enhancing the information-sharing processes with the SSA and the ESS during the 2009 hurricane season.
CIKR Resource Center Wed-based site hosted on the FEMA/EMI Web site.	**CIKR Resource Center** Contributed to the establishment of the Web-based site that holds ESS information including the SSP and Sector Annual Report. No data available to measure user's traffic.
Virtual Alabama Common Operating Picture The State of Alabama provided a secure common operations platform for incident management and emergency response personnel by overlaying important operational data on three-dimensional (3-D) maps. This initiative was the foundation for the development of vUSA.	**DHS S&T Virtual USA Project** Developed in partnership with the emergency response community, vUSA improves multijurisdictional interoperability and supports emergency response efforts by ensuring immediate access to critical information. ESS has engaged the S&T Directorate to integrate the interoperability focus of the vUSA real-time information-sharing platform with the collaborative platform of HSIN-CS-ESS.
N/A	**DHS S&T First Responder Coordinating Council and R&D Working Group** Partnered with the RDT&EWG to address capability gaps for the ESS; the working group serves as a forum and advisory group to develop and deliver technological tools to first responders at the Federal, State, local, tribal and territorial levels.
N/A	**RRAP** Initiated collaboration with PSCD to promote RRAP goals within the ESS. The regional analysis conducted in 2009 resulted in over $9 million in Buffer Zone Protection Program grant funding for those areas.

4.2 Implementation of the NIPP Risk Management Framework

The 2010 ES Sector Annual Report describes the relationships, systems, and methods that sector partners and the SSA use to implement the NIPP risk management framework depicted in Figure 4-1. Development of the ES Sector Annual Report exemplified the collaborative working relationship among sector partners and the SSA that drives the sector's progress in implementing the NIPP risk management framework.

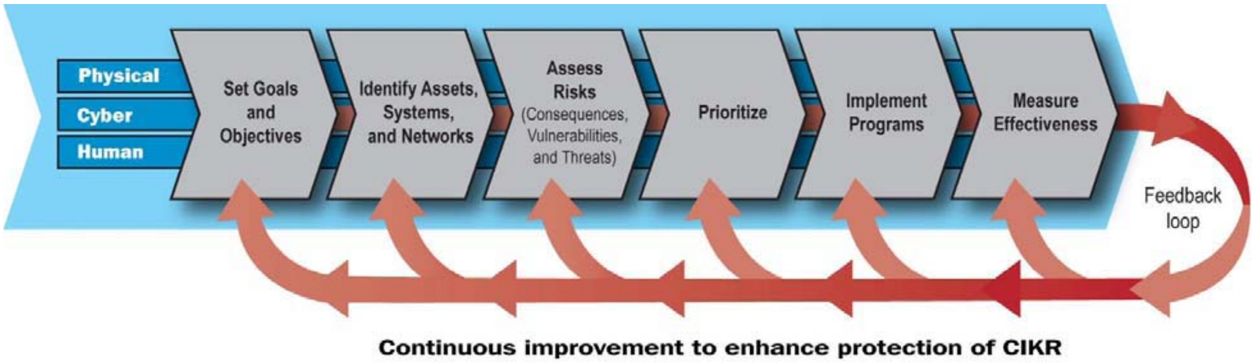
Physical
Cyber
Human
Set Goals and Objectives
Identify Assets, Systems, and Networks
Assess Risks (Consequences, Vulnerabilities, and Threats)
Prioritize
Implement Programs
Measure Effectiveness
Feedback loop
Continuous improvement to enhance protection of CIKR

Figure 4-1: NIPP Risk Management Framework

The 2010 ES Sector Annual Report builds on previous plans but reflects the 2009 NIPP's increased emphasis on resilience, all-hazards preparedness, and cybersecurity. By focusing on security and preparedness from the all-hazards approach, the sector can use prevention, protection, and response capabilities not only to reduce the threat of a terrorist attack on its assets, but also to prevent or mitigate damage in the event of a natural or unintentional manmade disaster. This comprehensive approach strengthens the sector so that it is fully prepared to face the challenges ahead. The SSA, working in conjunction with DHS, other Federal agencies, and additional sector partners, ensures seamless linkage between the NIPP and steady-state protection and incident management activities.

The revised goals and objectives included in this document more clearly reflect the priorities of the sector and represent the sector's view of how best to support the overarching goal of the NIPP to achieve a secure, protected, and resilient ESS. These goals underline the sector's emphasis on protecting the human assets as well as the physical and cyber assets of the sector. Alignment of the sector's priorities with the documented goals and objectives ensures consistent priorities and a common operating picture, which in turn enhances a coordinated approach to infrastructure protection within the ESS.

As stated previously, the ES SSA has reevaluated the sector's discipline categories, defining itself along five broad disciplines: LE, Fire and Emergency Services, Emergency Management, EMS, and Public Works. Supplementing these disciplines and overall sector operations are specialized capabilities specific to the ESS: HAZMAT, S&R, EOD, SWAT, Aviation Units, and PSAPs. The physical, cyber, and human critical infrastructure that support and comprise each ESS discipline and specialized capability define the parameters for information collection and infrastructure identification. These updated disciplines and capabilities enhance the sector's ability to define its assets, collect information, and further develop sector taxonomy, as well as ensure that the various components are best represented in meetings and initiatives falling under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework.

Significant NIPP Risk Management Framework Accomplishments

- *Collaborative development of the 2010 ES SSP.*
- *Sector partners have reevaluated its goals, objectives, and disciplines.*

The SSA has studied and made adjustments to its CIKR taxonomy, closely aligning it with FEMA's NIMS Resource Typing in order to better identify the sector assets. Resource Typing is categorizing, by capability, the resources requested, deployed, and used in incidents. Measurable standards identifying resource capabilities and performance levels serve as the basis for categories. Resource users at all levels use these standards to identify and inventory resources. DHS taxonomy changes are made every two years; the efforts for this process in 2010 included practitioner participation, especially from its newest discipline, Public Works.

To facilitate accurate and efficient risk assessment and analysis, sector representatives have identified three general risk assessment layers:

(1) Facility-specific or fixed assets;
(2) Specialized ES assets or systems; and
(3) Multiple systems in a region or multiple regions.

As with risk assessment in general, each risk assessment layer has individual aspects of prioritization, yet builds on the other layers, rolling up multiple systems into a regional perspective. Facility risk priorities generally relate to an individual facility such as a fire or police station, a 9-1-1 call center, and/or an emergency operations center. System risk priorities generally relate to the elements that build the system and the entities that rely on and manage the 9-1-1 call centers, HAZMAT, or SWAT teams. Regional risk priorities relate to multiple systems and multiple echelons of concern. This updated approach provides valuable information to inform the development of protective programs and the allocation of resources.

Currently, an ESSAT is in development. The tool will enable the ESS to select and define a region's area of response parameters, threat profile, and consequence profile to assess risk for the first of the three layers, facility-specific or fixed assets. The tool will encourage voluntary and interactive stakeholder involvement and allows for a coordinated effort among sector partners by collecting and sharing common risk gaps, obstacles, and protective measures. The tool benefits both individual partners and collective disciplines and supports sector-wide risk management efforts.

4.3 Cybersecurity

Significant Cybersecurity Accomplishments and Initiatives

- *The anticipated conduct of a cyber evaluation of Public Safety Answering Points (PSAP) in 2010.*
- *The formation of an Exercise Working Group.*

Cybersecurity, as defined by the 2009 NIPP, includes prevention of damage to, unauthorized use of, or exploitation of electronic information and communications systems, and the information contained therein to ensure confidentiality, integrity, and availability. The interconnected nature of these cyber systems, combined with their constant availability, increases the cybersecurity risks to the ESS operations and communication systems. Because of the increasing reach and inherent complexity of IT and cyber systems, functions, and activities, cyber issues are a major concern for the sector. Many ESS activities conducted in cyberspace, such as emergency operations communications, database management, biometric activities, telecommunications, and electronic systems (i.e., security systems) are vulnerable to cyber attack. The Internet is widely used by the sector to provide information and receive alerts, warnings, and threats relevant to the sector.

Certain cyber systems are so essential to first responders that their security in any individual facility must be considered in the risk analysis process. Degradation of these systems would significantly raise the overall risk to that facility and the first responder, and seriously impact the ability of ES to carry out its mission. Therefore, ESS included cybersecurity as one element of risk in its 2009/10 Strategic Homeland Infrastructure Risk Analysis (SHIRA) report. As noted in Section 2-Risk, the sector deemed itself most susceptible to the strategic targeting of cyber attacks on business systems, such as the CAD system for the PSAPs and Emergency Communication Centers. As a result, the sector has included the PSAPs as a sector critical element, and they are included in this year’s National Critical Infrastructure Prioritization Program (NCIPP). Over the next year, the sector, along with the PSAP community, will identify specific attributes related to PSAPs, which will further delineate cyber vulnerability gaps.

The nature of the ESS makes broad generalization of cyber system usage difficult. While some similarities exist, each discipline uses cyber systems differently in its daily activities. A lack of standards, combined with variations in organization, diversity of assets, availability of resources, and other factors, create a very diverse and dynamic cyber landscape. The ESS ISWG will strengthen the sector’s ability to identify and prioritize cyber threats, vulnerabilities, and risk and training opportunities. Cybersecurity is a core information-sharing competency, documented in the ISWG Charter. The ISWG also recommends and implements protective measures and provides tools and resources for the sector to conduct inventory assessments and audits of cyber assets and networks.

Recently, ESS identified a practitioner chairperson for the ESS Cyber Advisory Committee. Throughout the year committee participants will be identified and a path forward developed. The ESS acknowledges there are many other groups focusing on creating and ensuring a safe, secure, and resilient cyber environment. The purpose of the Advisory Committee is to determine, prioritize, and mitigate cybersecurity vulnerabilities and risk; assess current resources that can be leveraged for improving the cybersecurity posture of the sector; and provide relevant education and outreach.

A major resource within DHS that provides guidance and assistance to the sector is NCSD, which works collaboratively with public, private, and international entities to secure cyberspace and the Nation’s cyber assets. Through involvement and participation with these programs, the sector is able to leverage the tools, information-sharing forums, and expertise within NCSD. The NCSD Cyber Exercise Program (CEP) improves the Nation’s cyber security readiness, protection, and incident response capabilities through developing, designing, and conducting cyber exercises and workshops at the Federal, State, regional and international level. The Cyber Storm Exercise was one mechanism for the sector to evaluate incident response and coordination interdependencies and capabilities by assessing communications, coordination, and relationships in response to a large-scale cyber incident.

