

Committee
Findings and Recommendations

Homeland Security in Connecticut

December 18, 2007

Legislative Program Review
& Investigations Committee

Homeland Security in Connecticut

In April 2007, the Legislative Program Review and Investigations Committee voted to undertake a study of *Homeland Security in Connecticut*. The focus of this study is on the actions taken by the state Department of Emergency Management and Homeland Security (DEMHS) and its predecessor agencies to improve the status of the state's homeland security and related emergency management efforts. Specifically, the study is focusing on recent assessment, planning, and implementation activities related to improving the state's ability to prevent, protect against, respond to, and recover from terrorist attacks.

Staff presented an extensive description of the Department of Emergency Management and Homeland Security's historical background, authority, counterterrorism and emergency management functions, and federal and state funding sources in the briefing report issued in September 2007. Based on committee feedback, resource considerations, and staff identification of significant issues, analysis was concentrated after the briefing in a few key areas including the protection of critical infrastructure, intelligence sharing and terrorism investigations, communications, and other concerns that have been raised during the course of this review. In addition, staff have provided more specific expenditure information on the projects funded by federal grant programs.

Summary Findings

Clearly, the state has made progress in the area of homeland security and is better prepared than it was in the autumn of 2001. For example, federal, state, and local law enforcement agencies are now better connected and informed through a statewide central resource that collects, analyzes, and disseminates criminal and terrorism-related intelligence. A multi-jurisdictional law enforcement task force on terrorism serves to streamline investigations and responses to terrorism-related allegations. Critical infrastructure identification and prioritization are on-going, while assessment and protection efforts are being implemented. Further, a significant amount of DEMHS attention is focused on improving the redundancy and resiliency of Connecticut's emergency communications systems, though true interoperability is several years away.

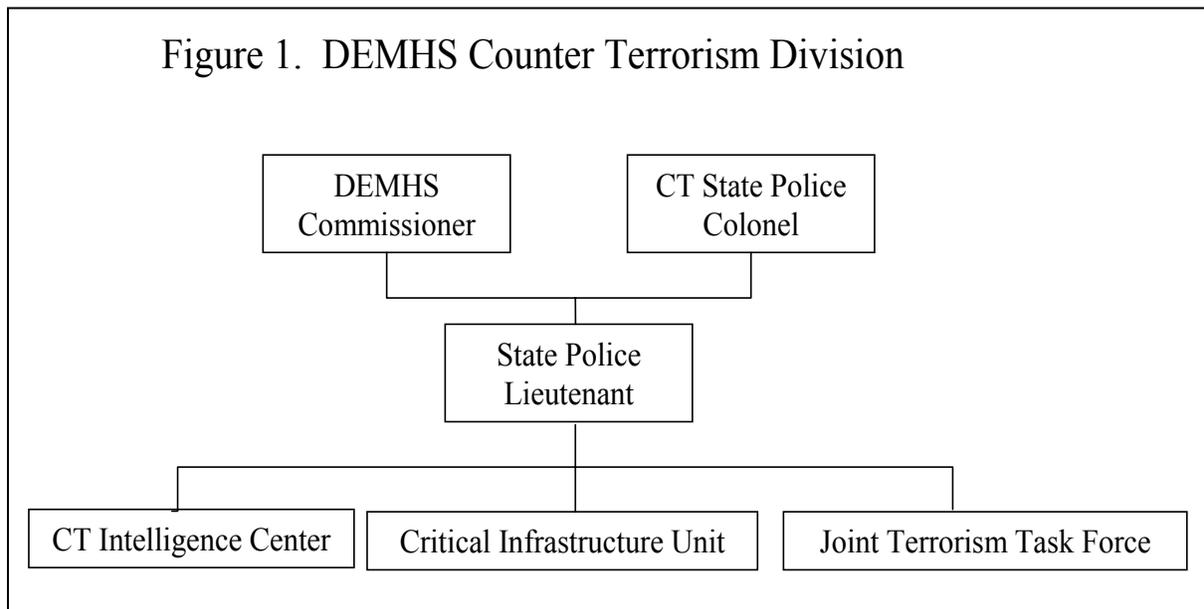
Additional enhancements that would better ensure the prevention, protection, and response capabilities of the state need to be further developed. Many improvements have already been identified by DEMHS and are in various stages of implementation. The aim of the program review recommendations offered here is refinement of the systems in place.

Counter Terrorism Division and Communications Overview

The Counter Terrorism Division of DEMHS contains many of the functions traditionally considered to be the core of the homeland security mission. Its three principal functions, which are a major focus of this document, are:

- *Critical Infrastructure Protection Unit (CIPU)*: identifies, assesses, and categorizes critical assets within the state and develops plans to improve the security at those sites.
- *Connecticut Intelligence Center (CTIC)*: an intelligence center staffed by local, state, and federal law enforcement personnel who collect, analyze, and disseminate information on criminal and terrorism-related activities.
- *Joint Terrorism Task Force (JTTF)*: a law enforcement unit that uses a multi-agency approach to investigating and combating terrorism.

These functions previously resided in the former Division of Homeland Security within the Department of Public Safety (DPS). The Counter Terrorism Division, currently staffed by 13 state police officers, works with a range of local and federal agencies in combating terrorism, as described later. As illustrated in Figure 1, the division is headed by a lieutenant who reports to both the state police colonel and the commissioner of DEMHS.



Communications. Given the committee’s expressed interest in the communications issue, updated information on the status of the state’s efforts to improve public safety communications systems, processes, and infrastructures is provided in this report. Communications interoperability among agencies and jurisdictions has been a long-standing problem in the public safety community. Efforts to address communications have been underway since 2002.

The first group to attempt to examine this issue was convened by the Office of Policy and Management in 2002. The initial findings of this ad hoc working group eventually evolved into the workings of the current communications sub-committee of the DEMHS Coordinating Council. The sub-committee and its different technical working groups have explored short-term as well as long-term emergency communications goals. The development of these goals and the ongoing implementation steps are contained in the Statewide Communications Interoperability Plan (SCIP) and are discussed in detail in Section IV.

Measuring Prevention and Methodology

Many of the activities discussed in this document relate to the prevention of and protection from terrorist events. In considering DEMHS performance of these functions, it is important to acknowledge the ultimate success of these endeavors depends on the cooperation of or direction from agencies and organizations not under the control of DEMHS. For example, the primary responsibility for collecting and disseminating intelligence, of which CTIC is a small part, and for identifying and apprehending terrorists, in which JTTF plays a role, rests with the Federal Bureau of Investigation (FBI) and other federal agencies.

Similarly, because 85 percent of the nation's critical infrastructure is in the hands of the private sector, businesses themselves have the principal duty to mitigate any vulnerability.¹ Government agencies clearly have an interest in supporting private sector risk management assessments and planning, and in addressing risks outside of individual properties. Except in very limited circumstances, federal grant programs do not provide for improvements to private sector facilities.² In addition, the direction and funding provided by the federal government is somewhat skewed. While prevention remains a top national priority, a majority of the federal funding in homeland security goes toward response efforts.³ Some have commented that homeland security efforts are biased toward response because the system overall is not designed to focus on prevention.

A second factor to consider is both DEMHS and the homeland security function are fairly new. What precisely constitutes homeland security and how the nation should go about it has evolved over a very short period of time. The first national strategy on homeland security was issued by the federal government in 2002. In that document, homeland security was about preventing and responding to terrorism. In October 2007, the current homeland security strategy was issued. The strategy outlined four new goals: prevent and disrupt terrorist attacks; protect the American people, our critical infrastructure, and key resources; respond to and recover from incidents that do occur; and continue to strengthen the foundation to ensure long-term success. However, in a post-Katrina environment, the scope of what constitutes homeland security has expanded. The 2007 strategy document acknowledges that "effective preparation for catastrophic natural disasters and man-made disasters, while not homeland security per se, can nevertheless

¹ U.S. Homeland Security Council, *National Strategy for Homeland Security*. Washington D.C., October 2007, p. 4.

² For example, in certain cases privately owned transit facilities are eligible for homeland security funding.

³ Christopher Bellavita, What is Preventing Homeland Security, *Homeland Security Affairs*, Volume I Issue 1, Summer 2005.

increase the security of the Homeland.”⁴ In the view of many, too much concentration on terrorism reduces overall readiness.

Similarly, the state of Connecticut has changed its approach to homeland security. The first agency responsible for homeland security efforts was located in the Department of Public Safety and was subsequently merged with the Military Department’s emergency management office to form a new agency. DEMHS has only been in existence since 2005 and does not have a long track record to evaluate. In fact, the department is still trying to consolidate its central functions and staff into one office, while simultaneously attempting to bolster its regional staff and capabilities. Furthermore, many of its goals involve creating new partnerships and cooperative arrangements that have to be viewed in the context of long-term change.

Finally, measuring prevention and protection directly is a very difficult thing to do.⁵ Often the question is asked, how do you prove something did not happen? In the case of homeland security, no entity is able to discern what the enemy has decided not to do or to count how many attacks were deterred or stopped. Nonetheless, being able to measure prevention is important for government accountability and for effectively directing investments. Waiting to measure protection activities once there is an attack may be too late.

One approach to measuring prevention activities is to use process measurement. Measuring effectiveness in this case means evaluating processes and systems that lead to preferred outcomes. This is one approach that the federal government has been refining through the development of target capabilities.⁶ The federal target capabilities list currently is used as a reference not a requirements document for states. The belief underpinning this approach is that if certain elements (e.g., people, processes, agreements) are in place then it will help to lead to the ultimate goal of preventing terrorist attacks.

Methodology. The approach taken in this review is to: 1) consider the process elements contained in homeland security literature, such as the U.S. Department of Justice’s Fusion Center Guidelines; 2) analyze and report on the status of the Department of Homeland Security and Emergency Management goals in the State Homeland Security Strategy (SHSS) and the department’s own internal strategic goals; and 3) examine the overall management of these functions.

Information about homeland security theory, practices, initiatives, and funding was obtained from a variety of sources. In addition to literature reviews, program review staff also conducted extensive interviews with DEMHS staff as well as other experts in the field, including: the Federal Bureau of Investigation (FBI); the federal Transportation Security Administration (TSA); the federal Department of Homeland Security (DHS); the Connecticut State Police (CSP); other law enforcement personnel; emergency management personnel; and private sector representatives. In addition, program review staff examined and, in conjunction

⁴ *National Strategy for Homeland Security*, p.3.

⁵ See for example, Rapheal Perl, *Combating Terrorism: The Challenge of Measuring Effectiveness*, Congressional Research Service, March 12, 2007, (Order Code RL 33160).

⁶ Target capabilities describe the 37 core capabilities that all levels of government are expected to develop and maintain in order to prevent or respond to a major catastrophe.

with DEMHS, analyzed confidential documents and information regarding the state's critical infrastructure program.

Program review staff interviewed and received feedback from Regional Planning Organization (RPO) staff and board members, and attended a meeting of the Capitol Region Emergency Planning Committee, a subcommittee of the Capitol Region Council of Governments. Staff attended meetings of the Emergency Management and Homeland Security Coordinating Council and the Connecticut Intelligence Center policy board. Staff also observed an Urban Search and Rescue field exercise.

The program review committee held a public hearing on this issue on September 25, 2007. The commissioners of the Department of Public Safety and the Department of Emergency Management and Homeland Security addressed the committee, and the Connecticut Conference of Municipalities submitted testimony.

Emergency Management Functions

Most of the analysis in this report is confined to typical homeland security functions as opposed to the emergency management tasks conducted by the department. As discussed in the briefing, emergency management is a vast enterprise. It encompasses a broad range of activities that involve being prepared to respond to and recover from disasters and other emergencies and likely merits a separate study. While in-depth analysis in emergency management area was not undertaken, staff did query all municipal chief elected officials (CEOs) in Connecticut as to their satisfaction with DEMHS' preparedness efforts through a survey.⁷

The survey results indicated a fairly high level of approval of DEMHS' leadership activities, but less so for its funding and financial disbursement capabilities. For example, most CEOs who responded (90 percent of 90 responses) believed DEMHS was very or somewhat effective at providing overall direction and leadership regarding preparedness for emergencies. Nearly 60 percent (of 91 responses) of the CEOs believed that the perspectives of municipalities are sufficiently represented in the state's planning process for federal preparedness grants.

Most CEOs (77 percent of 91) also believed that their municipality's overall capability for responding to a terrorist incident, involving a chemical, biological, nuclear, or explosive agent, has improved since 9/11/2001, though most (56 percent of 91) believed their municipality was only somewhat prepared to respond to a terrorist incident.

In addition, CEOs were nearly evenly split on a question regarding the effectiveness of DEMHS in providing an adequate level of funding to municipalities for emergency preparedness efforts (49 percent of 89 indicating very or somewhat effective and 51 percent indicating somewhat or very ineffective). Similarly, half of the CEOs felt DEMHS was very or somewhat effective (50 percent of 88) at disbursing promised funding in a timely manner. As discussed later in this document, the method of funding local jurisdictions has changed significantly since the survey was administered. The full survey results are included in Appendix A.

⁷ A total of 101 responses were returned for an overall response rate of 60 percent, though the response rate to individual questions varied.

Organization of Report

This report is organized into five sections. The first section summarizes the federal financial assistance programs for homeland security described in the briefing and provides a more in-depth analysis of actual expenditures. Section II examines the critical infrastructure program, while Section III assesses the Connecticut Intelligence Center and the Joint Terrorism Task Force. The fourth section reviews the actions taken by DEMHS to improve interoperable communications. Finally, Section V describes the top funding priorities of the Department of Public Safety and the Department of Emergency Management requested by the committee, as well as findings and recommendations related to selected management practices and other concerns.

Section I

Federal Financial Assistance

Between 2002 and 2007, Connecticut was awarded nearly \$154 million in federal grants to assist the state and local governments with preventing and preparing for terrorist attacks and other major catastrophes. The state and municipal governments have been using these funds to increase the state's overall level of preparedness. The discussion below identifies the major federal homeland security funding programs, trends in federal funding to Connecticut, and state and local expenditures by project. It also provides examples of the items purchased with federal homeland security funding.

Homeland Security Funding For Connecticut

Summarized in Table I-1 are the major federal homeland security and preparedness grants administered by DEMHS. Federal funding provides the majority of the resources for Connecticut's preparedness activities.

Table I-1. Federal Homeland Security and Preparedness Funding, FFY 2007 and FFYs 2002- 2007		
Grant Program	FFY 2007	2002-2007 Total
Homeland Security Grant Program		
State Homeland Security Grant Program*	\$5,840,000	\$91,723,248
Law Enforcement Terrorism Prevention Program	4,170,000	18,908,181
Citizen Corps Program	211,033	1,774,658
Metropolitan Medical Response System**	258,145	1,118,067
Urban Areas Security Initiative***	0	10,371,406
Emergency Management Performance Grant****	3,553,767	14,771,053
Buffer Zone Protection Program	194,000	1,233,000
Public Safety Interoperable Communications	13,000,000	13,000,000
Transit Security Grant Program - Ferry Security	414,350	414,350
Other	0	346,655
Total	\$ 27,641,295	\$ 153,660,618
FFY= Federal Fiscal Year		
*In 2002, this program was called the State Domestic Preparedness Equipment Program. ** The only eligible city is Hartford ***The only eligible city was New Haven. ****Includes FFY 2007 supplemental grant of \$728,231		
Sources of data: FFY 2007 HSGP Grant Guidance, Department of Homeland Security; Department of Emergency Management and Homeland Security; Connecticut State Budget Office, Office of Fiscal Analysis		

Homeland Security Grant Program (HSGP). Overall, the Homeland Security Grant Program is the single largest cumulative federal grant primarily employed for building and sustaining preparedness capabilities. It represents 81 percent of the federal homeland security

funding that Connecticut has received since 2002. The program consists of five sub-grants described below:

- ***State Homeland Security Program:*** Described as the “core” assistance program, SHSP provides funding for the equipment, training, exercise, and planning needs of state and local governments related to potential acts of terrorism. It is the largest of the sub-grants available under the HSGP. Initially, much of the funding under this program was aimed at equipping and training first responders to respond to incidents involving weapons of mass destruction. The scope of funded activities has evolved into supporting all types of catastrophic events, as long as the funded activities also support capabilities that relate to terrorism.
- ***Law Enforcement Terrorism Prevention Program (LETPP):*** This program provides funds to law enforcement and public safety organizations to support terrorism prevention activities. Examples of what DEMHS proposes to use FFY 2007 funding for under this program include: supporting and enhancing the Connecticut Intelligence Center, which gathers and disseminates intelligence information to the law enforcement community and its public safety partners; and providing equipment to local police departments in support of the state’s preparedness goals.
- ***Citizen Corps Program (CCP):*** The purpose of this program is to bring community and government leaders together to coordinate community involvement in emergency preparedness, response, and recovery activities. At present, 63 Citizen Emergency Response Teams that are trained or in training to perform a number of different duties including supporting first responders, providing assistance to victims in a shelter, and organizing spontaneous volunteers at a disaster, are funded.⁸
- ***Metropolitan Medical Response Systems (MMRS):*** The MMRS program supports local preparedness efforts in 124 specific areas of the country to respond to all mass casualty incidents including terrorism, epidemics, natural disasters, and large scale hazardous materials incidents. The Capitol Region Council of Governments represents the only metropolitan area in Connecticut to qualify for funding under this program; it has received almost \$260,000 in FFY 2007.
- ***Urban Area Security Initiative (UASI):*** The UASI program focuses on the planning, equipment, training, and exercise needs of high-threat, high-density urban areas. More specifically, the funds must increase the capacity of urban areas to prevent, protect against, respond to, or recover from terrorist threats (i.e., chemical, biological, radiological, nuclear, explosive, agricultural, and

⁸ As of June 21, 2007, there were 52 teams fully trained, 11 in training, and an additional 24 proposed.

cyber terrorism incidents). Only the city of New Haven qualified once, in 2004, for \$10.4 million under this program.

Emergency Management Performance Grant Program (EMPG). The EMPG program is designed to assist in the development, maintenance, and improvement of state and local emergency management capabilities, while addressing issues of national concern. This program pre-dates 9/11.

Buffer Zone Protection Program (BZPP). This program is designed to enhance the security surrounding the nation's critical infrastructure, including chemical facilities, financial institutions, nuclear and electric power plants, dams, stadiums, and other high-risk/high consequence facilities. The funding is intended to assist in developing effective measures that make it difficult for terrorists to conduct surveillance or to launch attacks within the vicinity of critical infrastructure, as well as increase the preparedness of local jurisdictions where such facilities are located. The buffer zone improvements focus on the perimeter outside the identified infrastructure. Funding cannot be passed on to private sector facility owners for internal security measures. Only DEMHS, as the State Administrative Agency for DHS grants, is eligible to apply for these funds, but the local jurisdictions with authority over and around the identified sites are subgrantees.

Public Safety Interoperable Communications Grant (PSIC). The PSIC grant is a new (FFY 2007), one-time program designed to assist public safety agencies to acquire, deploy, and train on interoperable communications systems. The grant was awarded on September 30, 2007. Each state was awarded a base amount of \$3 million with the balance distributed based on a DHS risk assessment. For more information on the PSIC grant see Section IV.

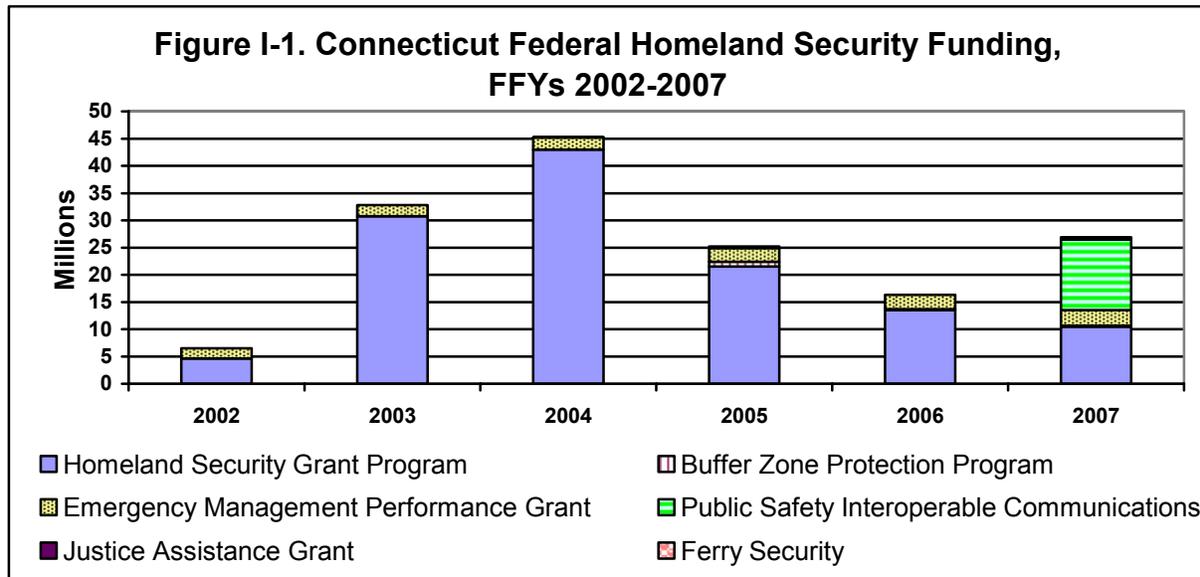
Transit security and other. The Transit Security Program's sub-program for ferry security is intended to enhance security measures around transit facilities. Connecticut's two major ferry operations (Bridgeport/Port Jefferson and New London/Orient Point) received a combined total of \$414,350 in FFY 2007. (This was the only year the ferry companies have received funding.) DHS selected DEMHS as the State Administrative Agency or responsible entity for this grant.

Connecticut has also received two one-time Justice Assistance Grants, available through the federal Department of Justice. These grants totaled \$346,000 and supported the former state terrorism task force and certain emergency management functions – mainly equipping the Urban Search and Rescue team.

Trends in Homeland Security Funding

Figure I-1 shows the trend in federal homeland security funding awarded to Connecticut since 2002. *After the events of 9/11, there was a considerable increase in federal homeland security funding, which peaked in 2004 when the state was awarded approximately \$45 million. From this point, the total funding declined over the next two years. In 2007, there was an increase in funding due to the one-time interoperability grant of \$13 million. In the absence of*

this interoperability grant, total homeland security funding would have been about \$14.6 million, or about half the actual amount awarded.



Federal Homeland Security Expenditures by Project, Sub-Program, and Discipline

At the September briefing, the program review committee asked staff to provide additional information on how federal homeland security money was invested. DEMHS, which was created in 2005, can account for total homeland security funding for the federal grant years for which it was responsible – from 2004 through present. Prior year’s federal grants were managed by the Department of Public Safety (2003) and the Military Department (2002).

Table I-2. Homeland Security Expense Breakdown

Department	Administrative	Equipment	Total
Department of Emergency Management and Homeland Security 2004-2006	\$10,609,312	\$42,916,023	\$53,525,335
Department of Public Safety 2003	2,465,000	27,693,000	30,158,000
Military Department 2002	274,298	4,198,321	4,472,619
Total	\$ 13,348,610	\$ 74,807,344	\$ 88,155,954

Source: DEMHS, DPS, Military Department. Note: Administrative includes: salary, overtime, consultant fees, office supplies, etc., and training and exercise expenses.

Due to the fact that different agencies were administering grants with different goals in different years, the grant funding was accounted for in different ways. In the discussion below, aggregated amounts from the various departments are presented to show how much was spent on

administrative costs versus equipment costs. There is also a description of the equipment purchased by each department. A more detailed analysis of DEMHS expenditures is also presented.

In Table I-2 staff has estimated the total amount of federal homeland security funding spent on administrative costs such as salaries, the amount spent on equipment, and the grand total. *As the table indicates, 85 percent of the funding was invested in equipment, and 15 percent was spent on administrative expenses.*

Military Department. In 2002, the Military Department administered the \$4.5 million federal grant through the former Office of Emergency Management.⁹ Approximately 94 percent of the money went toward equipment. About 75 percent of that total funded local, regional, and hospital investments, while 25 percent went to the state. Examples of equipment purchased include: decontamination trailer units; chemical identification kits; various tools; personal protective equipment; decontamination equipment; powered air purification respirators; gas masks; emergency response kits; gas monitors; air packs; air cylinders; and various smaller equipment items.

Department of Public Safety. The former Division of Homeland Security in the Department of Public Safety was the administrative agency for the \$30.1 million federal homeland security grant in 2003. Approximately 8 percent of the total funding went toward administrative expenses, though this included over \$1 million in expenses related to the nationally recognized TOPOFF 3 exercises. While the majority of funding went to municipalities, the exact breakdown was not immediately available for this portion of the funding. Examples of the equipment purchased include: personal protective equipment; chemical, biological, or radiological detection equipment; decontamination trailers; communications equipment; pharmaceuticals; CBRNE incident response vehicles; search and rescue equipment; and closed-circuit television cameras.

DEMHS. Since its inception, DEMHS has spent \$53.5 million in federal funding to enhance the state's preparedness and response capabilities. This does not include funding that has been encumbered or awarded and not encumbered. A total of \$10.6 million (20 percent) has been spent on salaries, overtime, and backfill (i.e., replacement of public safety personnel in training) while \$42.9 million (80 percent) has been spent on equipment.

The federal government provided the accounting architecture through which states can track expenditures. Expenditure information is classified on a project, program, and sub-program basis. Below expenditures are analyzed by project, the largest grouping of expenditures, and by sub-program, the smallest grouping of expenditures. In addition, information is provided on how much has been expended by discipline. Due to the method of financial coding and issues with the state's accounting system (CORE-CT), approximately \$6.2 million was not coded by program and sub-program. Consequently, the analysis below totals \$47.3 million.

⁹ The Military Department administered Department of Justice Domestic Preparedness Program Grants from 1999 through 2002. The earlier years were not included in this analysis because the time frame that this report covers is from 2002 through the present. The 1999-2001 preparedness grants totaled \$1.7 million.

In short, the largest project is the establishment of a public and private emergency preparedness program, while the largest category of expenditure is interoperable communications. Not surprisingly the public safety disciplines of police, emergency management, and fire received the most funding.

Table I-3. Homeland Security Funding by Project, 2004-2006			
Project	State	Local	Total
Establish/Enhance Public-Private Emergency Preparedness Program	\$2,669,606	\$21,282,805	\$23,952,412
Develop/Enhance Interoperable Communications	7,225,191	1,097,228	8,322,419
Assess Vulnerability/ Harden Critical Infrastructure	1,160,650	3,312,534	4,473,184
Establish/Enhance Regional Response Teams	439,925	2,848,791	3,288,715
Establish /Enhance Emergency Operations Center	1,718,063	1,208,949	2,927,012
Establish / Enhance Terror Intel /Early Warning System	46,858	2,229,543	2,276,401
Establish /Enhance Sustainable Homeland Security Training Program	343,365	399,006	742,370
Administer and Manage Homeland Security Grant Program	54,061	565,970	620,031
Establish/Enhance Public Health Surveillance System and Pharmaceutical Stockpile	480,799	2,971	483,770
Establish /Enhance Sustainable Homeland Security Exercise Program	181,081	75,304	256,385
Total	\$14,319,598	\$33,023,101	\$47,342,698
Note: Actual expenses only. No encumbrances are included. Includes the State Homeland Security Grant Program, Law Enforcement Terrorism Prevention Program, Citizen Corps Program, Metropolitan Medical Response System, and Emergency Management Performance Grant. Source: DEMHS			

Project. Table I-3 summarizes total federal grant expenditures by major project.¹⁰ As discussed above, a total of \$47.3 million in federal funding to enhance the state’s preparedness and response capabilities between 2004 and 2006 can be categorized by project. About \$33.0 million (70 percent) has been spent by municipalities, and the other \$14.3 million (30 percent) has been expended on state priorities.

¹⁰ Program review staff have consolidated the original 17 DEMHS project categories into 10 related project categories. For example, “Establish /Enhance Public Health Surveillance System” and “Pharmaceutical Stockpile” were two separate projects that were combined into one project

Table I-4. Examples of State and Local Purchase by Project, 2004-2006		
Project	State Level Purchases	Local Level Purchases
Establish/Enhance Public-Private Emergency Preparedness Program	Computers, laptops, detection systems (e.g. radiation dosimeters), personnel identification/security systems, personal protective equipment, search & rescue equipment, site clean-up/decontamination, traffic management, responder vehicles & trailers, generators, equipment storage.	Computers, laptops, detection systems (e.g. radiation dosimeters), personnel identification/security systems, personal protective equipment (PPE), search & rescue equipment, site clean-up/decontamination, traffic management, responder trailers, generators, and equipment storage.
Develop/Enhance Interoperable Communications	State Tactical On-scene Channels (STOCS) assigns frequencies to facilitate interoperable communications on high band UHF and 800 MHz systems, radio towers enhancements to improve range and coverage in state, anticipate procuring "black boxes" which will enable high band UHF and 800 MHz radios to talk to each other	Purchasing portable radios, mobile (walkie talkie type) radios, mobile data terminals (MDTs), Computer Aided Dispatch (CAD) systems (for individual towns and regionally), radio consoles, and repeaters to eliminate dead spots in jurisdictions
Assess Vulnerability/Harden Critical Infrastructure	Orange Alert overtime, rail security improvements, risk assessment software, night vision and surveillance equipment, patrol vessels	Installing fencing, lighting, security systems, and surveillance cameras at municipal government buildings to increase security and prevent unauthorized entry.
Establish/Enhance Regional Response Teams	Response vehicles, trailers, tow vehicles, field testing & detection equipment, meters (gas, chemical, biological and radiation meters, including replacement tubes and chips), Level A PPE, chemical libraries (databases)	Response vehicles, trailers, tow vehicles, field testing & detection equipment, meters (gas, chemical, biological and radiation meters, including replacement tubes and chips), Level A PPE, chemical libraries (databases)
Establish /Enhance Emergency Operations Center	Installing Geographical Information System (GIS) software in the state Emergency Operations Center	High band radio equipment to link local EOCs with regional and state EOCs and other equipment
Establish / Enhance Terror Intel /Early Warning System	Installing Automatic Fingerprint Information Systems (AFIS) within state law enforcement agencies to assist in investigations.	Installing Automatic Fingerprint Information Systems (AFIS) to assist local police in investigations, providing stipends to participating towns that send police personnel to staff the Connecticut Intelligence Center (CTIC).
Establish /Enhance Sustainable Homeland Security Training Program	CT Fire Academy and Police Officers Standards and Training Council (POST) instructor costs to plan and deliver National Incident Management (NIMS) and other training.	Providing backfill and/or overtime funding to allow local staff to attend Homeland Security training.
Administer and Manage Homeland Security Grant Program	Office equipment, staff time	Enhancement of plans and development of protocols for emergency management and recovery from disasters
Establish/Enhance Public Health Surveillance System and Pharmaceutical	Mass Color Spectrometry to identify agents of chemical terrorism and establishment of a pharmaceutical stockpile	Development of plans and protocols and a training program related to public health surveillance

Table I-4. Examples of State and Local Purchase by Project, 2004-2006		
Project	State Level Purchases	Local Level Purchases
Stockpile		
Establish /Enhance Sustainable Homeland Security Exercise Program	Provide funding for a CT Fire Academy instructor to design and coordinate exercises (drills).	Providing backfill and/or overtime funding to allow local staff to attend Homeland Security exercises.
Source: DEMHS		

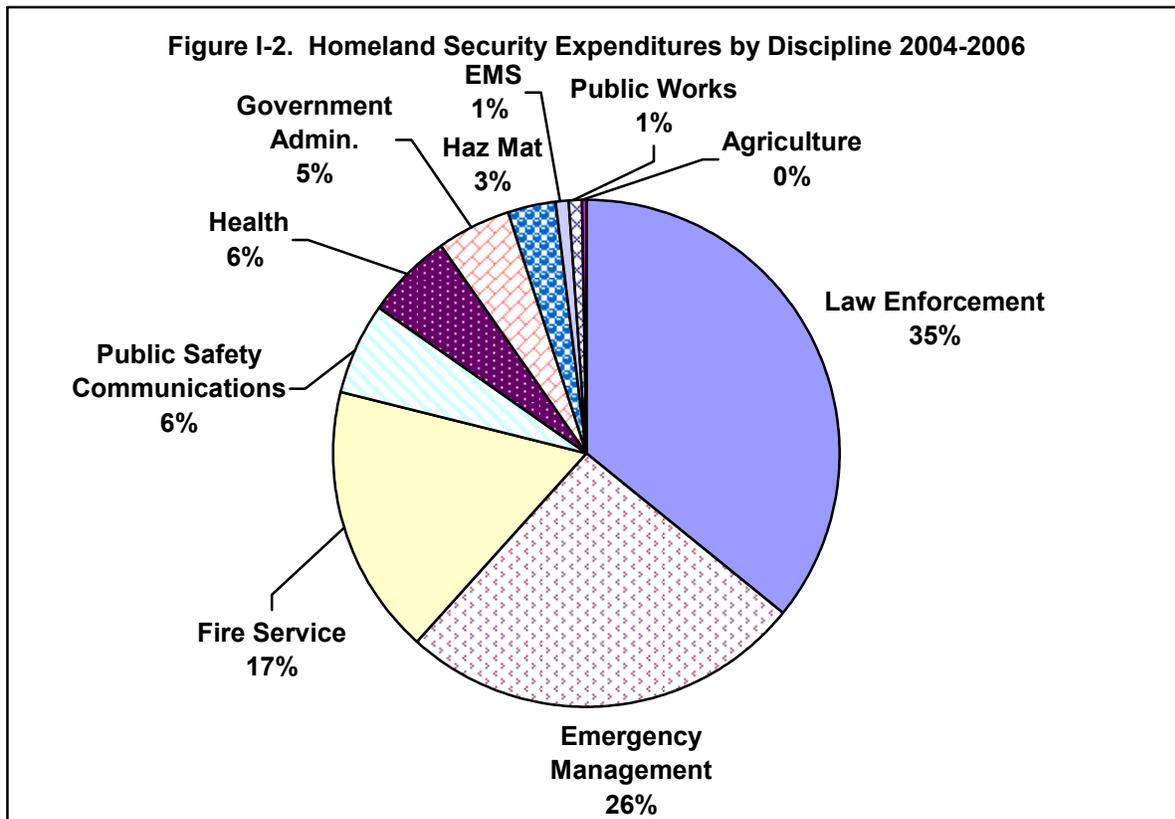
Examples of state and local purchases from federal homeland security funding are provided in Table I-4. The largest three project areas account for 77 percent of the funding and include:

- *Enhancement of Public-Private Emergency Preparedness Program.* At nearly \$24 million, this project comprises about 50 percent of funds spent. This project includes the purchase of computers, detection systems (e.g., radiation dosimeters), personnel identification/security systems, personal protective equipment, search and rescue equipment, site clean-up/decontamination equipment, traffic management, responder vehicles & trailers, generators, and equipment storage.
- *Develop/Enhance Interoperable Communications.* This program supports the development of interoperable communications and includes the purchase of portable radios, mobile radios, mobile data terminals, Computer Aided Dispatch systems (for individual towns and regionally), radio consoles, and repeaters to eliminate dead spots in jurisdictions.
- *Assess Vulnerability/ Harden Critical Infrastructure.* This program supports the purchase of equipment to better secure municipal structures and for the purchase of equipment to improve the ability of state and local law enforcement to surveil and protect critical infrastructure. This program does not include the buffer zone protection program funding, described above.

Table I-5. Homeland Security Expenditures by Sub-Program, FY 2004-2006	
Sub-Program Category	Amount
Interoperable Communications Equipment	\$ 12,454,357
Physical Security Enhancement	4,537,667
CBRNE Logistical Support*	4,206,247
Other Authorized Equipment	3,949,256
CBRNE Search and Rescue Equipment	3,437,542
CBRNE Incident Response Vehicle	3,403,558
Medical Supplies and Pharmaceuticals	1,983,718
Develop / Enhance Plans and Protocol	1,628,406
Intervention Equipment	1,606,527
Personal Preventive Equipment (PPE)	1,577,785
Terror Incident Prevention	1,532,592
Training Course / Program Development	1,211,252
Detection Equipment	1,037,344
Citizen Corps Public Education	781,298
Orange Alert Overtime	755,949
Explosive Mitigation / Remediation	503,723
Training Overtime	421,312
CBRNE Response Watercraft	390,945
Develop / Coordinate Plans & Programs	342,168
Decontamination Equipment	277,515
Exercise Program Development	266,842
Establish / Enhance / Evaluate Citizen Corps Program	222,125
CERT Team Responder Equipment	187,059
Develop or Conduct Assessments	145,526
Information / Investigation / Intelligence	126,758
Agricultural Terror Prevention Response	105,047
Exercise Overtime	101,689
Training Backfill	70,895
Cyber Security Enhancement	39,300
CBRNE Reference Materials	23,154
Exercise Backfill	15,142
Grand Total	\$ 47,342,698
* CBRNE = Chemical, Biological, Radiological, Nuclear, Explosive	
Source: DEMHS	

Sub-Program. Table I-5 shows homeland security expenditures by sub-program for FY 2004 through 2006. The four largest categories accounted for 53 percent of total funds expended. The largest categories are listed below along with the top expenditures in each category.

- *Interoperable Communications Equipment* - microwave towers and accessories, low power crossband/ multiband system, Connecticut State Police Emergency Radio Network, portable radios, and dispatch console.
- *Physical Security Enhancement* - access control systems, closed circuit television systems, and surveillance cameras.
- *Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) Logistical Support* - Geographical Information System project, electronic road alert signs, credentialing systems, generator, and command trailer.
- *Other Authorized Equipment* - Cots for sheltering and evacuation, generator for shelter, computer equipment for emergency operations center, military grade parks, and all-weather pants and liners for Joint Terrorism Task Force.



Discipline. Figure I-2 shows how homeland security funds for FY 2004-2006 have been expended by discipline. Of note is the wide range of disciplines who have received homeland security funding from the traditional public safety area to health, public works, and agriculture. As one would expect, law enforcement, emergency management, and fire service account for 78 percent of the total funding.

Critical Infrastructure Protection¹¹

It is well recognized that society is dependent on a reliable network of infrastructure in order for both the government and the economy as a whole to function normally. Certain social and economic activities, like the transportation of goods and people, banking, and the supply of electricity and water, are vital to the operation and security of the country. As discussed in the briefing, both the federal government and the state have a role in protecting critical infrastructure.

This section provides background information on the state's and the federal government's critical infrastructure programs, a descriptive overview of the state's critical infrastructure, an examination of the department's goals and objectives that relate to the protection of critical infrastructure, a comparison between the elements of an effective critical infrastructure program and DEMHS activities, and a comparison of the state's critical infrastructure list and the federal government's Buffer Zone Protection Program.

Background

In Connecticut, the Critical Infrastructure Protection Unit within DEMHS is responsible for identifying the state's critical assets, assessing the vulnerability of key sites, and developing mitigation strategies to reduce those vulnerabilities and improve the security at those sites. Ultimately, the purpose of critical infrastructure protection is to devalue a potential target by making it difficult to attack, deter an event from happening, detect an aggressor planning an attack, and defend against an attack. Infrastructure information is also used as part of a state risk assessment that directs funding to DEMHS regions to improve preparedness. The state's infrastructure list is also instrumental in being able to respond to federal data calls for infrastructure information when the federal government is interested in protecting specific types of assets or when certain threat information is received. There is no state program to assist in the funding of critical infrastructure upgrades for municipalities or for private facility owners.

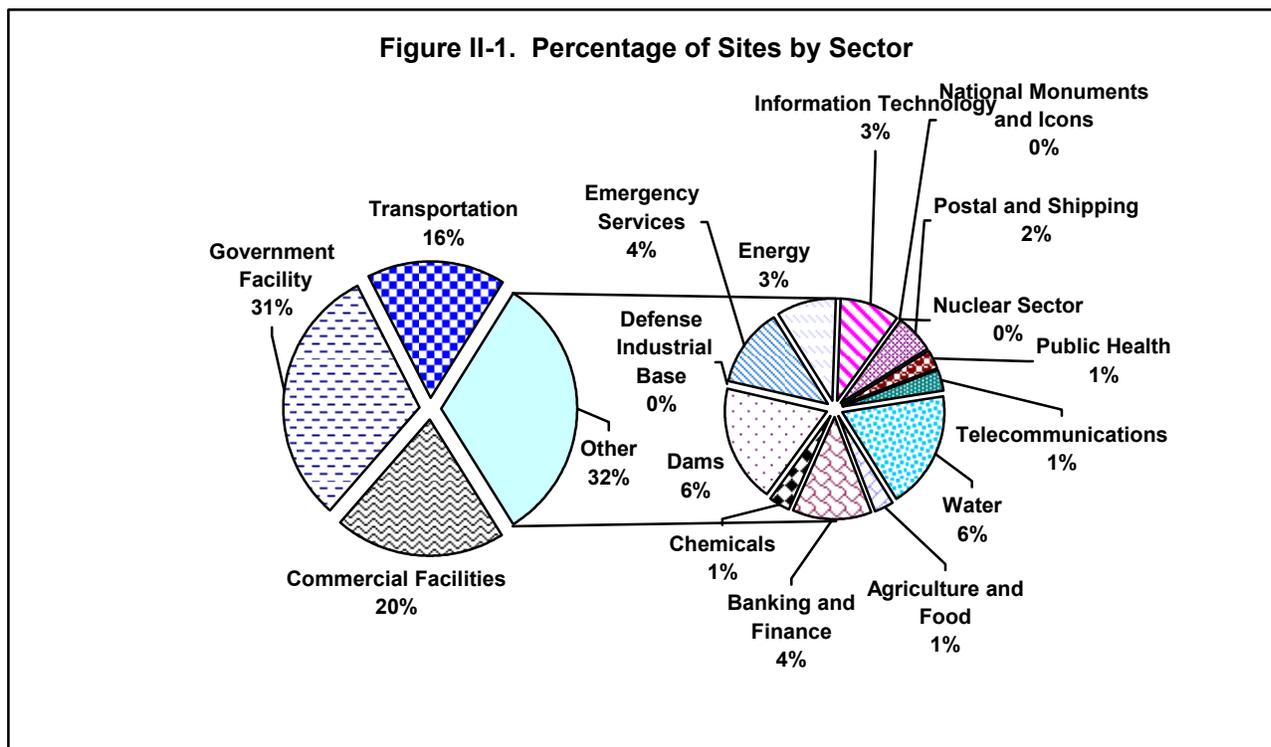
In general, the federal Department of Homeland Security has the responsibility to unify critical infrastructure protection efforts across the country through its National Infrastructure Protection Plan (NIPP). Through the NIPP framework, the federal government is developing ways to prioritize protection efforts and investments across the various infrastructure sectors. More specifically, the federal government also collects infrastructure information for its risk-based funding formulas and for its buffer zone protection program.

¹¹ The reference to critical infrastructure is meant to also include key assets. According to the USA Patriot Act of 2001, critical infrastructure includes those "systems and assets whether physical or virtual so vital to the United States that the incapacity or destruction of such ... would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Key resources are "publicly or privately controlled resources essential to the minimal operations of the economy and government."

The BZPP funding is intended to assist in developing effective measures that make it difficult for terrorists to conduct surveillance or to launch attacks within the vicinity of critical infrastructure, as well as increase the preparedness of local jurisdictions where the facility is located. The focus of buffer zone improvements is outside the perimeter of the identified infrastructure. Primary responsibility, though, for the protection, response, and recovery of the nation's critical infrastructure lies with the owners and operators. As identified in Section I, state and local governments are allowed to use federal homeland security funding for infrastructure upgrades for government-owned facilities, and about \$4.5 million has been expended for this purpose in Connecticut.

It should be noted at the outset that the federal buffer zone program has significant limitations. The program has been criticized for: 1) not providing enough money for mitigation activities, especially in the early years; 2) not allowing funding to be passed on to private sector facility owners for internal security measures or for capital expenditures, like fences and surveillance cameras; and 3) allowing local governments the final say over what gets purchased.¹² Program managers in Connecticut have noted that installing a fence around the perimeter of a facility may be more helpful in improving security at a particular location (a non-funded activity), than buying equipment for municipalities to better enable them to respond to an event at the facility (a funded activity).

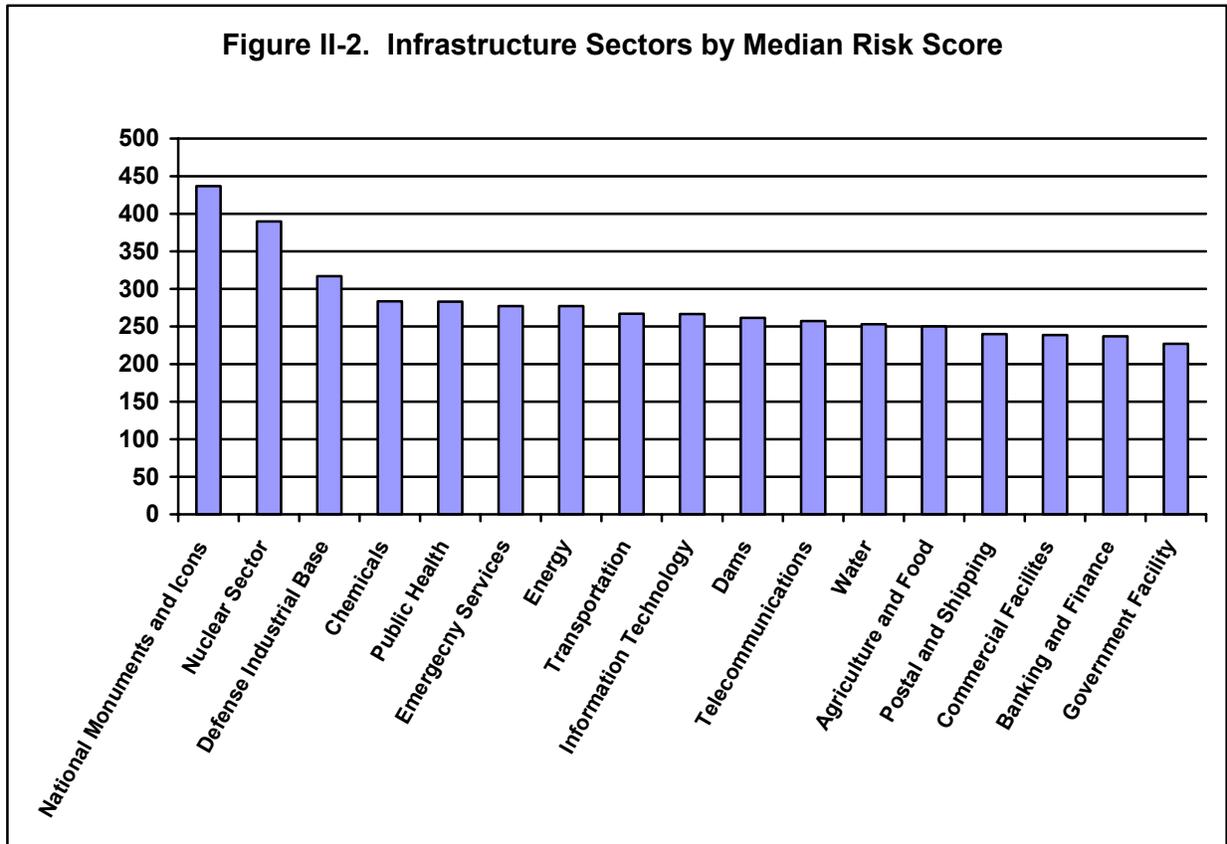
Descriptive Information Regarding the State's Critical Infrastructure



¹² See for example, U.S. Department of Homeland Security, Office of Inspector General, *Review of the Buffer Zone Protection Program*. Washington D.C. , July 2007

The current state infrastructure list is diverse and includes entries for each of 17 critical infrastructure types identified by the federal government. When program review staff began this review approximately 3,500 sites were contained in the database; by November 2007 less than 2,900 were in the database. In the last round of updates for critical infrastructure in 2006, the state’s critical infrastructure and key resources were cataloged largely in accordance with the latest DHS asset types and threshold limitations.

While the exact contents of the list remains confidential, program review staff worked with DEMHS to produce some aggregated descriptive information about the state’s critical infrastructure that did not compromise any security concerns. Figure II-1 shows the percentage of sites by sector. Government facilities, commercial facilities, and transportation sectors comprise about two-thirds of all critical assets, while national icons, nuclear sector, and defense industrial base are among the smallest sectors. (The smallest sectors do have facilities listed even though they appear on the figure as 0 percent.)



When the critical infrastructure sites are identified within each town, the information is entered into a risk assessment tool known as CARVER, which evaluates critical infrastructure across several factors. Each factor has various data points that must be entered so that a score can be generated. Each facility receives a total score and can be ranked and compared to every other facility. This process is described in detail below. The highest score that can be generated is 500. Figure II-2 shows the median risk score by infrastructure sector. National monuments and icons, the nuclear sector, and defense industrial base have the highest median scores, while

government facilities have the lowest. The principle reason that national monuments have the highest score is because they are considered irreplaceable at any cost.