While individual CIKR Sectors are addressing many sector-specific cyber issues, an integrated cross-sector cybersecurity perspective is needed to address the mutual concerns and issues that span numerous sectors. This cross-sector perspective facilitates the sharing of knowledge about various cybersecurity concerns, such as common vulnerabilities and protective measures. In addition, it leverages functional cyber expertise in a comprehensive forum. To meet this need, the DHS Assistant Secretary for Cyber Security and Communications proposed, and the Partnership for Critical Infrastructure Security (PCIS) agreed, to establish a Cross-Sector Cyber Security Working Group (CSCSWG) under the auspices of the CIPAC. The CSCSWG is a public-private collaboration made up of representatives from the 18 CIKR SCCs and GCCs. The CSCSWG serves as a forum to bring government and the private sector together to collaboratively address risk across the CIKR Sectors. Because the ES function is so closely intertwined with the other sectors, the ESS is an active participant in the CSCSWG's monthly meetings. Additionally, the sector has reviewed and contributed to the National Cyber Incident Response Plan, which is in draft phase at the writing of this report.

While involved and participating in cyber-related efforts, the ESS's strength is the ability to inform and disseminate cyber-related alerts and resilience strategies throughout the first responder community. The ESS continues to stay informed about cyber-related risks to the sector through a variety of mechanisms, including the Multi-State Information Sharing and Analysis Center (MS-ISAC), the EMR-ISAC, the U.S. Computer Emergency Readiness Team (US-CERT), and the CSCSWG.

State and local governments started the MS-ISAC, which is a collaborative voluntary effort, in January 2003. Its founders designed the center to facilitate communication regarding cyber and critical infrastructure readiness and response efforts. Coordinated by the New York State Office of Cyber Security and Critical Infrastructure Coordination, the MS-ISAC is recognized by DHS for its proactive role in bringing the States together. The MS-ISAC provides the ESS with a common mechanism for raising the level of cybersecurity readiness and response with the sector, and it provides a central resource for gathering information from the sector regarding cyber threats to critical infrastructure. The MS-ISAC publishes and e-mails daily cyber-related bulletins to ESS constituents. The bulletins also may be delivered via the EMR-ISAC, which has more than 30,000 ESS participants.

In recognition of the potential adverse impact to the sector should its cyber assets and systems be targeted, the ESS participates in many programs designed to identify emergent threats, protect vital systems, and mitigate the impact of a cyber event. Examples of sector cyber programs follow:

- **Control Systems Security Program (CSSP).** The CSSP coordinates activities among Federal, State, local, and tribal governments, as well as control systems owners, operators, and vendors to reduce the likelihood of success of and the severity of impact of a cyber attack against CIKR control systems through RMAs.

- **Critical Infrastructure Protection: Cyber Security Program (CIP CS).** In partnership with public and private sectors, CIP CS helps improve the security of the IT Sector and cyberspace across U.S. CIKR Sectors by facilitating risk reduction through infrastructure identification, vulnerability assessment, and protective measures initiatives.

- **CSCSWG.** The CSCSWG was established to improve cross-sector cybersecurity protection efforts across the Nation's CIKR Sectors by identifying opportunities to improve sector coordination around cybersecurity issues and topics, highlighting cyber dependencies and interdependencies, and sharing government and private sector cybersecurity products and findings.

- **CEP.** CEP improves the Nation's cybersecurity readiness, protection, and incident response capabilities by developing, designing, and conducting cyber exercises and workshops at the Federal, State, regional, and international level. CEP employs scenario-based exercises that focus on risks to the cyber and information technology infrastructure.

- **Software Assurance Program.** The Software Assurance Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development and deployment of trustworthy software products. These activities enable more secure and reliable software that supports the Nation's CIKR.

- **US-CERT.** US-CERT is the U.S. Government's principal cyber watch and warning center. It is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. US-CERT interacts with Federal agencies, industry, the research community, State and local governments, and others to disseminate reasoned and actionable cybersecurity information.

4.4 Partnership

The SCC continues to expand its members and increase its participation in working groups, exercises, and collaboration activities. Activities initiated this year include monthly Sector Extended Meetings, processing clearances, exercise involvement, and collaboration during the declared pandemic of influenza A (H1N1) last summer/fall. The Sector Extended Meetings were initiated by the SCC and intended to facilitate more frequent dialogue between the SCC and the ESS SSA. These meetings serve to share priorities and updates on working group activities and provide any SSA assistance that might be required. An Exercise Working Group, representative of members from the SCC and practitioners, guides the sector's efforts for involvement in National Level Exercise 2010 and 2011. That group developed exercise objectives and participated in various planning conferences, seminars, and tabletop exercises (TTXs).

Significant Partnership Accomplishments and Initiatives

- *The initiation of extended team meetings with SCC leadership.*
- *The formation of an Exercise Working Group.*

Additionally, the sector nominated and processed three SCC members for top-secret clearances and added four new SCC members for secret clearance. Prior to the declaration of a global pandemic of H1N1 by the World Health Organization, the SCC recognized many factors critical to the ability of the sector to respond effectively should this or a future pandemic cause severe illness to a greater numbers of U.S. citizens. As a result, the SCC reached out to the SSA and GCC members, primarily the Health Sector and Office of Health Affairs, to collaborate on specific issues identified by the SCC. Several meetings were held with the SCC and Federal partners that effectively communicated concerns and generated solutions that were shared with the U.S. Department of Health and Human Services (HHS) and the Centers for Disease Control and Prevention (CDC). Additionally, an influenza incident reporting tool was created in collaboration with the SSA/GCC/SCC to facilitate National Infrastructure Coordination Center reporting in HSIN-CS. The sector, as a whole, continues to enhance and support the partnership of the EMR-ISAC.

This year, the ESS GCC members worked to develop a value proposition for the Council and ultimately deliver a signed GCC Charter. The members focused strategically on the future of the Council and its role in enhancing the public-private partnership within ESS. Specifically, the goal is to establish clarity, common understanding, and consensus among members about the ESS GCC value proposition and how the Council needs to operate in order to create and deliver that value proposition. The expected results are that the Council will successfully implement a signed charter that provides a shared vision of purpose for members and a collective declaration of mission and value to partners and stakeholders.

The ESS understands that numerous Federal and other governmental agencies, associations, and practitioner-formed working groups exist to identify sector needs and gaps that generate products, tools, exercises, and information-sharing mechanisms impacting first responders. The ESS believes that ongoing communication and coordination enabled by a broad public-private partnership are critical to the ES SSA's mission to manage its responsibilities for leading the unified effort to manage risk to the sector.

4.5 Owners/Operators

The NIPP partnership model defines owners and operators as those entities responsible for day-to-day operation and investment in a particular asset or system. For ESS, the owners and operators represent multiple distinct disciplines and systems that inherently reside in the public safety arena within State and local government agencies as opposed to private, for-profit businesses. Most notably, much work is underway to incorporate the newest discipline into ESS, which is the Public Works sub-sector.

The SCC identified Public Works practitioners to serve on various working groups such as the Infrastructure Data Taxonomy (IDT) and IRWG. The IDT working group was formed to address technical issues related to the function of the IDT. The ES SSA worked with sector's subject matter experts, FEMA's Incident Management Systems Integration in the National Integration Center, and the American Public Works Association (APWA). The Public Works Subsector/discipline has been added to version 4 of the IDT, and Search and Rescue was moved from a sub-sector to a capability that encompasses multiple disciplines. APWA was an integral partner in providing the content for the Public Works section of the IDT. Additionally, through the IRWG, the Public Works members, assisted by the APWA, are engaged heavily in identifying information requirements for the HSIN-CS-ESS portal and in contributing content for the portal.

The ESS's most important factor is the safety of the first responder, or human asset, the protection of which is almost indistinguishable from the first responder's mission to protect the public. The partnership model from a private sector frame of reference is the protection of "goods and services," whereas in ESS, "goods and services" is defined as saving lives and property. The ESS is a system of prevention, protection, preparedness, response, and recovery elements that forms the Nation's first line of defense for preventing and mitigating risk. Therefore, the partnership activities and programs appropriate to the sector are those that allow for protection of the first responder and their capabilities, as well as maintaining the ability of the response community to engage in its mission during an all-hazard event.

4.6 Education, Training, and Outreach

Education, training, and outreach programs provide the basis for effective emergency preparedness and response, which are designed to empower the responder to effectively manage incidents. ETO activities available to members of the sector include formal educational programs offering associate degree or baccalaureate paramedic education, providing certification programs for a particular specialized skill such as HAZMAT, facilitating on-the-job training opportunities, and attending conferences.

Significant Education, Training, and Outreach Accomplishments

- *Launched a Responder and Family Preparedness Project.*
- *Developed a Who's Who in DHS Emergency Services Sector pamphlet.*

Enhancing awareness of CIKR protection initiatives and building effective partnerships to accomplish a more resilient sector are significant components of the sector's outreach activities. The highly skilled nature of first responders requires formal academic education and competency certification and recertification, in addition to ongoing refresher training in specialized skills and equipment use. As most incidents rarely involve only one discipline, first responders participate in numerous multidisciplinary education and training activities such as exercises that enhance the sector's ability to provide a seamless response through improving interoperability and partnerships.

Additionally, each discipline is represented by an association. Each association hosts a minimum of one annual conference, which enables an exchange of information and sharing of best practices. Due to the size and diversity of the sector, and the multitude of ETO programs available therein, it is not feasible to capture all of the ETO activities within a single document. Rather, this report discusses specific activities that highlight NIPP-related programs in addition to those activities across the CIKR protection and resiliency landscape.

4.6.1 DHS IP Programs

- **ESS Preparedness Brochure.** ESS continues to distribute the tri-fold handout, *Personal Readiness Guide for Responders and their Families, that addresses family preparedness and include*s suggestions for ma*k*ing a kit, a family emergency plan, and a list of Web site resources. First responders are quite skilled at educating the public on preparedness measures, but often neglect their own personal preparedness. Establishing effective personal protective measures for themselves and their families is the first step toward enhancing sector security and resiliency, which ultimately ensures effective emergency response. The brochure is distributed via the EMR-ISAC and is requested by conference organizers to distribute at annual conferences.

- **ESS Pandemic Influenza Preparedness, Response, and Recovery Guide for CIKR.** As discussed in Section 4, this sector-specific planning guideline, developed by the sector (in collaboration with the SCC), is an annex to the *Pandemic Influenza Preparedness, Response, and Recovery Guide for CIKR (CIKR Pandemic Influenza Guide*). The guidelines intend to assist the pandemic planning efforts for entities within the ESS. The annex addresses the major challenges the sector may face and should assess in its pandemic influenza planning within seven key areas of vulnerability. This guideline serves as a key protective measure for the sector, as its guidance allows for owners and operators to ensure there is resilience in the sector, should an influenza pandemic outbreak occur.

- **ESS Resource Training Catalog.** ES SSA is developing the training catalog to capture a variety of training programs and related resources sponsored by the Federal government and private partners that would be of value to first responders. This tool will provide a menu of training opportunities and raise awareness throughout the sector about available sector-wide training.

- **Who's Who in DHS ESS pamphlet.** ESS is developing an information-sharing pamphlet in order to facilitate out*r*each and increase awareness throughout the sector. Written primarily for ES stakeholders, the document clarifies roles and responsibilities, as well as provides high-level descriptions of, and purposes for, the various DHS entities. The *Who's Who in DHS Emergency Services Sector* was scheduled to be published in May 2010.

4.6.2 Responder and Family Preparedness Initiative (Resolve To Be Ready)

As noted in RMA 4.1.3, ESS and FEMA NPD, working in conjunction with the CHDS Alumni Fellowship Program, seek to improve upon the capability of at-risk public safety organizations such as first responders, emergency management, and public services to better train the individual, family and organization to prepare themselves and their loved ones in advance of catastrophes. One key component of the initiative includes the development of a Responder and Family Preparedness Technical Assistance Program. The desired result would be an improved ability of first responders to serve their communities following large-scale disasters.

Development of this initiative began in fall 2009. A pilot component was implemented with the Los Angeles Fire Department in the spring of 2010.

The project phases include: (1) assessment; (2) model development; (3) model implementation; and (4) evaluation. At the writing of this Sector Annual Report, training and outreach are occurring at conferences (NSA, Urban Area Security Initiative [UASI], and InterAgency Board [IAB]), meetings (ESS SCC/GCC Joint Meeting), and various individual ESS agencies such as the New York City Fire Department and the Arlington County Fire Department in Arlington, Virginia. The intent is for the ESS to continue to market this program and facilitate ongoing training of all disciplines on this critical aspect of protection and preparedness.

4.6.3 Improvised Explosive Device (IED) Awareness Training

The ESS works closely with the DHS Office for Bombing Prevention (OBP) as it regularly conducts IED training for first responders across the United States. The courses offered provide information necessary to develop the knowledge and skills required to establish surveillance detection operations to protect CIKR during elevated threat periods. Courses are provided at the awareness level stressing terrorist tactics and attack history, as well as the operational level, which allows participants to practice the methods of detection and surveillance through practical exercises.

4.6.4 InfraGard

The Federal Bureau of Investigation’s (FBI) InfraGard program is an outreach program comprised of businesses; academic institutions; State, local, and tribal law enforcement agencies; and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. The relationship supports information sharing at the national and local levels and fosters an increase in the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime, and other major crime programs. Additionally, it improves interaction and information sharing regarding threats to critical infrastructure, vulnerabilities, and interdependencies; provides members with value-added threat advisories, alerts, and warnings; and offers members a forum for education and training on counterterrorism, counterintelligence, cyber crime, and other related matters. There are currently more than 30,000 people subscribed to InfraGard, of whom approximately 1,000 receive specific ESS updates.

4.6.5 Tabletop/Exercises

ESS has had representatives from the sector participate in National Level Exercise (NLE)-10 exercises including the Recovery Seminar and the IP TTX. It is important to note that the sector as a whole participates in a multitude of exercises at the local, State, and national level, making it difficult to capture all of the activities and the value added from a national perspective. A focus of the ESS Exercise Working Group is to develop a methodology that provides a national perspective of the lessons learns and value-added results of these exercises on the sector as a whole.

4.6.6 Conferences and Speaking Engagements

During the past year, the ESS SSA participated in various conferences to brief practitioners and association executive staff on ESS CIKR protection initiatives to include the National Emergency Numbers Association, NSA, IAB Executive Council, the National Forum on Information Sharing, Fusion Center, APWA, and the UASI. Additionally, the ESS SSA provided a brief regarding Homeland Security Information Program alignment to ESS Infrastructure Data Taxonomy and the use of the data to further define sector attributes and priorities and enable value-added risk analysis at the Homeland Infrastructure Foundation-Level Data (HIFLD) Conference. As a result, the briefings generated significant interest in sector initiatives and helped increase participation in working groups.

4.7 International Coordination

Significant International-Focused Accomplishments

- *Participation in the Blue Water Regional Information-Sharing project.*
- *Participation in the HIFLD working group and Canadian Emergency Management.*

A new program involving ESS and St. Clair County, Wisconsin, is the Blue Water Regional Information-Sharing Platform. This project is multi-phased and occurs over a three-year period beginning with the writing of this Sector Annual Report and culminating in 2013. The Blue Water Regional Information-Sharing Platform is designed to improve the capacity and effectiveness of law enforcement and emergency response capabilities in St. Clair County and along the Canadian border. The ultimate goal is to enhance cross-border communications and asset coordination for emergency response operations by leveraging existing investments, while providing new technologies that address remaining communications gaps. This is a collaborative project as it expands upon the current “Virtual City” pilot project being developed for St. Clair County by the S&T Directorate and Space and Naval Warfare Systems Center Atlantic, and will allow St. Clair County to overcome interoperability gaps through the deployment of multiband radio systems, new data and video sharing tools, a shared data framework to permit better geospatial data fusion, and more timely warning to the public.

Outcomes to be achieved include:

- Establish reliable and routine direct cross-border voice communications;
- Create a shared data framework for geospatial integration and asset coordination;
- Use video integration as a tool to support cross-border emergency response; and,

- Invest in select technologies and platforms needed to monitor border activity and support security operations.

Metrics applied for the first year include the following:

- **Interoperable Voice Communications.**
  - Frequency/radio facility mapping via the Communication Assets Survey and Mapping Toolset, 9/2010–1/2011.
  - Life-Cycle Management Analysis and Assessment for next-generation, software-defined multiband radio integration, 12/2010–3/2011.

- **Geospatial Integration.**
  - Inventory of C2 requirements and information exchange use case development, 9/2010–3/2011.
  - Inventory of network assets, applications, and technologies that serve as "endpoints" for information exchange, 9/2010–3/2011.

- **Video Surveillance System Integration.**
  - Inventory, 9/2010–3/1/2011.
  - Define governance, 9/2010–3/2011.

As a member of the HIFLD Working Group, the ESS is currently engaging Canadian Emergency Management. The engagement is designed to identify collaborative relationships and opportunities for mutual RMAs in relationship to first responder protection. Such activities include establishing protocols for mutual assistance and support and developing mechanisms to facilitate information sharing in order to prevent, protect against, and respond to cross-border events. The St. Clair project cited above is directly related to work resulting from this initiative.

The HIFLD Working Group is a coalition of Federal, State, and local government organizations and supporting private industry partners who are involved with geospatial issues related to Homeland Defense, Homeland Security, Civil Support, and Emergency Preparedness and Response. Canadian representation is included in this group. HIFLD members share the goal of identifying and facilitating acquisition of authoritative homeland infrastructure geospatial data for common use by the Homeland Defense and Homeland Security communities. The group also promotes domestic infrastructure geospatial information sharing, protection, collaboration, and knowledge management.

The HIFLD Working Group is co-sponsored by the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (OASD HD&ASA); DHS Office of Infrastructure Protection; Geospatial-Intelligence Agency Office of Americas; and the U.S. Geological Survey (USGS) National Geospatial Program Office.

Additionally, it is important to note that many of the organizations comprising ESS are international organizations (i.e., IAFC, International Association of Chiefs of Police, and International Association of Emergency Managers). These same associations represent the Executive Council of the ESS SCC.

4.8 Other Programs and Activities

4.8.1 Personal Identity Verification-Interoperable (PIV-I)/First Responder Authentication Credential Technology Transition Working Group (FRAC TTWG)

The ESS has joined the Personal Identity Verification-Interoperable (PIV-I)/First Responder Authentication Credential (FRAC) Technology Transition Working Group (TTWG), which is led through a partnership with FEMA Office of the National Capital Region Coordination (NCRC), FEMA Office of Security, and the Command, Control, and Interoperability (CCI) Division within DHS S&T Directorate.

Other Significant Programs and Activities

- *Formation of the TTWG.*
- *Partnership with Commercial Mobile Alert Service (CMAS).*

Local and State emergency response officials must be able to collaborate and assist one another during a disaster to ensure the public's safety. In order for this to happen, many identity management challenges must be overcome. In the past, physical access to sites would be granted based on personal judgment, rather than on hard identity data. Logical access to computer systems required only a username and password. Today, Federal Information Processing Standard (FIPS) 201, Office of Management and Budget (OMB) memorandum M-05-24, and other White House guidance specify that access to all Federal computer systems require secure forms of identification based on smart card technology and identity-proofing procedures. Local, State, Federal, and private stakeholders need to collaborate to solve these identity management challenges. The working group is focused on exploring PIV-1 credentials as the standard that enables interoperability between local and State emergency response officials. The ESS will assist FEMA NCRC in strengthening stakeholder participation through education, training, and outreach and over the next year will be a conduit for future piloting with first responders and the private sector.

4.8.2 Commercial Mobile Alert Service

FEMA administers the alert and warning system for DHS in partnership with the S&T Directorate, the Federal Communications Commission, National Oceanic and Atmospheric Administration (NOAA), the U.S. Department of Justice's Office of Justice Programs for AMBER Alerts, the Joint Interoperability Test Command, and other Federal partners. The Integrated Public Alert Warning System (IPAWS) Program Management Office is also engaged with the FEMA Regions in order to coordinate requirements of local, regional, and State emergency managers.

In conjunction with the National IPAWS initiative the Commercial Mobile Alert Service (CMAS) Research, Development, Testing & Evaluation (RDT&E) Program is led by the CCI Division of the S&T Directorate within DHS. The development and implementation of CMAS is a coordinated effort that involves working with all levels of the emergency management community, other Federal partners, and commercial industry. The participation of these stakeholders is vital to ensure that CMAS efforts address the needs of the community. Over the past year and in collaboration with the ESS, the CMAS RDT&E Program has engaged in the following stakeholder activities.