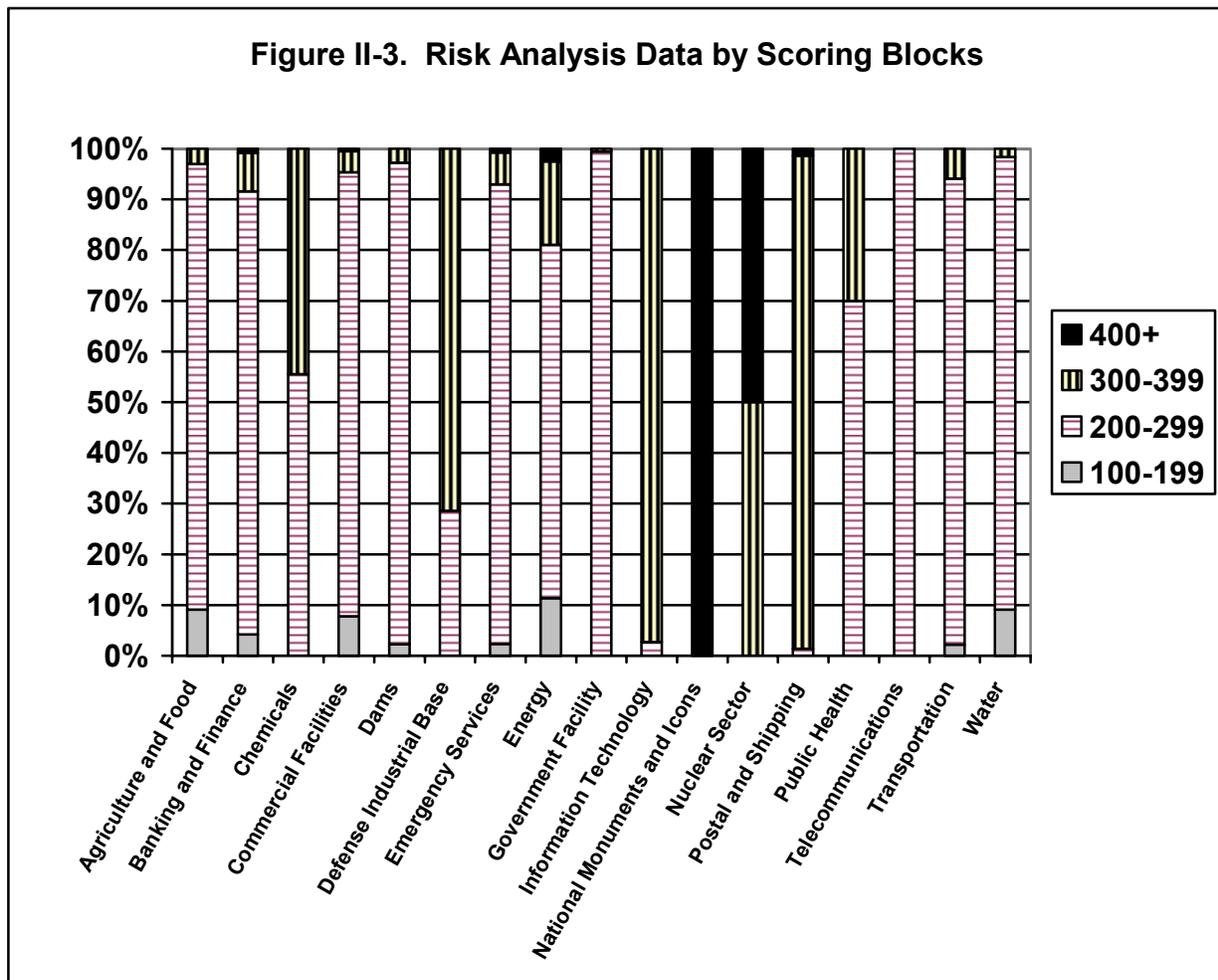
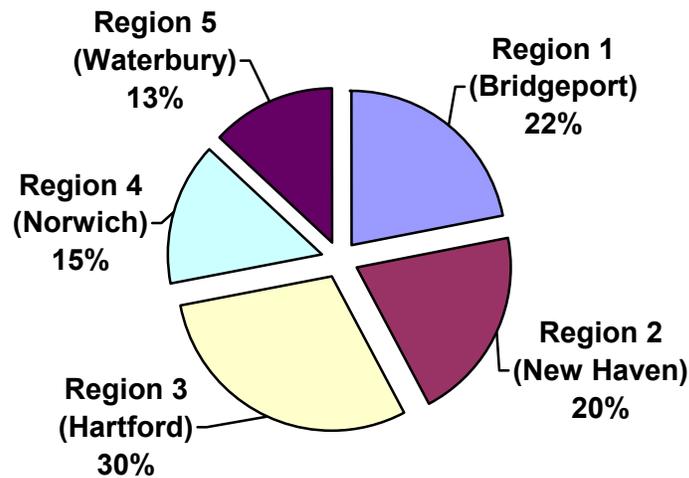


Figure II-3 shows critical infrastructure by scoring blocks. These scoring blocks show the percent of facilities that fall within a particular range of risk scores by sector. For example, for the water sector, 9 percent of its facilities fall within 100 and 199, 89 percent fall within 200 and 299, 2 percent fall within 300 and 399, and none fall in the range of 400 or more.

National monuments and the nuclear sector have the largest percentage of facilities that fall in the highest range. Other sectors with facilities that have high scores include the energy, commercial, and postal categories. Eighty-seven percent of all facilities fall within the 200 to 299 range, while less than 10 percent of all such facilities fall within the 300 to 500 range.

Figure II-4 shows the amount of critical infrastructure by region. As a reference point, the largest city in each region is also shown in parentheses. Region 3, which includes Hartford, has nearly one-third of all critical infrastructures; while Region 5, which contains Waterbury and Danbury, has the least (13 percent).

Figure II-4. Percentage of Critical Assets by Region



Goals and Objectives

Program review committee examined strategic goals and objectives regarding the critical infrastructure program contained in the State Homeland Security Strategies for 2003, 2006, and 2007 *as well as* related internal strategic goals and objectives for this area established by DEMHS. The SHSS is federally required and identifies planning, equipment, training, and exercise needs of the state to prevent, respond, and recover from acts of terrorism. The SHSS is developed in consultation with the Emergency Management and Homeland Security Coordinating Council and is required under federal grant guidelines. The latest SHSS published in 2007 has a time frame from 2007 to 2011. The department's internal strategic goals were promulgated by DEMHS in 2007.

The SHSS and DEMHS strategy documents establish two goals and a combined total of 12 objectives that relate to critical infrastructure.¹³ There has been one consistent overall goal regarding critical infrastructure contained within the State Homeland Security Strategies; "to enhance public safety through hardening of critical infrastructure sectors." DEMHS' strategic goal is to "continue the development of critical infrastructure plan for the state of Connecticut." The committee staff findings regarding the 12 objectives that support this goal are presented in the Table II-1. *In summary, five of the 12 objectives related to the protection of critical infrastructure have been completed, three of which are ongoing. Six other objectives are partially complete, and one objective is not yet started. (A complete list of the objectives and their status can be found in Appendix B.)*

¹³ The SHSS contains six objectives related to critical infrastructure. Three of the objectives have been in place for each of the three SHSS documents under review here; two additional objectives were added in 2006, and another one was added in 2007. The DEMHS strategic goals document contains eight objectives, but two of the objectives overlap with the SHSS. Combined, there is a total of 12 separate objectives.

Table II-1. Status of Objectives Related to Critical Infrastructure

Status	Objectives for Critical Infrastructure
Completed	<ol style="list-style-type: none"> 1. All of the state’s approximately 80 general aviation airports have been evaluated. (It should be noted that Bradley is not considered a general aviation airport and is currently being reviewed by the CIPU.) 2. A risk-based formula for determining regional funding amounts utilizing critical infrastructure information has been developed.
Ongoing	<ol style="list-style-type: none"> 3. A detailed inventory of the state’s critical infrastructure has been assembled and is maintained and updated by the critical infrastructure unit at DEMHS. 4. Critical infrastructure planning efforts are ongoing and being coordinated through various venues on the state, local, and federal level. 5. Terrorism awareness classes have been established for the public and private sector and are ongoing.
Partially Complete	<ol style="list-style-type: none"> 6. Mitigating strategies will be developed for the top 100 critical sites in Connecticut as they are assessed. DEMHS has assessed and local jurisdictions have implemented security or response improvements for 17 critical infrastructure sites that are eligible for funding under the Buffer Zone Protection Program for the first round of funding (FFY 2005). Plans are being developed for two sites in the second and third rounds of funding (FFYs 2006 and 2007), and no purchases have been made. 7. The Department of Information Technology (DOIT) has developed a risk assessment methodology and is in the process of conducting a risk assessment of the DOIT infrastructure. A documented report of the findings will be produced with required and recommended remediation activities. 8. DOIT has developed a draft incident response procedure that identifies methods to communicate with the key personnel throughout state agencies and defines roles and responsibilities associated with cyber-indent response procedures. 9. Background checks for certain DEMHS employees to obtain federal security clearances are in progress. 10. Regional plans are being developed that will integrate risk assessments. 11. A new position called an intelligence analyst is under development.
Not Yet Started	<ol style="list-style-type: none"> 12. The CIPU has not yet begun to develop infrastructure assessment guidelines to make available to the private sector.

Source: PRI based on DEMHS interviews

Basic Process Elements

In general, DEMHS has made progress in obtaining most of the basic elements of an effective critical infrastructure program. As noted above, the purpose of the infrastructure unit is to assist in the identification, prioritization of, and protection of critical infrastructure. Drawing from a variety of sources, the basic elements that define an effective program to identify and reduce vulnerabilities of critical infrastructure are listed below and are compared to DEMHS' activities.¹⁴

- *A lead entity to oversee and coordinate the critical infrastructure effort* - While DEMHS is the overall lead entity for coordination in the state, within the department, the critical infrastructure protection unit is responsible for managing this effort. The unit contains six state troopers (one sergeant and five troopers) who are on loan from the Department of Public Safety to DEMHS. The unit also represents the department at Infragard and other private sector outreach organizations.¹⁵ It lacks an overall strategy to protect infrastructure and clearly identify the department's role in assessing infrastructure and tracking protection efforts.
- *Ability to identify and prioritize critical infrastructure* – DEMHS has identified a process to identify and inventory critical assets based on federal criteria. The CIPU also aggregates and analyzes initial assessment results to prioritize planning efforts.
- *Capacity to assess risks and develop protection measures* - DEMHS has performed some assessments and identified protection measures for specific sites. The department has stated its intention to redistribute resources to each region to perform assessments. In addition, the department has trained 46 municipal police officers to enable them to perform assessments in their communities.
- *Effectiveness measures* – The department currently has not developed effectiveness measures and does not receive enough feedback regarding its activities to fully understand the impact of its efforts critical infrastructure program.

These elements are discussed in the context of the operation of the CIPU in detail below.

¹⁴ For example, U.S. Department of Homeland Security, *Target Capabilities List September 2007*. Washington D.C. and Glen Woodbury, Measuring Prevention, *Homeland Security Affairs*, Volume I Issue 1, Summer 2005.

¹⁵ Connecticut's Infragard chapter is a nonprofit voluntary organization that provides for a public/private sector partnership for the protection of infrastructure.

State's Critical Infrastructure: Identification, Prioritization, Assessment, and Protection

In conjunction with extensive interviews with CIPU personnel, program review staff reviewed the state's critical infrastructure program and its work on the federal buffer zone program to:

- understand the process and methodology that DEMHS uses to collect the data and prioritize the importance of infrastructure sites;
- obtain basic descriptive information about the state's critical infrastructure (provided above) and determine if the assets included appear to be reasonable and valid;
- examine how many assessments were performed and how associated recommendations to mitigate vulnerabilities were implemented;
- consider how the infrastructure list and ranking system impacts the regional funding formula; and
- determine how the state's critical infrastructure list compares or relates to the federal BZPP.

Identification and prioritization of critical infrastructure. Initially, the state's critical infrastructure list was developed in 2002 based on a data request from the federal government. It has been revised over the years using different criteria and most recently underwent a comprehensive update to reflect 2006 and 2007 federal asset types and thresholds. The asset types relate to the 17 infrastructure sectors and key resource types such as banking and finance, telecommunications, etc. Typically, the threshold criteria relate to some type of activity, size, or a volume measure related to the facility.

In the last year, DEMHS distributed its current infrastructure list to all municipalities to verify the sites were in their communities, still operational, and still considered critical. All chief elected officials in Connecticut were asked to designate a point of contact to review and revise the list of critical infrastructure within their respective jurisdictions. Based on this review and input, CIPU staff have refined and revised the number of sites in the database.

Prioritization. When the critical infrastructure sites were identified within each town, the information was entered into a personal computer-based risk assessment tool known as CARVER. This program is federally endorsed and evaluates critical infrastructure across several factors, including criticality (i.e., impact of the loss), accessibility, recoverability, vulnerability, "espionage" (i.e., recognizability), and redundancy.

Each factor has various data points that must be entered so that a score can be generated. For example, the number of facility users affected by the loss of a site and the economic loss and rebuild cost of each facility has to be entered as part of the criticality factor to generate a score. If the data are not provided, they must be estimated by CIPU staff. The multiple scores are placed in a decision matrix that calculates a "target ranking." In this way, each facility receives a total score and can be ranked and compared to every other facility. While the CIPU staff uses

federal threshold criteria as a basis to screen out inappropriate facilities from the state's infrastructure list, the staff also make exceptions for facilities that are "close" to those thresholds. If the municipality can make a convincing argument to CIPU staff, the facility is included.

Findings and recommendations. With regard to the process DEMHS uses to identify and prioritize critical infrastructure, the program review committee makes the following findings and recommendations.

Program review staff randomly reviewed the sites on the state's critical infrastructure list and did not find any sites that were unusual or apparently out of place. Staff randomly examined DEMHS' list of approximately 2,900 critical infrastructure sites. Staff questioned the inclusion of a number of sites, but DEMHS staff proved adequate justification for their inclusion. Of particular concern was identifying any unusual sites that have been criticized as part of the federal government's National Asset Database, such as petting zoos, landfills, and auto shops. While not every site on the state's list was reviewed by program review staff, similar concerns were not found.

The precise criteria for inclusion on the state's critical infrastructure list are not clearly defined and documented. While it may be desirable to expand on the federal threshold criteria for legitimate state purposes, it is unclear what the exceptions were or how consistently those exceptions have been applied. Given that the existence of critical infrastructure affects the amount of homeland security funding a region receives from the state, each municipality should know what the precise criteria are to ensure that all municipalities are responding to the same standards. Documented guidelines will also help to ensure a consistency of understanding among staff, assist with new staff orientation, and expedite any assessment of new infrastructure to be included on the list.

Recommendation. DEMHS needs to clearly document the critical infrastructure eligibility guidelines and provide that information to each municipality.

Nearly 56 percent of municipalities in Connecticut did not respond to the most recent data call for the critical infrastructure update. Ninety-four municipalities did not confirm or update the existing critical infrastructure list for their jurisdictions. Eighty-four municipalities have not appointed a point of contact for the risk assessment program. A number of the non-responders represent cities. While CIPU staff believe that they have captured most of the infrastructure information for those municipalities based on previous data calls, it is impossible to confirm because changes to infrastructure can occur when new businesses are created or when businesses cease to operate. DEMHS has also sent several letters from the commissioner to try to persuade municipalities to be more active participants. Program managers have speculated that the process may be perceived as cumbersome, and that municipalities, in the past, may not have received much feedback as to how the data are used. Because regional funding is tied, in part, to the identification of critical infrastructure, financial resources may not be directed to the appropriate regions as intended without accurate risk information.

Recommendation. DEMHS should encourage greater participation by municipalities in the infrastructure program by reinforcing with municipal leaders the

importance of the program and the impact it has on the funding of regional priorities. In addition, DEMHS should investigate the feasibility of providing an electronic means for municipalities to access and update infrastructure information through a secure internet portal.

The infrastructure assessment software tool has significant limitations and needs to be reassessed. The CARVER risk assessment software is provided to state governments free of charge and is used by 35 states, according to the manufacturer's website. DEMHS states that it had selected the CARVER program based on recommendations from the federal DHS and because it was the best available tool at the time of purchase several years ago. Program review staff have noted that the CARVER assessment tool makes it difficult to manipulate data and obtain various reports about infrastructure from the database. When CIPU staff make certain queries of the infrastructure data, they have indicated that the computer will "time out" before the run is completed. One solution is to download a portion of the information into another program, such as Excel, but this is not an optimal solution because of the time it takes. In addition the software does not include certain facility categories, such as public and private schools, which DEMHS would like to include and isolate from other categories.

Recommendation. DEMHS should investigate the use of other validated infrastructure assessment tools to better accommodate the categorizing, analyzing, and reporting needs of the department.

Assessment and protection of infrastructure sites. Part of the mission of DEMHS' infrastructure unit is to perform systematic assessments of the state's critical infrastructure and develop strategies to improve security at those sites. The unit is hoping that with the help of specially trained municipal police officers it will be able to work with the owners of the most critical facilities to assess vulnerabilities and develop plans to increase security at each site. Forty- six municipal officers have been trained to do assessments within their communities.

The unit also offers asset reviews at no cost to other government agencies and private entities who request such a review. To date, CIPU has assessed and developed mitigation plans for 180 sites, including:

- 90 private facilities;
- 20 ferry facilities;
- 22 state facilities; and
- 48 municipal sites.

Included within those 180 assessments are 42 of the state's top 100 most critical sites. The private and public (municipal and state) facilities also include rail, seaport, and airport facilities. The three major seaports in Connecticut have been assessed. In cooperation with the federal Transportation Security Administration, DEMHS initiated an airport security initiative targeting general aviation airports. The initiative includes security self-assessments and recommended guidelines that would help make the airports more security conscience.

Findings and recommendations. With regard to the infrastructure assessment process and protection activities, the program review committee makes the following findings and recommendations.

DEMHS has created a comprehensive general aviation airport evaluation initiative and it has recently begun a physical security assessment of Bradley International Airport. The assessment was apparently requested by the TSA's new federal security director for Bradley. The state Department of Transportation believes the review will provide an overall assessment of its ongoing efforts that have evolved since September 11, 2001. DEMHS has stated that it believes that Bradley has been well protected by a combination of entities, including the TSA, which is responsible for passenger and cargo security issues, the state police troop stationed there, and the state airport police.

Only a small portion of Connecticut's key infrastructure has been assessed to date. As mentioned above, 180 sites out of a potential 2,900 sites (6 percent) have been assessed by DEMHS. The function of state-sponsored infrastructure assessments, like the department itself, has only been in existence for a short period of time. In all likelihood, not all facilities on the list will receive an assessment. Some sites are important to know about, but it may not be cost effective for the state to assess the potential vulnerabilities at all sites. These facilities, for example, may have a redundant capacity or have a relatively small impact if disrupted compared to overall statewide effects. DEMHS has prioritized the list and will be concentrating on performing assessments based on its own risk analysis.

It is not clear how active DEMHS will be in performing critical infrastructure assessments, and ensuring mitigation activities are performed and business continuity plans are in place for the state's most critical assets. One goal that has been stated in this area is that DEMHS wants to assign resources to each region to perform assessments for the most critical and most vulnerable assets within each region. DEMHS would like to enlist the support of the 46 municipal officers they have trained to perform assessments in their communities. How this will be coordinated and implemented is not clear. A more specific implementation plan would be helpful indicating, among other items, what "the most critical" sites are (i.e., whether it is all 2,900 sites), what the responsibility of DEMHS should be versus the site owner in assessment and mitigation activities, strategies to encourage private sector cooperation with DEMHS, what the state's position should be if the owner is uncooperative, and whether and how DEMHS should track to see if continuity of operations plans are in place for the most critical assets.

No feedback is received from facility owners to know how many vulnerability mitigation recommendations are implemented. To understand how successful the infrastructure program is, two key metrics would be how many recommendations are implemented and what effect they have had in mitigating vulnerabilities. There is no requirement for facility owners to provide this information to DEMHS, nor does the department ask for it. While there may be some reluctance on behalf of private facility owners to provide that information, it is unclear why public sector organizations at least should not share with DEMHS what mitigation strategies have been employed. Understandably, given their limited resources, DEMHS has not performed any follow-up reviews to assess how well any changes that may have been implemented have improved security at these sites.

The department has estimated that 85 percent of the mitigation recommendations for facilities that they have assessed have not been implemented. Among the reasons cited for this are limited funding and a lack of authority to enforce security standards. Both DEMHS and representatives from the business community have indicated that security improvements for many facilities are costly and can be difficult to justify, especially for a low probability but high consequence event. The state does not provide any assistance for improvements and the amount of federal assistance is limited and is focused on improvements beyond the perimeter of the facility.

Some states, like New Jersey, have implemented minimum infrastructure security standards for certain facilities, like chemical plants. In addition, the federal DHS is in the process of promulgating regulations that require certain high-risk chemical facilities to comply with performance-based security requirements. Some controversy exists around the regulations because the universe of regulated facilities is not specified under the law and is left to the discretion of the DHS secretary. Some states have raised concerns that the federal standards would reduce the requirements enacted by state governments. Nonetheless, the principle of establishing security requirements is anticipated in the federal National Infrastructure Protection Plan. It states: “additionally, critical infrastructure /key resource owners and operators may be required to invest in security as a result of federal, state, and/or local regulations.”¹⁶ On the flip side of developing regulations, there may be merit in considering incentives to encourage certain facility owners to implement greater security protections. Incentives could take the form of grants, low interest loans, or tax breaks for improvements.

DEMHS staff have also noted uneven implementation of mitigating strategies around seaports in Connecticut. It is thought that the nature of the port authorities’ power may influence the extent to which recommendations are implemented. In addition, businesses make risk-management decisions based on a return on investment and ensuring business continuity. There may be, however, certain facilities or functions deemed to be critical to the state or have significant consequences that are not considered to be a part of normal private sector risk-management considerations. Smaller businesses or clusters of smaller business may especially find it difficult to justify increased investments in security or continuity planning. While DEMHS is still in the formative stages of infrastructure protection, the program may benefit from additional outreach into the private sector to understand barriers to providing improved protection at different levels of business.

Recommendation. To improve Connecticut’s infrastructure protection efforts and to better understand any barriers to reducing vulnerabilities in certain business sectors, DEMHS should:

- A. develop a specific implementation plan that outlines DEMHS intentions, goals, and responsibilities in assessing and mitigating vulnerabilities as well as in tracking the status of public and private sector security efforts at Connecticut’s most critical infrastructure sites;**

¹⁶ U.S. Department of Homeland Security, *National Infrastructure Protection Plan 2006*. Washington D.C., p 26.

- B. track core activity measures, such as, but not limited to, the number of assets, systems, and networks by sector, and the number of completed vulnerability assessments;
- C. develop a system to capture information about the usefulness of facility assessments performed by the department and the extent to which mitigating recommendations have been implemented by both public and private facility owners, including improvements made through grants awarded to ferry, port and transit operators in the state; other measures to consider include percentage of high-risk assets that have developed protective strategies, percentage that have implemented mitigation strategies, and percentage that have continuity of operations plans.
- D. report results of B and C in an aggregated and non-identifiable format in DEMHS' annual report; and
- E. convene a task force composed of coordinating council members, public safety officials, private sector facility owners, and other appropriate stakeholders to investigate the need for the regulation of security improvements or the development of incentives for certain critical infrastructure facilities, such as those that handle extraordinarily hazardous substances, transportation facilities, or other critical infrastructure.

Table II-2. Regional Risk Formula and Homeland Security Regional Allocations: FY 2007

	Number of Towns	Number of Assets	CARVER Total Regional Risk Score	Percent of Total Score	Total Risk-Based Allocation	Base Allocation	Total Allocation
Region 1	14	635	162,018	22.3%	\$238,479	\$800,000	\$1,038,479
Region 2	30	588	147,606	20.3%	217,266	800,000	1,017,266
Region 3	41	857	212,755	29.3%	313,160	800,000	1,113,160
Region 4	41	430	106,884	14.7%	157,326	800,000	957,326
Region 5	43	381	96,543	13.3%	142,104	800,000	942,104
Totals	169	2,891	725,806	100%	\$1,068,335	\$4,000,000	\$5,068,335

Source: DEMHS

Risk-based funding. The risk assessment process is important to Connecticut's municipalities because it has become an element in determining a portion of funding for each DEMHS region for FY 2007. This is similar to the federal government's use of risk-based methodologies to allocate funding under several of its grant programs among the states. DEMHS has allocated a base amount of \$800,000 to each of its five regions and an additional amount based on the CARVER risk assessment of the infrastructure in each municipality. The

sum of the “target rankings” within each municipality represents each municipality’s risk score. The total risk score for each DEMHS region was calculated by adding the scores of its constituent towns.

The risk-based funding amount for each region was calculated as a proportion of the region’s contribution to the statewide total risk score. Table II-2 shows the total scores and the total allocation for each region. Region 3, which includes Hartford, has received the most funding, while Region 5, which contains Waterbury and Danbury, has received the least.

Findings and recommendations. Regarding the process DEMHS uses to calculate its risk-based funding amounts, program review committee makes the following findings and recommendations.

The state’s critical infrastructure list has been used for funding decisions while still being refined. While the infrastructure list is dynamic, from September to November 2007 there was a 30,000 point decline in one region based on subsequent revisions made after funds were distributed. DEMHS maintains that the September score was a “picture in time” on that date, and the list is fluid. However, program review committee believes this is problematic because it is a fairly significant drop. For example, if the highest average score for the nuclear sector is about 400 or so points, this means that the 30,000 point drop would be equivalent to about 75 nuclear sector assets. The 30,000 point adjustment was nearly a 20 percent drop in points for Region One and resulted in a 5 percent gain in funding for the other regions.

The risk-based formula does not consider the preparedness needs of local jurisdictions. Currently, each DEMHS region, in association with the Regional Planning Organizations, is working on developing a number of items to strengthen regional collaboration and planning. These include:

- a standardized inventory of available emergency resources throughout the region;
- a Strength, Weakness, Opportunities, and Threats (SWOT) analysis (a planning tool to assist in evaluating a project) of each region’s emergency support functions (ESFs);¹⁷
- a regional spending plan to address needs in the region; and
- a regional emergency operations plan.

Each region is required to assess its own strengths and weaknesses for emergency preparedness and determine region-wide emergency preparedness priorities. The process is intended to be a bottom-up type of approach. This method clearly allows for variation and

¹⁷ The emergency support function (ESF) is defined by DEMHS as a “disciplined-oriented work group” intended to “foster collaborative planning within a particular discipline.” There are 15 emergency support functions, and each would have some type of subcommittee representation or acknowledgement at the regional level. For example, municipalities have different local law enforcement agencies. Under the ESF concept, these law enforcement agencies all function as one under ESF-13. Some ESFs may be state-level functions, such as Urban Search and Rescue, and would not require a subcommittee at the regional level.

flexibility to address regional needs as defined by the region. However, while each region will have different strengths and weaknesses, it is not clear that each region will meet some type of minimum or common standard of preparedness. Given the strengths of multi-disciplinary and inter-jurisdictional cooperation, something akin to minimum standards or response capabilities may be the natural result of the current processes. However, if this is not, the question of minimum capacities may have to be addressed directly by the department.

Even without a minimum standard to aim for, the funding formula does not weigh the preparedness needs of one region compared to the needs of another. For example, Region A could be receiving funding based on the existence of a chemical plant in its jurisdiction. Region A may decide that there are sufficient local resources to deal with any problems with the chemical plant, and it could then use that money to address other needs it has identified. But these other needs may be of a lower priority when compared to the needs of Region B that does not have a chemical plant and is struggling to meet basic preparedness necessities.

The logic of the current risk-based formula hinges on equating the existence of critical infrastructure in a municipality with the needed level of preparedness of local governments and regions. It is not at all clear what action the municipalities or regions will or should take to lower the vulnerability scores of private facilities in their towns. The point of homeland security funding for the regions is to increase their preparedness for and response to terrorist acts and other emergencies. The bulk of the funding goes to aiding first responders who can reduce the life loss and the extent of damage to facilities. While that is an important core responsibility of emergency management, it only relates in small part to the total CARVER overall risk score.

The current needs assessments may not provide adequate information about the status of statewide preparedness for planning purposes. The needs assessment to be completed this year will rely on each region to perform its own SWOT analysis. The quality and thoroughness of this analysis will depend on the number and type of first responders and other specialists in each region who will come to the table to identify the various strengths and weaknesses in their current preparedness efforts. The SWOT analysis, while helpful in many aspects of project planning, may be insufficient in systematically identifying gaps in preparedness activities. A comprehensive preparedness analysis can be a complex, technical, and data-driven exercise.

A SWOT analysis was used in the 2007 federal homeland security grant process. Stakeholders developed 25 strengths (preparedness elements to maintain) and 25 weaknesses (preparedness elements to improve) based on their own experiences and expertise. No comprehensive assessment of what effect a plausible catastrophe, like those outlined in the 15 federal planning scenarios,¹⁸ would have on Connecticut currently exists. While some regions have had the benefit of a natural disaster hazards assessment through prior grants from the Federal Emergency Management Agency (FEMA), no comprehensive assessment of risks to the state has been conducted.

¹⁸ The 15 national planning scenarios (NPS) highlight the scope and complexity of plausible terrorist attacks or major disasters (12 are terrorist-related scenarios, such as a chemical or radiological attack, and three are natural disasters, such as a hurricane). The NPS are intended to be a reference resource to government agencies to help evaluate and improve capabilities.

Recommendation. In conjunction with the risk-based funding methodology, DEMHS should consider adjusting the regional funding formula to include a factor or factors that take(s) into account the preparedness needs of each region as initial regional organizational objectives are met. In developing the information about preparedness needs, DEMHS should conduct a comprehensive all-hazard risk and vulnerability assessment of large scale disasters and catastrophes that can plausibly be expected to occur in Connecticut to assist in identifying the individual needs of regions.

Clearly, bringing together diverse, multi-disciplined professionals to establish emergency management planning and preparedness regions is a monumental task that DEMHS has taken on. It is understood that the initial activities, such as the SWOT analysis and regional operations plans, will aid in unifying each region to achieve a common goal. However, in the near future, additional refinements and more technical levels of assessment will be necessary to direct the ever diminishing resources to the right regions.

Buffer Zone Protection Program Comparison

The program review committee asked staff to compare the state's critical infrastructure list with the sites that are considered critical under the federal government's Buffer Zone Protection Program. Staff examined the state's complete critical infrastructure list, the list of the federally funded buffer zone sites for 2005 through 2007, and the lists of buffer zone sites that were eligible for funding in 2006 and 2007 but not selected by DEMHS because of limited federal financial support. Staff reviewed the lists to:

- determine how the federal government selected BZPP sites for eligibility and compare them to the state's ranking of the sites;
- establish how the DEMHS commissioner selected which sites would receive BZPP funding; and
- verify how many recommendations were implemented.

The specific criteria that the federal DHS uses for determining which critical sites to fund through its buffer zone protection program have not been made available to the state. Based on a review of sites deemed eligible for funding under the BZPP, the formula appears different from what the state uses for the creation of its list and priorities. In the first year of the BZPP -- 2005 - 17 Connecticut sites qualified for funding under the program. Eleven sites were originally identified by DHS, and the state recommended additional sites to DHS and got six sites added. The committee found that the original 17 federal buffer zone program sites are contained within the top 100 sites considered critical by DEMHS and are consistent with the state's priorities. Program managers have speculated that DHS uses more specific and updated threat information to select its priority sites.

In 2006 and 2007, DHS presented DEMHS with a list of sites it considered critical and allowed the state to pick one site for each year to receive funding. *The committee found that many of the choices DHS presented to DEMHS to fund under the federal buffer zone program for 2006 and 2007 were not within the top 100 sites considered critical by DEMHS; however, the*

commissioner selected sites that were consistent with the state's priorities. The DEMHS commissioner chose facilities in those years that were part of the original 17 sites, so that those sites would receive additional funding. The commissioner's rationale was that the original funding from 2005 was insufficient to complete necessary security improvements. It was believed that it was better to try to complete the work begun in 2005, rather than partially fund other sites. The amount of grants to jurisdictions is relatively small and is limited in the type of improvements that can be done. In 2005, the amount of funding was \$50,000 per site; in 2006, it was \$189,000; and in 2007, it was raised to \$194,000.

Buffer zone site assessment and protection. Once a site is determined to be eligible for the BZZP, a risk/vulnerability assessment must be conducted and a protection plan must be developed that identifies measures that will reduce the risk of a successful terrorist attack. To date, of the 17 sites requiring 19 plans, 17 buffer zone plans have been approved by DHS, and 16 plans have been implemented (meaning the equipment has been purchased and put into place). While DEMHS performs the assessments and makes recommendations, local law enforcement officials select which improvements to implement to increase the level of protection. According to DEMHS, all of the primary recommendations have been implemented from the 16 plans and the local jurisdictions have purchased equipment that the municipalities believe would best improve their ability to protect the sites.

Recommendation. Similar to the recommendation above, DEMHS should develop a system to capture information about the usefulness of the buffer zone protection program assessments performed by the department and the extent to which mitigating recommendations have been implemented and report the results in an aggregated format in DEMHS' annual report.