- The CMAS Forum was held on July 30, 2009, at the Hyatt Regency Crystal City in Arlington, Virginia. The purpose of the CMAS Forum was to convene the alerts and warnings community to address critical issues and determine next steps for the Program.

- The National Public Warning Working Group (NPWWG) was formed following the CMAS Forum, during which participants identified and signed up for Action Teams and prioritized issues that need to be addressed by the RDT&E Program. The activities of the NPWWG are implemented through the work of these Action Teams.

- The launch of the Action Teams aligns closely with CMAS RDT&E Program efforts. The Alert Origination Action Team was the first of the CMAS Action Teams to launch in February 2010. As the first component of the CMAS reference architecture, it seemed natural to begin by focusing on the critical issues in the area of origination of an alert. The Action Team held its first meeting on February 16, 2010, and developed a charter that outlines procedures for moving forward. The second Alert Origination Action Team meeting was held on April 21, 2010, and focused on identifying and documenting gaps and questions in regard to the origination of a CMAS alert message.

- The CMAS Forum Web site launched in September 2009 to provide follow-up information from the CMAS Forum to attendees, disseminate background information to new stakeholders, and provide a forum for participants to sign up for Document Review Teams. It is a public Web site and communication tool designed to disseminate CMAS-related information to stakeholders. Moving forward, the Web site also will serve as a place where stakeholders can download resources and find updates on the CMAS Action Teams.

- The CMAS RDT&E Program partnered with the National Academy of Sciences to host a Public Response Workshop April 13–14, 2010. The two-day workshop acted as a forum to bring together experts – researchers, academics, industry representatives, and practitioners – in the field of public alerts and warnings, specifically in the area of public response to mobile alerts. Keynote speakers and panelists presented current research and knowledge on public response to alert and warning topics, such as communicating with at-risk populations, and public education and training. The workshop resulted in an understanding of the current state of research regarding public response to alerts and warnings as well as an understanding of the gaps in current research.

The American public and the first responder are the ESS's greatest stakeholders. As with any disaster situation, it is the strength and resilience of the American people that ameliorates the initial devastating impact of a disaster, regardless of its origin. ESS continues to support the FEMA IPAWS Program Management Office and the CMAS RDT&E Program to ensure, through the many forums and venues available, that the needs and concerns of the public are known and integrated into the next generation of alert and warning.

Section 5: R&D and Other CIKR Protection and Resilience Mission Needs

This past year, the DHS S&T Directorate established the FRWG as an entity that can act as a clearinghouse for the technology requirements of the 2.4 million first responders in the United States. In addition, the FRWG is a vehicle for the coordination of research and development, and delivery of technological tools to first responders at the Federal, State, local, tribal, and territorial levels. The FRWG works in partnership with ESS and is composed of representatives from four of the five sector disciplines: LE, Fire and Emergency Services, EMS, and Emergency Management.

The mission of FRWG is to identify and prioritize significant first-responder needs and capability gaps, assist with the establishment of detailed operational requirements for proposed technology solutions, and assist in the development and periodic evaluation of a transparent and flexible mechanism for the DHS S&T priority of effort and focus for first-responder technologies. The FRWG Chair acts as the primary conduit for information to and from DHS S&T and, in conjunction with members, will inform and advise DHS IAB and S&T leaders as to their needs. It is important to note that a co-chair of the FRWG is on the Executive Council of the ES SCC and provides that link back to the sector.

The IAB is a voluntary, collaborative panel of emergency preparedness and response practitioners from a wide array of professional disciplines that represent all levels of government and the voluntary sector. The IAB seeks to be the source for emergency responder insight about any policy, doctrine, practice, standard, research and development program, or training and exercise program that affects interoperability, compatibility, and standardization.

The IAB is a trusted agent that represents the interests of first responders and is a valid repository of field perspective, operational knowledge, and technical expertise. Based on direct field experience, IAB members advocate for and assist the development and implementation of performance criteria; standards; test protocols; and technical, operating, and training requirements for all-hazards incident response equipment with a special emphasis on chemical, biological, radiological, nuclear, and explosive (CBRNE) issues. Members of the IAB R&D committee also participate on the FRWG.

The FRWG met in March 2010 to review capability gaps identified during the September 2009 FRWG meeting and match them to ongoing S&T projects. In addition, the group solicited direct feedback, both positive and negative, on ongoing technology projects with a special emphasis being placed on ensuring the accuracy of the operational capability gaps. In some cases, there was a high level of congruency between the technology project and the capability gap. In other cases, greater clarity between the first responders and the project managers was still required.

As a result of the candid feedback, the group refined the 2010 operational capability gaps as listed below:

- **Fire Service.**
  - 3-D locator for first responders;
  - Satellite-based remote location/communication; and
  - Advanced portable forced entry device.

- **Law Enforcement.**
  - Vehicle disablement (revised);
  - Explosive detection device; and
  - Integration of means and methods of analysis of suspects.

- **Emergency Management.**
  - Incident modeling capability; and
  - Crisis management information software.

- **EMS.**
  - Virtual simulators;
  - Renewable/alternative one-size-fits-all power source;
  - Integrated data collection, records management, reliable and consistent information sharing capability; and
  - Red card identification.

On an annual basis, the IAB surveys its membership to assess R&D items based on the following criteria: urgent need, life safety, mission performance, incident management, compatibility/interoperability, use by multiple responder disciplines, and use in day-to-day operations as well as major incidents. In comparing the FRWG-identified operational capability gaps with those found in the IAB survey, the ESS found a consistent cross-referencing of gaps.[4]

It is important to note that there are 13 Integrated Product Teams (IPTs) within S&T that span the gamut of DHS, all of which contain R&D projects that impact the sector. The intent of the ESS, through collaboration with the FRWG and the IAB, is to continually strive to provide a comprehensive review of the high-value R&D first responder activities for the sector.

5.1 New R&D and Modeling, Simulation, and Analysis (MS&A) Capability Gaps/Mission Needs

As a result of a March 2010 meeting, the FRWG identified five new projects for 2010, which are listed in Table 5-1. These gaps are considered by the group to be high priority but are not listed in any particular order of importance.

[4] Attachment C lists IAB priorities.

Table 5-1: ESS R&D Capability Gaps/Mission Needs Statement

Question	Response
Statement Tracking Number	2010-001-ESS
Proposed Title of Mission Need	**Personal Alert and Tracking Systems (PATS)**
2010 Priority Number	N/A
Is this submission an MS&A Mission Need?	No
Goal/Objective/Driver to which Mission Need Responds	ESS Goal: Sustainability, Resilience, and Reconstruction
Theme	▪ Detection and sensor systems; ▪ Protection and prevention; and ▪ Response, recovery, and reconstitution.
Sector Risk	As primary responders, ESS personnel would be among the first victims and would suffer subsequent exposure as they made their initial assessments.
Gaps of Existing Capabilities	▪ Current personal alert systems cannot pinpoint the locations of the firefighter. ▪ Existing devices lack sensors to identify hazards that are not immediately recognized such as carbon monoxide or a fallen live wire ▪ Existing GPS systems do not function well in situations where the GPS signal is weak or nonexistent. ▪ Lack of suitable technology currently exists. Other technologies are not robust for field deployment.
Description of Operational Requirement	▪ The goal is to develop an accountability system that provides location, communication, and alerting capability for responding to wildfires and remote location operations. ▪ The technology will be used to assist firefighters who work in extreme environments, such as the wilderness where they may become disoriented and/or disabled.
Description of Secure Implementation	▪ The output of the system will be interoperability with other situational awareness equipment currently available to emergency managers. The user interface will be intuitive and graphical with the ability to plot the location of first responders and provide up-to-date status information on every firefighter. ▪ The proposed system will have the ability to operate reliably in harsh environments of high temperature, smoke, and particulate matter; must have the ability to span a vast range; must operate over varied terrain, including plains and mountains that can obstruct radio signals; must be lightweight, easy to use, and not interfere with typical activities of a firefighter; and must be able to detect common ancillary dangers associated with wildfires.
Identification of the End User	Firefighters and other emergency response personnel responding to wildfires or other large fires.
Identification of Existing Related Capabilities or Technology	▪ The existing GLANSER program will be leveraged to develop an early solution to meet the 2-D tracking needs. ▪ Technologies and equipment from NASA’s jet propulsion laboratory projects.
Cybersecurity Implications	▪ This technology does not pose a significant cybersecurity risk to the sector.

Table 5-1: (Cont.)

Question	Response
Statement Tracking Number	2010-002-ESS
Proposed Title of Mission Need	**Ambulance Design Safety Standards**
2010 Priority Number	N/A
Is this submission a MS&A Mission Need?	N/A
Goal/Objective/Driver to which Mission Need Responds	ESS Goal: Prevention, Preparedness, Protection ESS Goal: Sustainability, Resilience, and Reconstruction
Theme	▪ Protection and prevention; and ▪ Advanced infrastructure architectures and system designs.
Sector Risk	The successful completion of this project and design implementation by ambulance manufacturers can significantly reduce ambulance crash-related injuries and deaths. (There were 91 EMS deaths in 2008, half of which were from ambulance mishaps.)
Gaps of Existing Capabilities	There is no uniform ambulance standard for interior design and construction based on scientific data, and currently the interior of an ambulance can be very dangerous during an accident.
Description of Operational Requirement	▪ The goal is to develop uniform standards that address safe construction and design of ambulances to reduce accidents and injuries to EMS and patients while in transit; and ▪ The technical capability will be used to build/retrofit ambulances with greater safety features.
Description of Secure Implementation	The standard will address ambulance crashworthiness, stability, and safety systems in the passenger compartment (including restraints, interior arrangements, equipment retention and tie-downs), human safety interface for ambulance passenger compartment design and layout, and metrics for assessing success of design interventions.
Identification of the End User	Emergency medical technicians and patients.
Identification of Existing Related Capabilities or Technology	The new standard may utilize standards from organizations such as National Institute for Occupational Safety and Health and the National Institute of Standards and Technology.
Cybersecurity Implications	This technology does not pose a significant cybersecurity risk to the sector.

Table 5-1: (Cont.)