Connecticut Intelligence Center

Successful counterterrorism efforts require the coordinated efforts of federal, state, tribal, local, and private sector agencies. Together, these entities must create an integrated and standardized network to share information to ensure that a multitude of classic stovepipe operations do not exist. This integration concept is known as fusion.

The Connecticut Intelligence Center is part of the fusion endeavor to produce a collection of information from various sources, analyze the information to develop actionable intelligence, and share the intelligence across jurisdictional and disciplinary lines. This multi-agency center is currently located at the FBI's Connecticut office in New Haven.

Although the federal government has recognized the importance and necessity of intelligence and information sharing, guidance in this area only recently emerged. In 2006, the federal Department of Homeland Security and the Department of Justice (DOJ) collaborated to develop fusion center guidelines. The following section examines CTIC's adherence to some of these guidelines as well as the status of its goals and objectives.

Mission statement. According to the federal government, "a fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources."¹⁹ The federal guidelines recommend developing a mission statement and identifying goals for the fusion center. The fusion center's mission statement must be clear and concise and convey the purpose, priority, and role of the center.

The current CTIC mission statement revised in May 2007 is presented below. As the mission statement reveals, the purpose of CTIC is to serve as the focal point for collection, analysis, sharing, and dissemination of information relevant to threats or attacks of a terrorist or criminal nature within and against the state of Connecticut, its citizens, or its infrastructure.

CTIC Mission Statement

The Connecticut Intelligence Center is the primary multi-agency intelligence operation representing various jurisdictions. CTIC serves to collect, analyze and disseminate both criminal and terrorism-related intelligence to all law enforcement agencies in the State of Connecticut. The CTIC takes an all crimes approach to intelligence. The CTIC will also endeavor to identify emerging threats or crime trends and serves as a statewide central resource to effect intelligence sharing. CTIC is Connecticut's primary Fusion Center.

¹⁹ Department of Homeland Security and Department of Justice, *Fusion Center Guidelines* (August 2006), p.2.

Goals and objectives. The CTIC policy board, which is chaired by the DEMHS commissioner, has established eight goals regarding intelligence and information sharing. *Overall, most of the basic objectives related to establishing an intelligence center in Connecticut have been met.* These goals, along with the status level assessed by the program review staff, are presented in Table III-1. As the table shows, *two of the eight CTIC policy goals have been completed; two goals are partially met; and four goals are ongoing.* Further discussion of these goals is provided throughout this section.

Table III-1. Status of CTIC Policy Board Short-term Goals	
Status	CTIC Policy Board Short-term Goals
Complete	<ol style="list-style-type: none"> 1. Intelligence Liaison Officers (ILOs) have been identified and assigned in all law enforcement agencies. 2. Each DEMHS region has a designated Regional Intelligence Officer (RILO).
Ongoing	<ol style="list-style-type: none"> 3. Various efforts continue to maintain and enhance communications with law enforcement agencies including publishing weekly bulletins along with other products and holding conferences. 4. CTIC has established relationships with a wide range of organizations including DHS, FBI, and the private sector (Infraguard) as well as others that will be useful as information sources to contribute to intelligence networking. 5. Currently, teleconferences with other national organizations occur on a bi-weekly basis, allowing participating organizations to share and exchange intelligence products and minimize duplication. 6. CTIC continues to be involved in the collection, analysis, and dissemination of intelligence with emphasis on detection and prevention of criminal, gang, or terrorist activity.
Partial	<ol style="list-style-type: none"> 7. Discussions with the Connecticut State Police have begun regarding the establishment of a computer link to New England State Police Information Network (NESPIN) as the central platform for secure and timely information collection, analysis, and dissemination throughout the state and nation. Further progress is anticipated when CTIC relocates to the Hartford headquarters. 8. Work is underway to ensure connectivity with the Homeland Security Information Network (HSIN- unclassified) and the Homeland Security Database Network (HSDN –classified).

In addition to the CTIC policy board goals, the program review committee examined the goals and objectives regarding CTIC contained in the State Homeland Security Strategies for 2003, 2006, and 2007, as well as the related internal strategic goals and objectives for this area established by DEMHS. A full listing of these goals is provided in Appendix B.

The SHSS and DEMHS strategy documents establish one consistent goal in this area and that is to “enhance intelligence capabilities.” The committee findings regarding the seven objectives that support this goal are presented in Table III-2. As the table shows: *one of the seven objectives regarding intelligence and information sharing has been completed; four objectives are ongoing; one objective is partially completed; and one has not yet started.*

Status	Objectives for Intelligence and Information Sharing
Completed	1. Standards and security protocols for intelligence information have been developed and adopted.
Ongoing	2. CTIC has most of the components of a fully functioning fusion center. Certain aspects such as partnerships with multi-disciplines (fire, health, and medical) are evolving. 3. CTIC, in conjunction with other law enforcement and intelligence agencies including the FBI, continue to identify and address terrorist threats and activities. 4. JTTF continues to operate both a domestic and international unit. 5. The Homeland Security Information Network is operational and has been made available to various first responder groups.
Partial	6. One objective is to establish a 24-hour watch desk to serve as a single point of contact for state assets that will monitor international, national, and state incidents. Currently, the Connecticut State Police Message Center provides CTIC with 24-hour coverage. DEMHS anticipates operating its own 24-hour watch desk as part of the relocation of CTIC to its Hartford headquarters.
Not yet started	7. Compliance with the Federal REAL ID Act to standardize the requirements and procedures for state-issued driver’s licenses and identification cards awaits further guidance from the federal government.

Governance. The federal guidelines recommend creating a representative governance structure that includes law enforcement, public safety, and the private sector. The governing body should be composed of high-level officials who have the power and authority to commit their respective agency resources and personnel to the center. In addition, the guidelines suggest collaboration with the federal efforts of the Joint Terrorism Task Force (JTTF), the Attorney General's Anti-Terrorism Advisory Council (ATAC), the U.S. Department of Justice, and the U.S. Department of Homeland Security.

CTIC has instituted a governance body that contains representatives from a range of disciplines. CTIC's 12-member policy board was established through a memorandum of understanding among its members and currently includes:

- the commissioner of DEMHS, as chair of the CTIC board;
- the special federal agent in charge for the New Haven FBI field office;
- the commissioner of the Department of Public Safety;
- the deputy commissioner/colonel of the Department of Public Safety;
- the president of the Connecticut Police Chiefs' Association;
- the host police chiefs of the five regional intelligence liaison officers;
- the captain of the U.S. Coast Guard for Sector Long Island Sound; and
- the commissioner of the Department of Correction.

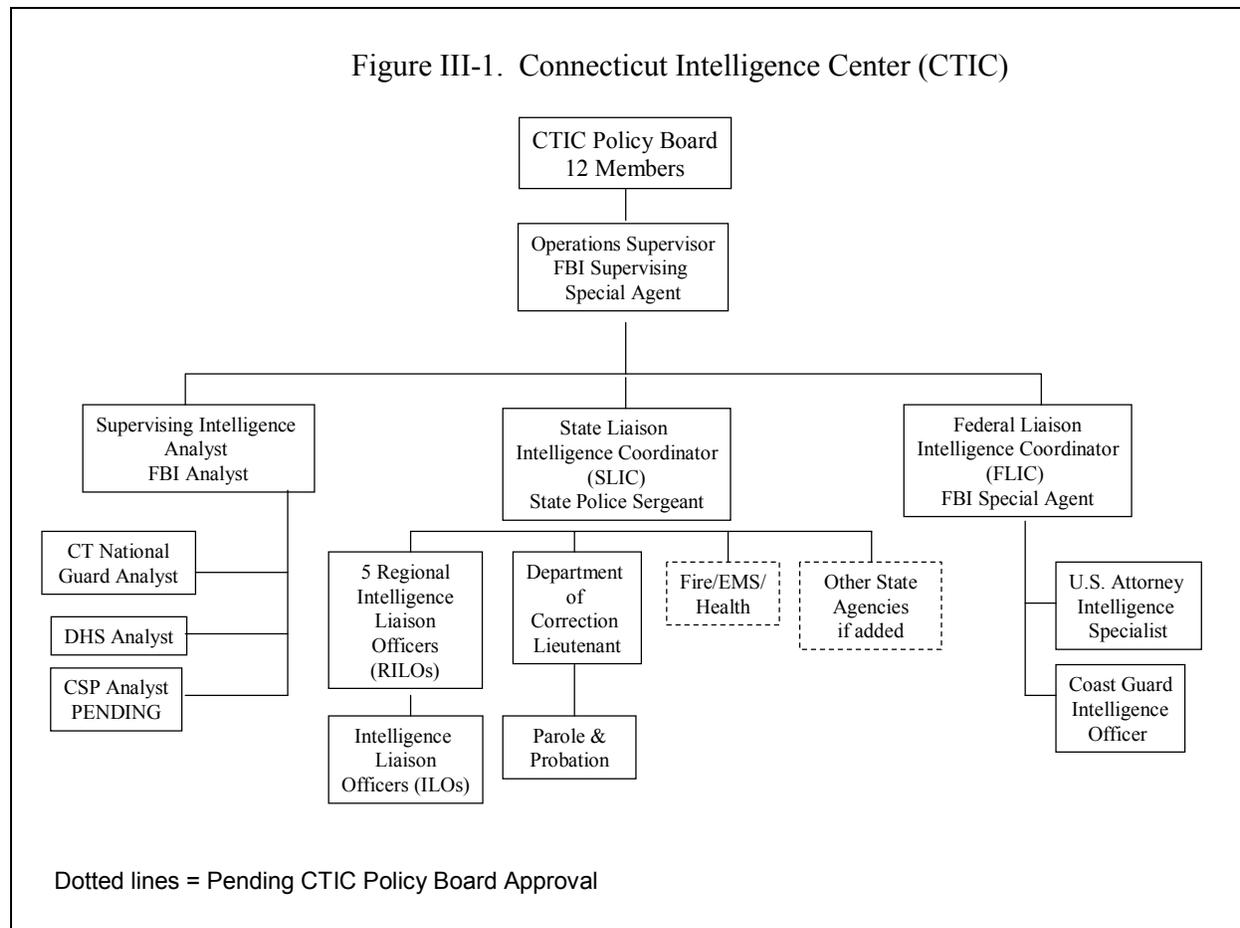
In addition, *collaborative efforts with the JTTF, ATAC, DOJ, DHS and others have been established and are on-going.*

Current CTIC staffing. The CTIC focus is an all-crimes approach with an emphasis on terrorist-related criminal intelligence. According to national experts, support for and acts of terrorism most often take the form of traditional crimes. Therefore, all crime activity should be analyzed for any nexus to terrorism such as narco-terrorism. As such, CTIC partners with law enforcement entities such as the FBI and the Bureau of Criminal Investigations within the Connecticut State Police. However, CTIC was not intended to replace or duplicate the counterterrorism duties of the FBI or investigative duties of the state police.

The CTIC operations supervisor is a supervisory special agent of the FBI who facilitates and coordinates the exchange of intelligence with the appropriate members of the national intelligence community. As Figure III-1 shows, the center includes several federal, state, and local law enforcement personnel working side by side to develop leads and solve cases. CTIC is connected to every local law enforcement agency by intelligence liaison officers who report to regional intelligence officers who in turn report to a State Liaison Intelligence Coordinator (SLIC). The SLIC is a supervisory representative from the Connecticut State Police (CSP). This is a full-time position with a two year minimum commitment.

The center is also staffed by individuals with subject matter expertise from law enforcement and state agencies such as the Department of Correction who work together to develop a complete picture of the state's current situation as well as an indication of future or

potential threats. All of the personnel assigned to these units are screened for the necessary security clearances allowing for a coordinated and collaborative exchange.



Program review staff interviews with various CTIC representatives revealed two administrative staffing issues. Currently, the five RILOs are appointed by the Connecticut Police Chiefs Association while the ILOs are appointed by the police chief of their local department. CTIC reports that all RILOs and ILOs have been assigned. However, *these appointments are voluntarily made by the police chiefs and there is no statutory requirement for municipalities to cooperate with CTIC. To formalize these appointments and ensure continued cooperation, program review committee recommends the appointment of ILOs and RILOs shall be codified into statute. Furthermore, the number of ILO appointments should be relative to the size or population of the community.*

The second issue involves the reporting structure for the state liaison intelligence coordinator. As noted above, this position is filled by a supervisory representative of the Connecticut State Police who reports to the head of the CSP Bureau of Criminal Investigations and ultimately to the commissioner of DPS. Within the context of CTIC operations, this position reports to the operations supervisor who is a federal supervisory special agent. However, as a

state entity CTIC is technically under the auspices of DEMHS within its Division of Counter Terrorism (also supervised by another CSP representative). As such, *the state liaison intelligence coordinator position has multiple reporting structures.*

Officials of the various reporting structures state that the current configuration has not presented problems or conflicts. While this may be the case presently, the program review committee believes **formal clarification regarding the reporting structure for the state liaison intelligence coordinator position is needed.** DEMHS and DPS were statutorily required to enter into an interagency memorandum of understanding regarding the assignment of personnel for homeland security purposes. Despite multiple requests, program review committee was unable to obtain a signed copy of this agreement. This issue is pursued further in Section V.

Partnerships with other disciplines. The fusion center guidelines issued by the federal government recommend the involvement and participation of all levels of government and private sector enterprises in order to identify the intelligence gaps. Ideally, the most effective of fusion models include multi-level (local, state, federal), multi-disciplinary (law, fire, health, emergency management) participants who can blend all perspectives into a complete picture of threat, risk, and vulnerability.

In Connecticut, CTIC has traditionally been a law enforcement-driven endeavor. As noted above, the FBI, the federal Department of Homeland Security, and Connecticut State Police as well as local law enforcement officials are essential partners that need to be linked with the state intelligence center. However, one benefit of creating a fusion center is derived from the partnership of staff from agencies and jurisdictions drawn from a broader range of disciplines.

One of the DEMHS goals is to expand CTIC to a fully functioning fusion center by incorporating other public safety disciplines such as fire and public health. Having more than just law enforcement focus, CTIC could use its diversity to capitalize on the cooperation and collaboration of a vast information and intelligence network. The inclusion of other disciplines such as fire and public health would allow CTIC to view the terrorism problem from additional points of view. As Figure III-1 illustrates, the CTIC policy board is considering inclusion of other disciplines.

CTIC also builds an expanded network through a partnership with the private sector and the operators of critical infrastructure facilities. The Connecticut chapter of Infragard, the largest chapter in the nation, is the state's link to the private sector. According to Connecticut Infragard, a strong working relationship exists with the DEMHS commissioner who is the chair of CTIC. The commissioner or his designee frequently attends Infragard meetings, and members of the department's Critical Infrastructure Protection Unit serve as the state homeland security coordinators for Infragard. DEMHS also reports a conference will be held in March 2008 for further private sector involvement.

The private sector can offer CTIC a variety of resources such as expertise in various industry specific subject matters such as cyber security or information regarding certain private sector operations that may assist with risk assessments. The private sector can also provide suspicious incidents and activity information or information that relates to critical infrastructure

that may be targets for terrorism. It should be noted that collaboration efforts may be hampered because the private sector may not want to disseminate certain information such as trade secrets critical to a business operation, proprietary information such as customer lists, or sensitive security information like site plans.

Program review committee finds *DEMHS has established a good working partnership with the private sector through Infragard*. However, Infragard is only one avenue to the private sector. Program review committee recommends **DEMHS further expand its private sector outreach efforts particularly to small businesses and security personnel of major critical infrastructures**.

Standards and protocols. The federal guidelines advise fusion centers to develop and adhere to standards and formal protocols (policies and procedures). CTIC has adopted a policies and procedures manual covering a range of items including an outline of the roles and responsibilities of all parties involved. The manual also addresses the receipt and flow of information, the types of intelligence products to be used, and the training of CTIC personnel.

CTIC also adheres to federal regulations that are aimed at law enforcement entities that operate federally funded, multi-jurisdictional criminal intelligence systems (28 CFR Part 23). These regulations relate to the collection, access, storage, and dissemination of information. It states, among other things, that databases (manual or electronic) shall be located in a physically secure area that is restricted to designated authorized personnel. The CTIC board has also developed policy in accordance with the federal Privacy Act of 1974 (Title 5 U.S.C. 552).

Program review committee finds CTIC developed a basic framework for various policies and procedures. Supplemental revisions may be required as state and federal law evolves in certain areas such as privacy.

CTIC Information and Intelligence Process

In general, the CTIC process is to capture investigative information, gather intelligence from all sources, and analyze the information. The information is then synthesized into a usable product for decision-makers. Products, including advisories, bulletins, alerts, and warnings are then disseminated as deemed appropriate.

Data collection. There is no single source for terrorism-related information. Terrorism-related information may come through the efforts of federal, state, tribal, and local law enforcement authorities; other government agencies (e.g., transportation, health care); the private sector (e.g., financial, internet/information technology); and by people living and working in local communities. CTIC personnel receive information through a variety of formats including a telephone hotline, homeland security websites, news media outlets, public records, publications, mail, e-mail, fax, and in person.

Each information lead must be evaluated as to source reliability and content validity. The RILOs and ILOs are the personnel assigned and responsible for intelligence gathering, source development, fostering relationships and ongoing liaison with all information sources and investigative agencies to access criminal intelligence. Any information developed by the ILOs is

communicated to their respective RILO. The RILO will collate all the information, cross reference it with information collected by other RILOs, and check it against federal and other pertinent databases. The CTIC SLIC coordinates and oversees all intelligence received from the RILOs and submits it to the operations supervisor for any further data analysis.

Program review committee finds that a regional information collection structure has been established and methods to exchange information are in place.

As referenced above, the state operates a toll-free Terrorism Tips Hotline that can generate leads through suspicious activities reported by the public. Currently, the hotline is staffed by the Connecticut State Police Message Center on a 24-hour basis. However, committee staff was informed that *statistics regarding the Tips Hotline do not exist because they are not collected or tracked.* **The program review committee recommends basic statistical information regarding the Tips Hotline should be generated (i.e., the number of calls received and the outcome of the calls) and provided to the members of the CTIC policy board on a periodic basis. In addition, the annual number of hotline calls received should be reported on the DEMHS website and its other various public relations materials.** The committee believes this information should be easily attainable and may provide decision makers with some measure of effectiveness of public awareness. At a minimum, publicizing the annual number of calls received may help reinforce the importance and potential success of this community based approach.

Data analysis. All incoming information must be properly documented and managed so that any valid indicators of actual terrorist activities and/or attacks can be recognized and referred for preventive action and consequence management as quickly as possible. The CTIC operations supervisor, in conjunction with the federal intelligence analyst coordinator assigned to CTIC, is responsible for monitoring trends and potential activities that provide indications that a terrorist incident may occur.

The operations supervisor assigns intelligence and analytical projects to CTIC personnel as appropriate. Currently, intelligence analysts from the FBI, DHS, and the Connecticut National Guard are used to support intelligence and analytical functions conducted by CTIC. These analysts assess information from a variety of sources, including open sources and classified material. The analysts look for any patterns of activity occurring over time that appear as developing or existing trends. The analysts contribute to the intelligence reports and when appropriate their findings are published for statewide law enforcement distribution. The analysts, along with other law enforcement personnel, try to identify any potential terrorism link in other criminal activities being investigated. These results can produce strategic and action-oriented intelligence data for the benefit of policy makers, administrators, and managers.

It should be noted that “results” are rarely immediate. Pieces of information from all perspectives are most often retrieved and shared one small piece at a time. This type of data analysis entails sorting, combining, categorizing, and arranging the data collected so relationships can be determined. It is not an exact science and sometimes it just results in more information. As such, this function is time-consuming in an environment that can sometimes be time-sensitive. Program review committee staff discussions with various CTIC and federal

representatives indicate that *the current intelligence analyst staffing level is inadequate*. As the organizational chart in Figure III-1 shows, there are currently two analysts (one DHS and one National Guard) and one FBI supervising analyst assigned to CTIC. Whenever feasible, the FBI provides additional resources, but they report also experiencing staffing constraints. According to CTIC officials, a state intelligence analyst position is in the process of being created. Job specifications are now being developed at the Department of Administrative Services for a CSP position.

The program review committee believes *data analysis is a critical component of the fusion center function that should be supported with adequate levels of resources*. Analysis transforms raw data into products that are useful. The analysis function separates information from intelligence. Without analysis, the data collection is merely disjointed pieces of information to which no meaning has been attached.

Data dissemination. Once data analysis has been completed and information assessed, a determination must be made as to what persons and/or organizations should be notified and by what means. General dissemination policies are contained within the CTIC policies and procedures manual that address the flow of information both within and outside the agency. The operations supervisor determines the priority of information dissemination. The SLIC serves as the intelligence sharing conduit between CTIC and all state agencies. CTIC maintains a list of telephone numbers, pager numbers, and email addresses for officials and designated points of contact for most of Connecticut's federal, state, and local public safety agencies.

Terrorism intelligence information is disseminated to members of CTIC participating agencies when there is a need to know and a right to know the information in the performance of their duties. The right to know means the recipient has the legal authority to obtain the information pursuant to court order, statute, or decisional law. The need to know means the requestor had the need to obtain information to execute official responsibilities.²⁰

CTIC produces weekly intelligence briefings that are distributed electronically to law enforcement and others like fire chiefs, fire marshals, emergency managers, and health directors who work in the field. CTIC also distributes terrorism intelligence assessments and bulletins and other assorted reports for state and local law enforcement and public safety agencies, homeland security officials, and other need-to-know entities.

Federal guidelines for fusion centers recommend leveraging databases, systems, and networks available through participating entities to maximize information sharing. Jurisdictions employ a number of mechanisms to share terrorism-related information. The FBI, DHS, and other intelligence agencies use secure electronic communications systems to disseminate terrorism intelligence/threat information to state and local stakeholders. These systems include:

- *Regional Information Sharing Systems (RISS)* – a secure web based communications system that is managed through six regional centers across the country, funded and overseen by various federal agencies. RISS is available to local, state, and federal law

²⁰ U.S. Department of Justice, *National Criminal Intelligence Sharing Plan Glossary* (2003)

enforcement personnel. The New England State Police Information Network is the regional center serving Connecticut.

- *Federal Bureau of Investigations Law Enforcement On-line (LEO)* – a secure internet based communications system available to local, state, and federal law enforcement personnel. Supported by the FBI, this system manages secure e-mail communications between enrolled members.
- *Homeland Security Information Network (HSIN)* – managed by DHS, this is the primary nationwide information sharing and collaboration tool for transmitting sensitive but unclassified information. It links government counter-terrorism intelligence and homeland security entities with other stakeholders. HSIN disseminates information and alerts to network members and allows for submission of information.

Federal guidelines advocate that a fusion center become a member of a regional or state secure law enforcement network such as RISS, LEO, and U.S. Department of Homeland Security Information Network. According to the CTIC policy manual, the NESPIN/RISS database system is the primary means for intelligence sharing for CTIC. This bi-directional system enables local law enforcement to input and query information, and at the same time, provide CTIC with the ability to gather, collate, analyze, and disseminate intelligence. The program review committee finds *CTIC access to federal data sources and other law enforcement based information sharing systems has been achieved. Active collection and dissemination of intelligence has been on-going.*

24-Hour operation/Watch Desk. When considering staffing levels, the federal guidelines for fusion centers propose maintaining a 24-hour/7-day-a-week operation with appropriate staffing. Although CTIC personnel are available on-call, CTIC is currently not operational 24 hours a day. Emergencies, urgent matters, and tips are routed through the Connecticut State Police Message Center, which is staffed on a 24-hour basis.

In its FY 06 Homeland Security grant application, DEMHS proposed an initiative for a “watch” desk that would be the central location for all information coming into CTIC from across all disciplines. Conceptually, this desk would be designed as a 24-hour, seven-day operating facility to take all incoming information. The Tips hotline would then be routed through CTIC rather than the Connecticut State Police Message Center. The watch desk would be part of a State Interagency Coordination Center (SICC) that would allow for the coordination and monitoring of all state agencies and all tactical level responders.

SICC would receive and integrate information that could alert officials and first responders at the earliest stage of potentially significant incidents, handle the initial notification of a potential health crisis, and have the capacity to maintain a centralized data base. DEMHS believes a move in this direction would provide more immediate response to local, state, and federal shareholders. However, *DEMHS reports the SICC initiative is still in a conceptual stage although federal money is available for this project.*

Location of CTIC. The location of a fusion center may have an impact on which agencies will participate. The center should be represented by various federal, state, and local agencies that have been brought together for the processing of terrorism-related information and producing analyzed intelligence with one common purpose. The federal guidelines for fusion centers advise integrating technology, systems, and people preferably through co-location.

It is recommended that participating agencies strive to locate personnel in the same facility whenever feasible. By seating officers and analysts from various agencies together at one location, they naturally develop personal relationships that help break down interagency resistance that impedes information exchange. In addition, this approach consolidates resources and equipment. If co-location is not possible, the federal guidelines suggest virtual integration of information and communications systems for seamless access and exchange.

At present, DEMHS is preparing to re-locate CTIC operations from the FBI offices in New Haven to the DEMHS headquarters located in Hartford. According to DEMHS, this move was precipitated by the need for additional office space. However, discussions with the various stakeholders suggest other reasons for the relocation may have been the arduous federal operating policies as well as the perception that CTIC is primarily a FBI operation. It is unclear when the relocation of CTIC will be finalized. Physical reconstruction at the Hartford headquarters is underway to prepare the site with secured computer systems and other security requirements. Renovations are expected to be completed within six to eight months.

At the FBI offices, CTIC is also co-located with the Joint Terrorism Task Force. It has not been determined if the JTTF may have a satellite office in Hartford. Regardless of location, the federal government is required to locate two personnel (one FBI and one DHS) at CTIC. DEMHS officials are confident that collaboration among the entities will not diminish with relocation. The program review committee finds *it is unclear what the impact of moving CTIC from the FBI offices in New Haven to DEMHS headquarters in Hartford will be.*

Training and certification. The federal guidelines state that fusion centers must ensure personnel are properly trained and provided specialized training as necessary. Personnel should be equipped to identify suspicious activities or threats and when appropriate provide information to the fusion center. In addition, staff should have adequate training in information and intelligence collection and synthesis. According to the federal government, the lack of uniform training and standards creates a problem not only for the state center but also hampers effective intelligence coordination and dissemination between other state and federal fusion centers.

To date, training for CTIC state personnel has been provided through the Police Officer Standards and Training (POST) council courses on topics such as suicide bombers, aspects of state and local anti-terrorism training (SLATT) and Operation Safeguard.²¹ In addition, CTIC has sponsored conferences for ILOs and RILOs on issues relating to proper collection, submission, and dissemination of information through the CTIC network as well as on other intelligence

²¹ The SLATT training program is funded by the federal DOJ and provides specialized training on terrorism and extremist criminal activity. Operation Safeguard provides awareness of activities such as applying for licenses and permits that facilitate terrorist plots.

sharing issues through the LEO and HSIN networks. However, attendance at the training conferences was not mandatory, and no tracking was done of who attended the sessions.

The program review committee finds *limited in-state training and exercise opportunities exist for CTIC personnel*. DEMHS is developing a certification program, known as terrorism liaison officer (TLO) training, that would cover various subjects such as intelligence gathering methods and techniques, handling and processing information, and training on various data bases used by the center and the state. The program review committee believes the initiative of a certification program such as TLO should be further explored. To supplement these training efforts, the program review committee also recommends **whenever feasible and appropriate, CTIC personnel should have more involvement in the joint tabletop, functional, and full-scale homeland security exercises throughout the state. Furthermore, as an administrative matter, CTIC should track the participation rate and training level of all of its personnel particularly for CTIC sponsored events.**

Performance measures and audits. Another fusion center guideline put forth by the federal government is to define expectations, measure performance, and determine effectiveness. The guidelines suggest this could be achieved through regular reporting and reviewing of performance in board meetings with adjustments made to operations as appropriate. The guidelines also advise integrating feedback and suggestions into fusion center operations.

CTIC has been in operation for over two years. Although the CTIC policy board meets regularly, the program's outcomes have never been formally measured to validate performance expectations. However, there has been some indication, though not verified, that a process of mapping information flow to identify crucial areas has been taking place as well as the use of a customer satisfaction survey. In any case, *CTIC has not implemented a formal audit or review process to ensure compliance with policies and procedures. Performance measures for CTIC do not exist and feedback opportunities on the usefulness of CTIC products are limited.*

The program review committee recognizes prevention is difficult to measure in any program. However, without performance measures, it is difficult to evaluate the success of these counter-terrorism efforts and determine the effectiveness of the program to meet its intended goals or objectives. Therefore, the program review committee recommends the **CTIC policy board establish a mechanism for ongoing monitoring of the center's operations, procedures, and policies to ensure that all information and intelligence needs of the shareholders are being met. The evaluation mechanism should also provide CTIC product users feedback opportunities.**

Without such a mechanism, stakeholders may obtain indiscriminate and unfocused information. CTIC members should engage in a process of deciding what they want to know (or what they need to collect) before they collect it. The purpose of this type of audit/evaluation function is for the center and stakeholders to ensure that what is being collected, analyzed, and disseminated is factual, timely, and relevant. It is through this mechanism that adjustments and improvements can be made to the fusion process.

A review of the literature suggests that fusion center operations may at some point be legally challenged. Therefore, it is in the center's best interest to have an oversight mechanism in place to validate that it is operating within constitutional and legal limits and that when necessary, appropriate corrective actions are taken.

Joint Terrorism Task Force

A significant partner of CTIC is the personnel assigned to the FBI Joint Terrorism Task Force. JTTF is responsible for providing investigative and operational support for terrorism cases. JTTF accomplishes that mission by joining federal, state, and local law enforcement agencies in a coordinated manner to detect, deter, prevent, and investigate acts of terrorism that threaten the national interest of the United States at home or abroad.

Personnel assigned to JTTF are sworn agents, detectives, and analysts with additional training and security clearances to work with and analyze classified information. The JTTF is organized into squads by investigative category – domestic terrorism and international. These units are responsible for vetting and validating leads, and assessing specific threats. It is the primary point of contact with all classified, national and state databases, and with investigative and intelligence efforts at all levels of government. As such, JTTF is the main repository for any classified information received, and it allows for classified information to be collected, analyzed, scrubbed, and then disseminated for local use.

As the link between the FBI and other intelligence and investigative entities, JTTF is an integral partner to CTIC and is housed within the same building. This partnership allows for lateral and horizontal communications to achieve full connectivity to information. *Connecticut's participation and presence on a multi-jurisdictional terrorism investigation entity has been established. However, assignment of state police officers to the task force has been inconsistent.*

In November 2006, a total of four CSP members were assigned to JTTF – one sergeant and three detectives. Currently, there are three vacancies in the assignment of JTTF personnel. These are due to promotions and military deployment. One of the concerns heard by the committee is that often well-trained and experienced personnel have to decide whether to leave CTIC and/or JTTF to advance within their agency such as CSP or stay at the center or taskforce in a career limited position. According to DPS and DEMHS, the statutory limit on the number of authorized state police personnel makes filling these vacancies difficult. DPS anticipates CSP staffing resources to be somewhat alleviated with a new trooper class graduating from the state police academy.

As noted in the briefing report, the Connecticut JTTF has had a role in several publicized cases including the following:

- Based on a criminal complaint issued by a U.S. Magistrate in the District of Connecticut, British law enforcement authorities arrested Babar Ahmed in London. A federal grand jury returned a four count indictment against Babar including conspiring to provide and providing material support to a terrorist, conspiring to kill persons in a foreign county, and money laundering.

- The JTTF began a long-term investigation of the Liberation Tigers of Tamil Eelam in 2004. Eight arrests were made in 2006, including a Simsbury resident on charges of conspiracy to commit material support to a designated terrorist organization.
- The investigation of the Yale bombing and the arrest of a Berlin, Connecticut man on 30 counts of possession of machine guns, destructive devices and silencers.

Given the critical role and success of the taskforce, the program review committee believes **Connecticut should have a continued presence on the JTTF with additional assignments when staff resources are available.**

CTIC Success Stories

At the request of the program review committee, CTIC also compiled a list of “success stories.” The list is provided in Appendix C and contains only unclassified information as appropriate. The list underscores the benefit information sharing through CTIC has for general law enforcement as well as for homeland security. In particular, CTIC has been recognized as an FBI “Best Practice” for its use of an information sharing and crisis management tool known as the Law Enforcement Online Virtual Command Center (VCC). The VCC is an electronic command center that allows law enforcement to submit and receive information and intelligence at local and remote sites.

Expanded role for Virtual Command Center. *Through the use of the Virtual Command Center an expanded operational role for CTIC has been established.* In April 2007, CTIC assisted in overseeing the special operations at the University of Connecticut (UConn) Spring Weekend. The Eastern District Commander of the Connecticut State Police requested CTIC help to set up and implement the Virtual Command Center to coordinate three separate command post operations. The VCC was used during the three-day event to facilitate the gathering and dissemination of reported activities from the CSP, UConn police, and local fire and EMS services. The VCC captured all reported incidents that public safety officials were handling during the sanctioned and unsanctioned events occurring on campus. The VCC provided public safety personnel streamlined operational and time-critical information.