Question	Response
Statement Tracking Number	2010-003-ESS
Proposed Title of Mission Need	**Data Integration and Interoperability**
2010 Priority Number	N/A
Is this submission a (MS&A) Mission Need?	Yes
Goal/Objective/Driver to which Mission Need Responds	ESS Goal: Situational Awareness ESS Goal: Prevention, Preparedness, and Protection ESS Goal: Sustainability, Resilience, and Reconstitution
Theme	▪ Protection and prevention; ▪ Advanced infrastructure architectures and systems design; ▪ Analysis and decision support systems; and ▪ Response, recovery, and reconstitution.
Sector Risk	Sector is susceptible to strategic targeting of cyber attacks on business systems such as the Computer-Aided Dispatch (CAD) system and other interoperable communication systems.
Gaps of Existing Capabilities	▪ Often several jurisdictions within a single region or county have different operating platforms that are not compatible and do not communicate with each other; and ▪ Currently communicating across different platforms is limited related to exchange of information and conversion of various dynamic file formats.
Description of Operational Requirement	▪ The goal is to develop the ability for multiple organizations to jointly manage personnel; direct equipment; and seamlessly communicate, gather, store, redistribute, and secure any mission-critical information needed by incident commanders and emergency responders during an emergency situation. ▪ The project provides a middleware framework based on open-architecture standards that allow multiple organizations and information technology tools to seamlessly communicate, gather, store, redistribute, and secure mission-critical information needed by incident commanders and emergency responders during an emergency situation. ▪ The device must have the ability to interface with other systems. ▪ The key characteristic of this project is interoperability. The device will enable various operating platforms used by multiple agencies and departments to share information and communicate with each other.
Description of Secure Implementation	▪ An open-source Dynamic File Converter software tool and accompanying best practices document will be developed that will enable real-time seamless data integration and interoperability among GIS systems that support emergency response; ▪ All stakeholders will have the ability to communicate and share necessary resources effectively and efficiently; and ▪ Software solutions will be transitioned directly to those who need it via an open-source development strategy, enabling its use in multiple systems.
Identification of the End User	Emergency managers, incident commanders, and emergency response personnel.

Table 5-1: (Cont.)

Question	Response
Identification of Existing Related Capabilities or Technology	Gap analysis of current file conversion solutions is required.
Cybersecurity Implications	Sector is susceptible to strategic targeting of cyber attacks on business systems such as the CAD system and other interoperable communication systems.

Table 5-1: (Cont.)

Question	Response
Statement Tracking Number	2010-004-ESS
Proposed Title of Mission Need	**Alert and Warning System**
2010 Priority Number	N/A
Is this submission a MS&A Mission Need?	Yes
Goal/Objective/Driver to which Mission Need Responds	ESS Goal: Situational Awareness ESS Goal: Prevention, Preparedness, and Protection
Theme	▪ Protection and prevention; ▪ New and emerging threats and vulnerabilities; and ▪ Human and social issues.
Sector Risk	An efficient alert/warning system will give emergency managers, first responders, and alert originators a greater ability to process and send emergency alerts to the American public to save lives and protect property.
Gaps of Existing Capabilities	The current system does not provide emergency managers, first responders, and alert originators with the ability to process and send emergency alerts to the public.
Description of Operational Requirement	▪ The system must address both technical and training considerations. ▪ The system must develop a strategy that incorporates social networking and remote-access features for selective notification and single-point triggering of other alert forms. ▪ The capability will be used to alert citizens from all-hazards emergency situations such as weather-related floods, hurricanes, tornados, terrorism, and active shooter scenarios. ▪ There must be an integrated interface with CMAS products.
Description of Secure Implementation	▪ The system is to incorporate social networking systems and feature development of Web-based systems that allow for remote access from multiple locations, identification of security risks for online applications, configuration of tools and network security, and development of a feature which allows the responder to choose the medium through which an alert message is communicated to the public. ▪ An efficient Federal emergency alert system will be implemented that meets the stated needs of the end users.
Identification of the End User	Emergency managers, alert originators, and first responders.
Identification of Existing Related Capabilities or Technology	This ORD is complementary to, but not directly addressed by, current CCI efforts for IPAWS and the CMAS.
Cybersecurity Implications	Sector is susceptible to strategic targeting of cyber attacks on business systems such as the CAD system and other interoperable communication systems.

Table 5-1: (Cont.)

Question	Response
Statement Tracking Number	2010-005-ESS
Proposed Title of Mission Need	**Field Biometric and Credential Identification Capability**
2010 Priority Number	N/A
Is this submission a MS&A Mission Need?	No
Goal/Objective/Driver to which Mission Need Responds	ESS Goal: Prevention, Preparedness, and Protection ESS Goal: Sustainability, Resilience, and Reconstitution Develop mobile biometric and credential reading device for first responders in the field.
Theme	▪ Protection and prevention system; ▪ Entry and access portals; and ▪ Response, recovery, and reconstitution.
Sector Risk	Improves officer safety with the ability to identify dangerous people in near real time.
Gaps of Existing Capabilities	▪ Currently, a standardized mobile, biometric credential-validation device is not available across Federal, State, and local jurisdictions. ▪ This tool will increase efficiency by allowing officers to conduct identity checks on the streets rather than at the patrol station.
Description of Operational Requirement	▪ The project will produce a lightweight and rugged, mobile four-finger biometric and credential validation tool that will be capable of collection, storage, image-quality assessment, wireless transmission of biometric data, receipt, and display that provides biometric matching results. ▪ The device may be used by law enforcement during a traffic stop or other situation in which a person's credentials require validation. It will be used for both planned and unplanned events. The required information is captured when a person places four fingers on the device. ▪ The finger print module hardware will be integrated into a multimodal device that will include off-the-shelf modular technologies. ▪ Key characteristics of the device are that it is easy to use, compact, lightweight, and has the ability to operate in a variety of conditions including offshore and remote land locations.
Description of Secure Implementation	▪ The project requires interoperability between local, State, and Federal levels. ▪ The project provides the ability for rapid and secure identification standards for responder access to disaster sites, thus reducing vulnerability for the sector. ▪ The project will produce a lightweight and rugged, mobile four-finger biometric and credential validation tool that will be capable of collection, storage, image-quality assessment, wireless transmission of biometric data, receipt and display that provides biometric matching results.
Identification of the End User	Field law enforcement officers.
Identification of Existing Related Capabilities or Technology	Enables mobile biometric and credential reading capabilities for officers in the field.

Table 5-1: (Cont.)

Question	Response
Cybersecurity Implications	This technology does not pose a significant cybersecurity risk to the sector.

5.2 Progress

Last year, the sector reported on the 2008 Capability Gaps and Mission Needs. As discussed earlier in this section, the FRWG reviewed all identified capability gaps, which included 2008 and 2009. After an extensive review, the FRWG determined the current 2009 and projected start projects for 2010. The status of the 2008 gaps submission is outlined in Table 5-2. As noted, these gaps have either been referred or considered a non-material project that cannot be achieved through R&D.

Table 5-2: Progress on 2008 Capability Gap/Mission Needs

Statement Tracking Number	2008-001-Emergency Services
Requirement Title	**Occupational Safety and Health Research.** The National Occupational Research Agenda, National Public Safety Sub-Sector agenda for Occupational Safety and Health Research and Practice identified significant data gaps for occupational illnesses and injuries among public safety workers. A strategic approach for improving occupational safety and health research is needed to improve the resiliency of human elements of the ESS. Improvements will enable better staffing of public safety workers during day-to-day and disaster response activities, increasing the reliability of public safety workers and thus improving ESS resiliency.
Action	This gap was previously submitted to R&D. It was determined that it requires a non-material solution that cannot be achieved through R&D.
Status	Closed.

Statement Tracking Number	2008-002-Emergency Services
Requirement Title	**Simulating ESS Response and Recovery for Pandemic Influenza.** Computational modeling of ESS response and recovery from pandemic influenza will improve ESS preparedness for an influenza pandemic and other biological threats. Modeling will allow ESS leadership to better understand the potential or likely impact of pandemic influenza on worker illness and absenteeism, the varying effectiveness of ESS workforce protection measures, and the role of ESS in community mitigation strategies.
Action	This gap was submitted to National Institute for Hometown Security.
Status	The University of Louisville has completed its first year of research as part of a three-year project. Closed.

Table 5-2: (Cont.)

Statement Tracking Number	2008-003-Emergency Services
Requirement Title	**First Responder CBRNE Equipment Standards.** Refinement of first responder equipment standards is needed to establish minimum performance and interoperability requirements for CBRNE equipment utilized by local, State, and Federal first responders. Such standards, and the associated requirements and test protocols, serve multiple purposes including: (1) establishing baseline capabilities and limitations for currently available equipment; (2) guiding production and technological developments by manufacturers and designers; and (3) guiding equipment procurement decisions by the public safety and health communities. Because first responders have varied functional and ergonomic requirements for personal protective equipment, a "one-size-fits-all" approach is not appropriate.
Action	This gap was previously submitted to R&D. It was determined that it requires a non-material solution that cannot be achieved through R&D.
Status	Closed.

Statement Tracking Number	2008-004-Emergency Services
Requirement Title	**Equipment Positioning Modeling.** The ESS requires the development of an approach and/or software to assist Federal, State, and local emergency managers and responders with preplanning regional distribution of resources and equipment to optimize resources in the event of a disaster.
Action	This project was submitted to Incident Management IPT but has not moved forward.
Status	Closed: Rolled into current PATS initiative.

Statement Tracking Number	2008-005- Emergency Services
Requirement Title	**Enhanced Training Modules.** The ESS requires development of model training scenarios that effectively apply simulation and analysis. Quality in ES education is assured by consistent scopes of practice, education standards, accreditation of education programs, standardized testing and certification, and licensure and credentialing where appropriate.
Action	No action has been taken to date.
Status	This need is referred back to the originator for further scoping and specificity.

5.3 Other Mission Needs

For the 2010 Sector Annual Report reporting period, there are no “other mission needs” to report. The mission needs identified for 2010 can be achieved through R&D.

5.4 Other Mission Needs – Progress and Updates

Other mission needs are summarized in Attachment B to include the total list of S&T Capability Gaps. Attachment C lists the 2009 priority needs identified in the IAB survey discussed earlier in this section.

This page intentionally blank

Section 6: Funding of CIKR Programs and Activities

This section provides available funding information for the ES SSA, located within the SSA Executive Management Office. The ES SSA oversees the implementation of the ES SSP. However, it is important to note that many other Federal agencies and their components have made significant investments in programs to secure the ESS. Specific funding amounts for these programs are not available.

6.1 Planned Agency Investments

Table 6-1 lists investment totals for all programmatic activities allotted to the ES SSA.

Table 6-1: ESS and Agency Investments

Sector:	Emergency Services						
Agency:	DHS						
					Budget ($ in millions)		
Program/ Investment Title	Priorities Addressed	Program/Investment Description: How Program/Investment Supports CIKR Protection	OMB Account	Included in the HSDB?[a]	FY 2010 Request	FY 2010 Enacted	FY 2011 Request (est.)
ES SSA Program Support	Goals 1–6	Implementation of NIPP within ESS			2.957	2.957[b]	4.589[b]
Agency Total:					2.957	2.957	4.589

[a] HSDB = Homeland Security Database; FY = fiscal year.

[b] Includes Federal employees' salaries.

This page intentionally blank

Section 7: Sector CIKR Challenges and Path Forward

The challenges of the ESS arise because of its diversity. The sector is composed largely of State and local governmental agencies, not-for-profit and for-profit corporations, multiple disciplines, and numerous specialized capabilities. The sector is in a unique position of being both the "protector" and the "protected," with a dual mission to protect the public and itself. As the ESS continues to evaluate and embrace resiliency as it relates to the sector, the lines between its dual protection missions will not be as clear. It is very difficult for the sector to separate itself from "response" while conducting its role of infrastructure protection.

7.1 Summary of Sector Challenges

In 2010, ESS partners present the following list of significant challenges for the sector:

- Incorporating cross-sector information sharing and the sharing of Fusion Center information into ESS information-sharing activities;

- Continuing development of a risk management framework that includes the assessment of specialized capabilities, which places more emphasis on the human element as well as the supporting systems and networks; and

- Fostering a true ES collaboration across the sector, across all 18 CIKR Sectors, across all Federal agencies, and across the Nation.

7.2 Path Forward to Address Challenges

The sector will continue to focus on protecting the responders as well as protecting specialized capabilities, both the physical and cyber components. The SSA will build on its relationships and activities with CIKR partners to ensure that the sector has an ability to respond, thus ensuring a large aspect of resiliency for the sector.

By reviewing its activities and combining efforts to reduce costs, increase transparency, streamline processes, and eliminate duplication, the sector will be enhanced. Strong relationships between the SCC, GCC, and other sector partners are essential as the sector continues to develop programs, tools, and resources that reflect responder needs. The use of conference calls and Web-based training and meetings, minimizing print publications, and combining activities when possible will help to reduce costs.

The full launch of the HSIN-CS-ESS portal is expected in 2010. The portal will not only increase sector information sharing, but increase transparency. An ESSAT pilot for fixed assets, scheduled to be launched in late 2010, will help the sector continue to develop its risk management framework. Practitioner-based working groups will continue to lead the way by providing insight on information sharing, first-responder preparedness, research and development, exercises, and cybersecurity. Working group participation allows for more effective collaboration and a broadened network down to the ground-level assets of the sector.

As the sector matures, sector participation is expected to increase and expand. Increased sector member involvement is necessary in order to drive focused and meaningful protection and resiliency activities, measure activity effectiveness and progress, and address emerging challenges that the sector will face tomorrow.

Acronym List

3-D	three-dimensional
APWA	American Public Works Association
BZPP	Buffer Zone Protection Program
CAD	Computer-Aided Dispatch
CBRNE	chemical, biological, radiological, nuclear, and explosive
CCI	Command, Control, and Interoperability (DHS S&T)
CDC	Centers for Disease Control and Prevention
CEP	Cyber Exercise Program
CHDS	Center for Homeland Defense and Security
CIKR	critical infrastructure and key resources
CIP	critical infrastructure protection
CIP-CS	Critical Infrastructure Protection – Cyber Security Program
CIPAC	Critical Infrastructure Partnership Advisory Council
CMAS	Commercial Mobile Alert Service
CSCSWG	Cross-Sector Cyber Security Working Group
CSSP	Control Systems Security Program
DHS	U.S. Department of Homeland Security
DOT	U.S. Department of Transportation
EMAC	Emergency Management Assistance Compact
EMI	Emergency Management Institute
EMR-ISAC	Emergency Management and Response – Information Sharing and Analysis Center
EMS	emergency medical services
EOD	Explosive Ordnance Disposal
ES	Emergency Services
ESS	Emergency Services Sector
ESSAT	Emergency Services Self-Assessment Tool
ETO	education, training, and outreach
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency (DHS)
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
FR/IPT	First Responder Integrated Product Team
FRAC	First Responder Authentication Credential
FRCC	First Responder Coordinating Council
FRWG	First Responder Research, Development, Testing & Evaluation Working Group
FRTC	First Responder Technology Council

FY	fiscal year
GCC	Government Coordinating Council
HAZMAT	Hazardous Materials
HD	Homeland Defense
HD&ASA	Homeland Defense and Americas' Security Affairs
HHS	U.S. Department of Health and Human Services
HIFLD	Homeland Infrastructure Foundation-Level Data
HSDB	Homeland Security Database
HSIN-CS-ESS	Homeland Security Information Network-Critical Sectors-Emergency Services
HSPD	Homeland Security Presidential Directive
IAB	InterAgency Board
IAFC	International Association of Fire Chiefs
IDT	Infrastructure Data Taxonomy
IED	improvised explosive device
IP	Office of Infrastructure Protection
IPAWS	Integrated Public Alert Warning System
IPT	Integrated Product Team
IRWG	Information Requirements Working Group
ISAC	Information Sharing and Analysis Center
ISWG	Information-Sharing Working Group
IT	information technology
LAFD	Los Angeles Fire Department
LE	law enforcement
MAA	Mutual Aid Agreement
MS-ISAC	Multi-State Information Sharing and Analysis Center
MS&A	modeling, simulation, and analysis
NCIPP	National Critical Infrastructure Prioritization Program
NCRC	National Capital Region Coordination
NCSD	National Cyber Security Division
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NOAA	National Oceanic and Atmosphere Association
NPD	National Preparedness Directorate
NPWWG	National Public Warning Working Group
NLE	national-level exercise
NSA	National Sheriffs' Association
OASD	Office of the Assistant Secretary of Defense
OBP	Office for Bombing Prevention

OMB	Office of Management and Budget
PATS	Personal Alert and Tracking System
PCIS	Partnership for Critical Infrastructure Security
PHMSA	Pipeline and Hazardous Materials Safety Administration (DOT)
PIV-I	Personal Identity Verification-Interoperable
PSAP	Public Safety Answering Point
PSCD	Protective Security Coordination Division
R&D	research and development
RDT&E	Research, Development, Testing & Evaluation
RIST	Regional Incident Survey Team
RMA	risk mitigation activity
RRAP	Regional Resiliency Assessment Program
S&R	Search and Rescue
S&T	Science and Technology Directorate (DHS)
SCC	Sector Coordinating Council
SHIRA	Strategic Homeland Infrastructure Risk Analysis
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
SWAT	Special Weapons and Tactics/Tactical Operations
TTWG	Technology Transition Working Group
TTX	Tabletop Exercise
UASI	Urban Area Security Initiative
US-CERT	U.S. Computer Emergency Readiness Team
USFA	U.S. Fire Academy
USGS	U.S. Geological Survey
vUSA	Virtual USA

This page intentionally blank

Attachment A: RMA Information for the Emergency Services Sector

A complete list of the Emergency Services Sector's 2010 risk mitigation activities (RMAs) is provided in this attachment. Table A-1 lists all of the sector's key RMAs; other RMAs; and associated descriptive data, output data, and outcome metrics, if available. This information was downloaded from the NIPP Metrics Portal and is current as of June 7, 2010.

Table A-1: RMAs and Progress Indicators

Key RMAs

DHS S&T First Responder Coordinating Council and R&D Working Group

Overview

Description:
The DHS Science and Technology Directorate sponsors the First Responder Coordinating Council (FRCC), a forum and advisory group to discuss, analyze, and serve as the mechanism for the coordination of investment, programs technology, research, development and delivery of technological tools to first responders at the Federal, State, local, tribal and territorial levels.

Key: Yes

Data and Metrics

Descriptive Data:
First Responder RDT&E Working Group reviewed capability gaps and gave recommendations for new start projects to the FRCC. Participants assisted in the vetting of the operational requirements of on-going first responder Science and Technology projects. The working groups assessed capability gaps from four ESS disciplines: Fire Service, Law Enforcement, Emergency Management, and Emergency Medical Service.

Output Data:
The FRCC created a portfolio over $7.5 million in five programs to address capability gaps and submitted the portfolio for funding.

Outcome Metrics:
The New Start Funding was approved for the following projects: Personal Alert and Tracking System; Ambulance Design Safety Standards; Data Integration and Interoperability; Alert and Warning System; and Field Biometric Identification and Credential Validations. The individual timelines for the projects encompass a 12-18 month period.

DHS S&T Virtual USA Project

Overview

Description:
DHS Science and Technology Directorate has launched Virtual USA, a voluntary, practitioner-driven, and federally sponsored initiative focused on cross-jurisdictional information sharing and collaboration among the homeland security and emergency management communities.

Key: Yes

Table A-1: (Cont.)

Data and Metrics

Descriptive Data:
Building on the momentum created through Virtual Alabama, emergency management and homeland security representatives from Alabama, Alaska, Florida, Georgia, Idaho, Louisiana, Mississippi, Montana, North Carolina, Oregon, South Carolina, Tennessee, Texas, Virginia, Washington, FEMA Regions I, IV, VI and X, and FEMA Headquarters are participating at some level in a vUSA regional interoperable information-sharing pilot throughout the United States.

Output Data:
In 2009, only two states had developed information-sharing platforms and as a result of vUSA-led efforts nine stakeholders are engaged in the development of platforms. Some of the practitioners at the state level have begun the process of institutionalizing vUSA through a regional memorandum of agreement which has been adopted by five states (Alabama, Florida, Mississippi, South Carolina, and Virginia). The White House Open Government Initiative recognized vUSA as a DHS flagship initiative that enables better access to information and collaboration. Developed in partnership with the emergency response community, vUSA improves multijurisdictional interoperability and supports emergency response efforts by ensuring that stakeholders at all levels have immediate access to the information they need to make critical decisions.

Outcome Metrics:
In the state of Virginia, it has reduced response times to hazardous material incidents by 70% allowing the state to quickly address threats to the health and safety of its citizens.

Department of Transportation/International Association of Fire Chief's National Hazardous Materials Fusion Center

Overview

Description:
The National Hazardous Materials Fusion Center is a joint partnership between the DOT's PHMSA and the IAFC. The purpose of the center is to provide a secure, Web-based network that will facilitate information sharing for emergency responders training for and responding to HAZMAT incidents.

Key: Yes

Data and Metrics

Descriptive Data:
The National Hazardous Materials Fusion Center is a joint partnership between the DOT's PHMSA and the IAFC. The purpose of the center is to provide a secure, Web-based network that will facilitate information sharing for emergency responders training for and responding to HAZMAT incidents.

Output Data:
The fusion center provides crucial knowledge for all decision-makers about the transportation and delivery of hazardous materials. It is the first data center of its kind for the first responder community. The Regional Incident Survey Teams (RISTs) are now fully operational in each of five PHMSA regions: southwest, western, central, eastern, and southern. Surveys are currently being conducted nationwide and information products are being produced. RISTs gather information for the National Hazardous Materials Fusion Center. RISTs are composed of individuals from around the country who are skilled and experienced in hazardous materials (hazmat) response or experienced in the hazmat industry. RIST members are part of a team invited by a local jurisdiction or state authority to conduct a survey of an incident response of interest and record information from the responder's perspective. In no case is

Table A-1: (Cont.)

the data intended to be used to criticize or condemn response actions, but rather to share lessons learned and smart practices with other emergency responders who may face a similar response.

Outcome Metrics: The RIST teams have posted three Executive Summary Reports on the National Hazardous Materials Fusion Center web-site.

Emergency Management and Response–Information Sharing and Analysis Center (EMR-ISAC)

Overview

Description:
The Emergency Management and Response–Information Sharing and Analysis Center is another critical outreach program that has the responsibility to disseminate critical infrastructure protection and resilience information to ESS leaders and first responders throughout the sector. The ES SSA continues to coordinate with the EMR-ISAC in an ongoing concerted effort to align and coordinate initiatives across the sector, and to improve information sharing and connectivity.

Key: Yes

Data and Metrics

Descriptive Data:
The ES SSA continues to coordinate with the EMR-ISAC in an ongoing concerted effort to align and coordinate initiatives across the sector, and to improve information sharing and connectivity. Initiatives include collaboration through the ESS ISWG, HSIN-CS-ESS, and coordination for future exercises and incident response. As an example of its effectiveness, the EMR-ISAC was instrumental in enhancing the information-sharing processes with the SSA and the ES Sector during the 2009 hurricane season.

Output Data:
EMR ISAC delivers information to more than 30,000 ESS stakeholders. EMR ISAC delivers products that contain emergent, actionable information regarding threats and vulnerabilities to support effective advanced preparedness, protection, and mitigation activities.

Outcome Metrics:
The EMR-ISAC distributes FOUO alerts and advisories to more than 10,000 vetted leaders, owners, and operators of the sector. Additionally, the ISAC has approximately 40,000 direct subscribers to its weekly INFOGRAM.

Emergency Services Self Assessment Tool (ESSAT)

Overview

Description:
An Emergency Services Self Assessment Tool (ESSAT) enables government and public and private entities to perform risk assessments of fixed assets, systems, regional systems, and critical assets. The tool encourages voluntary and interactive stakeholder involvement and allows for a coordinated effort among sector partners by collecting and sharing common risk gaps, obstacles, and protective measures. The tool benefits individual partners and collective disciplines, and supports sector-wide risk management efforts

Key: Yes

Table A-1: (Cont.)

Data and Metrics

Descriptive Data:
The tool encourages voluntary and interactive stakeholder involvement and allows for a coordinated effort among sector partners by collecting and sharing common risk gaps, obstacles, and protective measures. The tool benefits individual partners and collective disciplines, and supports sector-wide risk management efforts.

Output Data:
An ESSAT Prototype pilot for fixed assets is scheduled to be launched in late 2010.

Outcome Metrics:
Eight Emergency Services fixed assets will be self-evaluated.

First Responder Readiness Pilot Project

Overview

Description:
ESS and FEMA National Preparedness Directorate (NPD), working in conjunction with the Center for Homeland Defense and Security (CHDS) Alumni Fellowship Program, seek to improve upon the capability of at-risk public safety organizations such as first responders, emergency management, and public services to better train the individual, family, and organization to prepare themselves and their loved ones in advance of catastrophes. One key component of the initiative includes the development of a Responder and Family Preparedness Technical Assistance Program.

Key: Yes

Data and Metrics

Descriptive Data:
ESS and FEMA National Preparedness Directorate (NPD), working in conjunction with the Center for Homeland Defense and Security (CHDS) Alumni Fellowship Program, seek to improve upon the capability of at-risk public safety organizations such as first responders, emergency management, and public services to better train the individual, family, and organization to prepare themselves and their loved ones in advance of catastrophes. One key component of the initiative includes the development of a Responder and Family Preparedness Technical Assistance Program.

Output Data:
The desired result would be an improved ability of first responders to serve their communities following large-scale disasters. Training and outreach is occurring through national conferences, meetings and individual ESS agencies. A pilot of this project was launched in the spring of 2010.

Outcome Metrics:
4,000 Los Angeles Fire Department personnel received Responder and Family Preparedness information.

Table A-1: (Cont.)

Information Sharing Activities

Overview

Description:
ESS created the ISWG in 2009 to enhance the sector’s information sharing capabilities within ES, with other CIKR sectors and Federal, State, and local partners. The Information Requirements Working Group (IRWG), a subcommittee of the ISWG, is a team of highly experienced practitioners charge with identifying ESS information requirements and developing the HSIN-CS-ESS portal.

The IRWG serves to identify the requirements for information sharing that protects and ensures the continuity and resilience of the sector. The group is working towards a HSIN portal design and function that is user-friendly and contains relevant content and collaboration tools.

Key: Yes

Data and Metrics

Descriptive Data:
ESS created the ISWG in 2009 to enhance the sector’s information sharing capabilities within ES, with other CIKR sectors and Federal, State, and local partners. The Information Requirements Working Group (IRWG), a subcommittee of the ISWG, is a team of highly experienced practitioners charge with identifying ESS information requirements and developing the HSIN-CS-ESS portal.

The IRWG serves to identify the requirements for information sharing that protects and ensures the continuity and resilience of the sector. The group is working towards a HSIN portal design and function that is user-friendly and contains relevant content and collaboration tools.

Output Data:
The IRWG had quarterly on-site planning meetings and monthly conference calls throughout 2009 to identify requirements for the HSIN portal design. The ESS HSIN portal is schedule to go live in September 2010

Outcome Metrics:
A prototype HSIN-CS-ESS portal was launched in February 2010.

NCSD Critical infrastructure Protection - Cyber Security

Overview

Description:
The CIP-CS Program is responsible for leading cross-sector cyber security collaborative efforts under the National Infrastructure Protection Plan (NIPP). In partnership with public and private sectors, CIP CS helps improve the security of the IT Sector and cyberspace across the U.S. CIKR sectors by facilitating risk reduction through infrastructure identification, vulnerability assessment, and protective measures initiatives.
CIP CS engages with CIKR sectors to share IT findings, sector practices, and lessons learned to enhance the Nation’s cybersecurity posture.

Key: Yes

Table A-1: (Cont.)

Data and Metrics

Descriptive Data:
The CIP-CS Program is responsible for leading cross-sector cyber security collaborative efforts under the National Infrastructure Protection Plan (NIPP). In partnership with public and private sectors, CIP CS helps improve the security of the IT Sector and cyberspace across the U.S. CIKR sectors by facilitating risk reduction through infrastructure identification, vulnerability assessment, and protective measures initiatives.

CIP CS engages with CIKR sectors to share IT findings, sector practices, and lessons learned to enhance the Nation's cybersecurity posture.

Output Data:
A major resource within DHS that provides guidance and assistance to the Sector is NSCD, which works collaboratively with public, private, and international entities to secure cyberspace and the Nation's cyber assets. Through involvement and participation with these programs the Sector is able to leverage the tools, information sharing forums, and expertise within NCSD.

Outcome Metrics:
A sub-group to the ESS Information Sharing Working Group (ISWG) is scheduled to stand up in the summer of 2010.

National Sheriffs Association-NSA Homeland Security Initiative Training

Overview

Description:
The NSA, through this initiative, has supported the capability and capacity of local emergency responders to prevent, plan for and response to all-hazards events. The following courses are part of the NSA's Homeland Security Initiative Program:

- Jail Evacuation Planning
- First Responder Training
- Managing the Incident, a Leadership Guide for All-Hazards Events
- Community Awareness and Partnership Training

Key: Yes

Data and Metrics

Descriptive Data:
The National Sheriffs Association Homeland Security Initiative sponsored the following courses as part of their first responder training curriculum: Jail Evacuation Planning, First Responder Training, Managing the Incident, and Community Awareness and Partnership Training

Output Data:
The NSA conducts regular training designed to build technical expertise for its members. In total, the NSA has offered 76 classes with 3,002 total attendees.

Outcome Metrics:
The total classes and attendance are significantly down from last year due to reduction in budgetary allotments in NSA for these programs.

Table A-1: (Cont.)

Regional Resiliency Assessment Program (RRAP)
Overview **Description:** DHS Protective Security Coordination Division, Regional Resiliency Assessment Program (RRAP) led interagency assessment of specific CIKR and regional analysis of the surrounding infrastructure. **Key:** Yes
Data and Metrics **Descriptive Data:** DHS Protective Security Coordination Division, Regional Resiliency Assessment Program (RRAP) led interagency assessment of specific CIKR and regional analysis of the surrounding infrastructure. **Output Data:** In 2009, there were five RRAP’s conducted in Chicago, New Jersey, New York, North Carolina and Tennessee. **Outcome Metrics:** The RRAP's resulted in over $10.5M in Buffer Zone Protection Program grant funding for those areas. The grants are allocated to build terrorism prevention and protection capabilities including planning and equipment acquisition by local first responders.

Table A-1: (Cont.)

Other RMAs

Buffer Zone Protection Program (BZPP)

Overview

Description:
The Buffer Zone Protection Program (BZPP) is a targeted infrastructure protection grant program that seeks to build terrorism prevention and protection capabilities in States and local communities through allowable planning and equipment acquisition. A Buffer Zone Plan (BZP) is a strategic document developed by responsible jurisdictions that: identifies significant assets at the site that may be targeted by terrorists for attack; identifies specific threats and vulnerabilities associated with the site and its significant assets; develops an appropriate buffer zone extending outward from the facility in which protective measures can be employed to make it more difficult for terrorists to conduct site surveillance or launch attacks.

The BZP also identifies all applicable law enforcement jurisdictions and other Federal, state, and local agencies with a role in the prevention of and protection against, threats or attacks specific to the CI/KR site; evaluates the capabilities and gaps of local jurisdictions with regard to terrorism prevention; and identifies specific planning, equipment, training, and/or exercise capabilities needed by the responsible jurisdictions to mitigate the threats and vulnerabilities of the site and its buffer zone.

Key: No

ESS CIKR Resource Center

Overview

Description:
The CIKR Resource Center was established to provide a public-facing, Web-based site that has information on the ESS, including the Sector-Specific Plan and Sector Annual Report. This site is hosted on the FEMA/Emergency Management Institute (EMI) Web site and connects to a CIKR Learning Series and other training opportunities. The link to the Web site is located at: http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/index.htm

Key: No

ESS Information Sharing Working Group (ESS ISWG)

Overview

Description:
The ESS ISWG project is a collaborative effort to identify the information and intelligence requirements, sources, and mechanisms for supporting the continuity of Federal, State, local, tribal, and territorial ESS operations and the protection of ESS personnel. In 2008, ESS developed the ISWG charter and established the working group. The initial work of the ISWG is to focus on improving information sharing relative to alerts/warning, suspicious activity reporting, and situational awareness. Additionally, the ISWG also identified database sources of information for its selected critical elements and is working with selected sector practitioners and DHS Infrastructure Information Collection Division (IICD) to validate the information. This data will be used for sector information sharing, risk management, incident planning, and management and response activities.

Key: No

Table A-1: (Cont.)

ESS Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources

Overview

Description: The sector-specific planning guideline, supported by the ES SCC, is an annex to the Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources (CIKR Pandemic Influenza Guide). The guide assists entities within the ESS as they plan for a pandemic, and it addresses major challenges the sector may face and should assess in its pandemic influenza planning within the seven key areas of vulnerability highlighted in the guideline. This guideline serves as a non prescriptive reference for owners and operators and as a practical tool for business planners who wish to augment and tailor their existing emergency response plans given the unique challenges presented by pandemic influenza.

Key: No

ESS Relevant Portals (HSIN INTEL)

Overview

Description:
This HSIN INTEL community provides a secure, sensitive but unclassified (SBU) Web site that allows authorized Federal, State, local, tribal, and territorial security professionals to access DHS I&A products. This portal is currently accessed by appropriately vetted sector personnel, and for-official-use-only (FOUO) information is disseminated throughout the sector via the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC). This enterprise is a collaborative effort with USFA and I&A to establish an Intelligence Portal on HSIN as a way for ES emergency responders to access FOUO information

Key: No

ESS Risk Assessment Working Group (RAWG)

Overview

Description:
The Sector began laying the groundwork for assessing risk by identifying sector critical elements as part of the National Critical Infrastructure Prioritization Program (NCIPP) within the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). This year ESS held an initial exploratory meeting with selected practitioners representing one identified critical element which was the HAZMAT community. From that meeting we developed an approach to the establishment of a Risk Assessment Working Group (RAWG). These efforts will include representatives from FEMA Incident Management Systems Integration Division (IMSID) and Office of Preparedness Policy, Planning, and Analysis (PPPA) to leverage existing work and collaborate on their Target Capabilities List (TCL) methodology and program.

Key: No

FBI InfraGard

Overview

Description:
The FBI’s InfraGard program is an outreach program comprised of businesses; academic institutions; State, local, and tribal law enforcement agencies; and other participants dedicated to sharing

Table A-1: (Cont.)

information and intelligence to prevent hostile acts against the United States. The relationship supports information sharing at the national and local levels and fosters an increase in the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime, and other major crime programs. Additionally, it improves interaction and information sharing regarding threats to critical infrastructure, vulnerabilities, and interdependencies; provides members with value-added threat advisories, alerts, and warnings; and offers members a forum for education and training on counterterrorism, counterintelligence, cyber crime, and other related matters.

Key: No

FEMA-Target Capabilities (TCL)

Overview

Description:
This activity is designed to enhance the resilience of target capabilities of emergency responders on a regional level. The National Preparedness Guidelines and TCL establish the system's all-hazards framework and establish national priorities. The Target Capabilities List (TCL) is a national-level, generic model of operational readiness capabilities that defines all-hazards preparedness and serves as a planning, assessment, and training tool. The TCL is an ongoing preparedness activity that provides the means to accomplish a mission and achieve desired outcomes by performing critical tasks, under specified conditions, to target level performance. Many of the associations affiliated with the SCC continue to be engaged in FEMA's TCL work.

Key: No

IED Awareness Training

Overview

Description:
The ESS works closely with the DHS Office for Bombing Prevention (OBP) as it regularly conducts IED training for first responders across the United States. The course provides information necessary to develop the knowledge and skills required to establish surveillance detection operations to protect CIKR during elevated threat periods. In addition to providing awareness level training of terrorist tactics and attack history, the course allows participants to practice the methods of detection and surveillance through practical exercises.

Key: No

Multi-Jurisdiction Improvised Explosive Device (IED) Security Planning

Overview

Description:
The Multi-Jurisdiction IED Security Plan (MJIEDSP) aids multi-jurisdiction areas in developing a detailed IED security plan. The IED security plan outlines specific bombing prevention actions that reduce vulnerability and mitigate risk against the primary terrorist IED attack method within a multi-jurisdiction area. The program is intended to support State, local, and tribal efforts to enhance IED security capabilities by adopting effective practices to maximize available resources to prevent and respond to an IED threat.

Key: No

Table A-1: (Cont.)

Protective Security Advisor (PSA) Program
Overview **Description:** PSAs serve as DHS's on-site critical infrastructure and vulnerability assessment specialists assigned to local communities throughout the United States. PSAs serve as DHS liaisons between Federal, State, territorial, local, and tribal governments and the private sector. A PSA's primary responsibilities are to: assist in the identification of CIKR assets; maintain a close working relationship with government and public safety officials; serve as a communication conduit between DHS and the security community; coordinate risk-reduction efforts and protective security initiatives requiring Federal involvement; coordinate requests for services and resources from CIKR asset owners and operators; function, when needed, as the on-scene Office of Infrastructure Protection (IP) representative within State and local Emergency Operations Centers (EOCs); and support the officials responsible for special event planning and exercises in their district by providing local knowledge of CIKR. **Key:** No
Surveillance Detection Training
Overview **Description:** The ESS works closely with the Office of Bombing Prevention to ensure that first responders and specifically State, Local, and Tribal Law Enforcement Officers are aware of the OBP Surveillance Detection Training Course. The course provides the knowledge and skills necessary to establish surveillance detection operations to protect CIKR during periods of elevated threat. The course provides awareness level training of terrorist tactics and attack history and allows participants to practice the methods of detection and surveillance through practical exercises. **Key:** No

This page intentionally blank

Attachment B: R&D Activities/FRWG Capability Gap List

Capability Gap	Supported Discipline					
	LE	FIRE	EMS	EM	MIL	OTHER
Public Alert and Warning		x	x	x		x
Data Analysis and Real-Time Situational Awareness	x	x	x	x		PW[a]
Voice Communication Interoperability	x	x	x	x		PW
Enhanced Situational Awareness Data at the Operator Level	x	x		x		
License Plate Recognition and Data Analysis	x					
Pandemic Disease Indication Capability	x	x	x	x		CI/KA[a]
Vertical Vehicle-Borne IED Engagement	x	x			x	
Field Biometric Identification	x	x	x	x	x	USCG
Handheld Weapon Detection	x					
Vehicle Disablement	x				x	
Real-Time Tracking of Patients, Standardized Triage Tags	x	x	x	x		DOS[a] CDC
Standardized Construction and Design Standards for Ambulances	x		x			
Integrated Data Collection, Records Management, Reliable and Consistent Information Sharing	x	x	x	x		
Respiratory Protection	x	x	x	x	x	ALL
Improved Respiratory Protection	x	x	x			PVT SEC[a]
Tracking Operational Personnel and Accountability	x	x	x	x	x	OTHER
Detection, Remote Sensing, Image Exfiltration for Wild Fires in Rural Environments	x	x	x	x		CBP[a]
Immerse EMS Training	x	x	x	x		
Chem/Bio IPT Detection Standards	x	x	x	x		
Common Software/Display Common Operating Platform	x	x	x	x		

[a] PW = public works; KA = key assets; DOS = U.S. Department of State; PVT SEC = private sector; CBP = U.S. Customs and Border Protection.

This page intentionally blank

Attachment C: 2009 IAB R&D Priorities

Priority List	
1	Personal Bluetooth (like) Radio Interference
2	3-D Tracking of Personnel
3	Hands-Free Radio Intercom
4	Validated Performance Criteria and Certification Testing Methods for Wireless Personal Alert Safety Systems (PASS)
5	Noise-Filtering Digital Speaker/Microphone for SCBA Face piece
6	Improved Single Detector for Chemical Warfare Agents and Toxic Industrial Chemicals
7	Emergency Responder Body-Worn Integrated Electronics System Development
8	CAD-to-CAD Interface Information Resources
9	Improved Explosive Detection Capability
10	Handheld Standoff Chemical Identifier
11	Study and Standard Development of Incident Management Qualification
12	Multi-Agent Biological Detection Field Assays
13	Vehicle-Borne Improvised Explosive Device Render-Safe Tool
14	Identification of Wildland Firefighting Respiratory Hazards and a Certification Standard for Wildland Firefighting Respiratory Protective Equipment
15	Device for Standoff Casualty Locator
16	Research Feasibility of Air-Purifying Respirator Use During Late-Stage Incendiary Incident Operations
17	Rapid System(s) to Decontaminate Ambulance Interiors
18	Modeling, Simulation, and Gaming Software Evaluation Tool
19	Improved Mass Decontamination Systems
20	Guide for Increasing Patient Transport Capability
21	Equipment/Supply Guide for Relocating Special Needs Evacuees
22	Enhanced Decontamination Capability for Special Needs Victims

The research and development items are assessed based on the following criteria: urgent need, life safety, mission performance, incident management, compatibility or interoperability, use by multiple responder disciplines, and use in day-to-day operations, as well as major incidents.

This page intentionally blank