Fusion Centers in Other States

According to a recent U.S. Government Accountability Office (GAO) report, most states and many local governments have established fusion centers to address gaps in information sharing.²² These centers vary in their stages of development from completely operational to the early planning stages. GAO identified 58 fusion centers nationwide. Of these, 21 are fully operational and fully functional centers. Sixteen centers, including Connecticut, are in an

²² U.S. Government Accountability Office, *Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, (October 2007).

intermediate development stage, while six centers are between intermediate and fully developed. Fifteen centers are in the early development and/or planning phase.

The centers vary in many of their characteristics, but generally they have missions that are broader than counterterrorism, have multiple agencies represented - including federal partners - and have access to a number of networks and systems that provide homeland security and law enforcement-related information. Centers vary in their staff size, but many had federal personnel assigned to them as intelligence analysts. Law enforcement entities, such as state police or state bureaus of investigation, are the lead or managing agencies in the majority of the operational centers. A summary table of the fusion centers as reported by GAO is provided in Appendix D.

The fusion center model most often mentioned in homeland security literature is the Los Angeles Terrorism Early Warning group. This is based on the fact that it is a full-time, multi-agency, multi-discipline (law, fire, and health), multi-jurisdictional (local, state, and federal) operational entity that addresses all phases (pre-, trans-, and post) of a terrorist threat or incident. This fusion center reportedly provides the ability to facilitate both lateral and vertical unrestricted communication both within and among agencies. However, few places, particularly smaller jurisdictions, recognize the need nor have the resources necessary to establish and maintain an elaborate intelligence operation like Los Angeles.

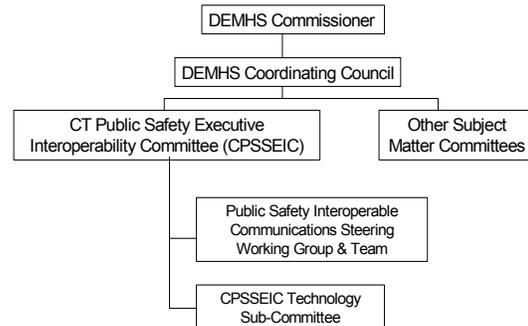
It should be noted that in late 2006, the federal DHS assessed CTIC operations to determine the best way for DHS to support information sharing among CTIC and the federal government. The DHS assessment team concluded that CTIC had the basic underpinning for a successful and smoothly functioning fusion center.

Communications

Pursuant to state law, DEMHS is responsible for coordinating homeland security communications and other state government communications systems with state and local government personnel, agencies and authorities, the private sector, and the general public. The DEMHS coordinating council, established to advise DEMHS on a variety of issues, is charged with developing recommendations for the state’s overall communications system. Over the years, several efforts to address statewide communication interoperability have been initiated and continue to evolve. The following section provides an overview of the current status of the state’s progress regarding emergency communications.²³

As Figure IV-1 shows, there are various working groups within the DEMHS organizational structure assessing the communications issue. The primary purpose of the Connecticut Public Safety State Executive Interoperability Committee (CPSSEIC) is to make recommendations to the DEMHS coordinating council and the DEMHS commissioner with respect to sharing real-time voice, data, and video information with first responders and other critical components of the emergency management and public safety community. Assisting the work of the executive interoperability committee is a steering committee and technology sub-committee.

Figure IV-1. Governance Structure for Communications



Goals and Objectives

The State Homeland Security Strategy (SHSS) and DEMHS internal strategic documents have essentially one goal in this area – enhance the existing statewide communications system. Combined these strategic documents contain nine objectives related to communications. An examination of these objectives reveals that *five of the nine objectives regarding communications are ongoing while four have been partially met*. The nine objectives, along with the program review committee findings, are provided in Table IV-1 and discussed throughout this section. (A complete listing of communication goals and objectives is provided in Appendix B.)

²³ Many of the findings noted in this section are derived from the State Communications Interoperability Plan.

Table IV-1. Status of Communications Goals and Objectives

Status	Objectives for the Statewide Communications System
Ongoing	<ol style="list-style-type: none">1. The state continues to enhance the statewide emergency telecommunications infrastructure and emergency notification system.2. A Statewide Interoperable Communications Plan (SCIP) has been drafted. Although a final plan is expected in December 2007, the plan is considered a living document that will be reassessed and updated on an annual basis.3. An emergency notification system for local emergency management directors, DEMHS staff and key stakeholders has been developed and tested. Locals will be permitted to pursue this at their level.4. The Emergency Broadcast System continues to be tested on a weekly basis.5. A high-band radio system is being maintained and tested statewide on a monthly basis.
Partial	<ol style="list-style-type: none">6. A Tactical Interoperable Communications plan has been completed for DEMHS Region 1. TIC plans for the remaining four DEMHS regions are currently being developed.7. DEMHS and DPS have coordinated a testing system for the ITAC/ICALL system.8. The mechanism to disseminate information regarding terrorist threats and attacks to state and local authorities via e-mail is anticipated by March 2008. The dissemination of information that has a law enforcement purpose is handled by intelligence bulletins and is distributed via the Homeland Security Information Network.9. An e-alert system to notify private sector stakeholders of any change, specific to their sector, is expected by March 2008. Information distributed to the private sector is pushed out via Infragard, which is provided by FBI.

Source: LPR&IC analysis of SHSS and DEMHS documents

State Communications Interoperability Plan (SCIP)

Through the Public Safety Interoperable Communications grant program and the 2007 Homeland Security Grant Program (HSGP), the federal government has required all states to develop and adopt a statewide communications interoperability plan. DEMHS, the state's HSGP administrator, has prepared a plan to comply with the federal mandate. The CPSSEIC and its working groups drafted the plan using a practitioner-driven approach where input was sought from stakeholders at the local level. (Further discussion of the plan development is provided below.)

A final state communications interoperability plan was submitted in December 2007 for peer review and federal approval. The expectation is that the federal Department of Homeland Security will provide grant money to be spent over a three-year period (2010) for plan implementation. The grant money provided by DHS will be used to make progress toward the goal of communications interoperability. Additional funds will be provided by Connecticut to continue and maintain this project.

There are federal criteria and specific components that must be addressed in the plan. The SCIP must define a strategic vision and a set of goals and objectives for improving interoperable communications statewide. Among other things, the plan must describe the state's existing communications interoperability environment and specifically address the current level of technology and equipment, the use of standard operating procedures (SOPs), and the availability of training and exercise. The plan is considered a living document to be assessed and updated annually as progress develops and circumstances change. An updated statewide plan must be submitted to DHS at least every three years.

Existing Communications Systems

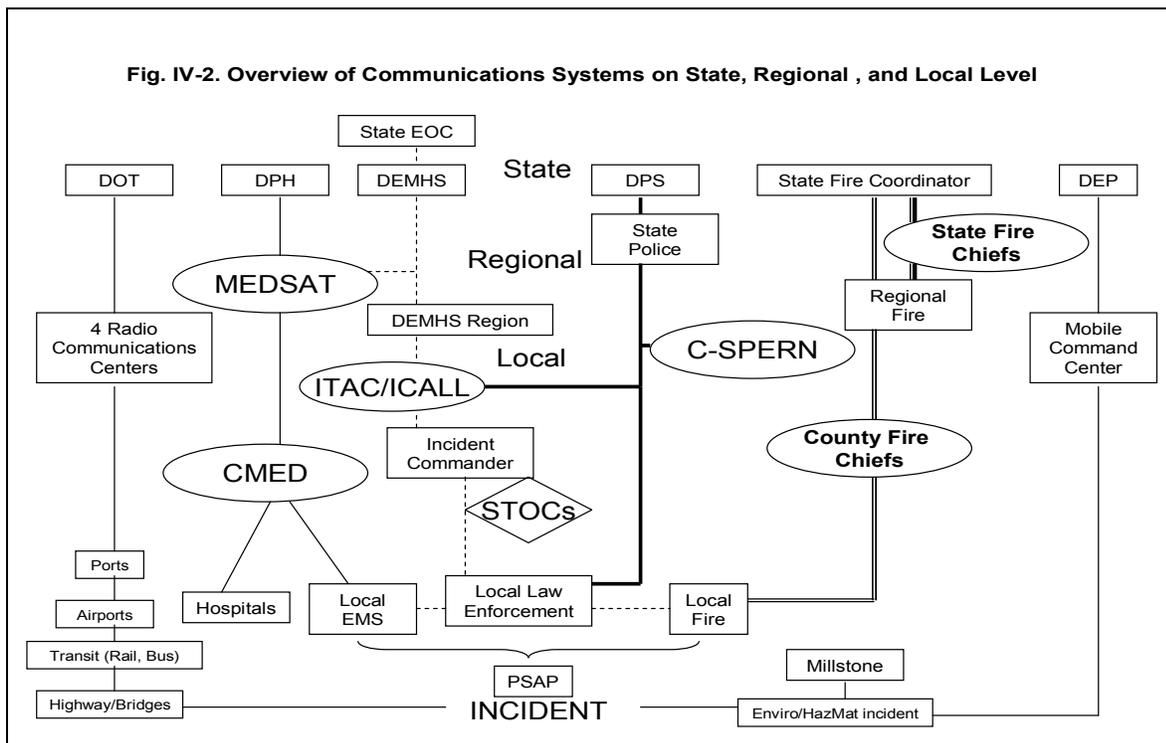
The first phase of the plan is to assess existing communications systems. The state is in the process of conducting an inventory of the different communications systems and equipment operating throughout the state. The inventory process is an ongoing project as equipment and systems evolve and are subsequently replaced.

Based on the information collected to date by the various communications working groups, Connecticut currently does not have a complete interoperable system. Connecticut has several legacy communications systems that are used for interoperable communications. Historically, emergency response communications systems within the state were built as stand-alone systems designed to meet the individual system user needs. The capability of these existing communications systems varies widely due to the state's terrain and the financial limitations of the various communication operators.

Other factors contributing to the current level of interoperability include: incompatible and aging communications equipment; inadequate and restricted funding; disjointed planning efforts; lack of coordination and cooperation; and limited and fragmented radio spectrum. As a result, there are gaps in local, regional, and statewide emergency communications systems.

Voice communications systems. Connecticut has several voice communications systems that range from local to regional to statewide. Figure IV-2 provides a general outline of the various emergency response communications systems used in the state. As illustrated in Figure IV-2, different state agencies have their own communication networks and systems.

The Department of Public Safety operates and maintains an 800 MHz system primarily used by the Connecticut State Police, which also serves as the backbone of the communication infrastructure for different groups. This DPS statewide system was installed in the 1990s and supports ITAC/ICALL, which allows all public safety (police, fire, and EMS) commanders to communicate. The DPS system also supports the Connecticut State Police Emergency Radio Network (C-SPERN), installed in 2007 and available to all Connecticut law enforcement.



Fire services utilize two primary communications systems. Both were established in the 1950s and are supported by the Connecticut Fire Chiefs Association. The Connecticut State Fire Chiefs System is used by Connecticut regional fire communications centers and the State Fire Coordinator. The Connecticut State County Fire System serves the local fire services, regional fire communications centers, and the State Fire Coordinator in Connecticut.

The Department of Public Health operates and maintains a medical satellite network (MEDSAT) for voice communication among medical personnel. Deployed in 2004, this network provides a connection to all Connecticut general hospitals, DPH, DEMHS, coordinated medical emergency dispatch centers (CMED), and the Connecticut Hospital Association. DPH also has both a health alert network for surveillance and a wide area network capable of transmitting both voice and data communications.

The Department of Transportation has multiple voice channels and utilizes four district radio communications centers to manage day-to-day operations. Two DOT operation centers monitor statewide DOT communications and traffic. Radio broadcasts are used to alert motorists of traffic conditions in certain parts of the state. DOT also provides radio communications for four airports and for the agency's movable bridges over waterways.

The state Emergency Operations Center (EOC), overseen by DEMHS, has several voice radio systems covering a range of spectrum, an emergency alert system, a microwave broadcast fax capability, and partners on a number of systems that include ITAC/ICALL and MEDSAT.

Finally, the Department of Environmental Protection (DEP) has a mobile command center that is equipped the several technological devices and is available for large and small scale events. In addition to having the capacity for data communications, the command center works with 8 operating towers with an additional tower planned. DEP has many different channels available for communications with its districts, the state police, and other state agencies. DEP is contacted for oil or chemical spills, dam flooding, hazmat incidents, and radiation problems. The emergency operation centers for the municipalities that are within the Millstone emergency planning zone or that serve as host communities for a Millstone incident have received a control station for ITAC/ICALL.

Interoperability at the local level. Communications become more critical when an incident overwhelms the response and resource capability at the local level. Locals may request other area responders to assist in managing the situation. Responding units must have a communications system in place that will provide interconnectivity among the various responders at the incident scene.

The existing communications and interoperability environment among Connecticut localities varies widely. Some localities can communicate among their various first responders (fire, law enforcement, and EMS) as well as with other localities and emergency response partners, while others can not. Some municipalities have new or relatively new radio communications systems that are not interoperable with their neighboring communities. At the moment, certain regions of the state as well as several disciplines have attained a high level of communications interoperability, while others have not. A brief discussion of the current status of communication systems by discipline is provided below.

Local fire and law enforcement. All municipal fire and police departments in the state have a voice communications system. In some communities, both police and fire departments are on the same system. However, in most areas of the state, they are not. As stated previously, the Connecticut Fire Chiefs Association supports two systems for local, regional, and statewide voice communications.

Some municipal police departments have limited common regional communications system, depending on the area of the state. However, all law enforcement personnel have access to C-SPERN. All first responders, including police and fire, may also utilize 800 MHz radios with the ITAC/ICALL frequencies provided by DEMHS to communicate. In addition, DEMHS

has assigned State Tactical On-scene Channel (STOC) boxes to allow incident commanders to communicate.

Local emergency medical services. Each basic ambulance and paramedic unit in Connecticut is required to be equipped with a two-way radio capable of communicating with the state’s 13 coordinated medical emergency centers (CMED). CMED links EMS field personnel with the hospitals and emergency departments. CMED is one of the state’s oldest (25 years+) communications systems. CMEDs are now part of MEDSAT, which is operated by DPH.

Public safety answering points (PSAPs). Public safety answering points are the first point of reception of a 911 call. Operated on a 24-hour basis, these facilities dispatch emergency response services or relay 911 calls to other public safety agencies. PSAPs are typically housed in a police department, fire department, or emergency communications center. Most municipalities operate their own PSAP. However, some municipalities provide 911 services through a regional communications center. All PSAPs have been provided a control station for ITAC/ICALL.

One weakness of PSAPs noted by the DEMHS State Strategic Plan is that “there is no overarching governance regarding standards of dispatch, communication flow, outbound communication and prioritization flow of information.”²⁴ To address this weakness, DEMHS has proposed an initiative to establish a state interagency coordination center (SICC). As discussed in Section III, SICC would serve as the hub and hotline for all state answering points. SICC would coordinate and monitor all state agencies and all tactical level responders. (Further discussion of the SICC is provided later.)

Development of the Statewide Communications Interoperability Plan

As noted earlier, the Statewide Communications Interoperability Plan was developed by the Connecticut Public Safety State Executive Interoperability Committee. The committee is composed of 20 individuals representing a variety of disciplines. As seen in Table IV-1, *DEMHS has established a governing structure with representatives from all pertinent emergency response disciplines to address the state’s interoperable issues.*

Table IV-1. Participating Agencies	
CT Commission on Fire Prevention and Control	CT EMS Advisory Board
CT Emergency Manager’s Association	CT Fire Chiefs Association
CT Police Chiefs Association	Department of Correction
Department of Environmental Protection	Department of Information Technology
Department of Public Health	Department of Public Safety
Department of Transportation	Department of Emergency Management and Homeland Security
Judicial Department	Military Department
Office of Statewide Emergency Telecommunications	Representatives from all 5 DEMHS regions

²⁴ DEMHS State of Connecticut Enhancement & Strategic Plan (2007-2011),p.32

The groups represented include public safety, transportation, corrections, public health, the military, information technology, environmental protection, judicial, the police chief's association, the fire chief's association, fire prevention, the EMS advisory board, statewide communications, the emergency manager's association, and representatives of each of the five DEMHS regions. This multi-disciplinary approach should enhance coordination and cooperation as well as potentially reduce any internal jurisdictional conflicts.

Regional meetings and questionnaires were used to develop information from the different stakeholders. The questionnaires were provided to all chief executive officers, tribes, fire departments, police departments, emergency management directors, emergency medical services departments, homeland security points of contacts, state and federal agencies, and non-governmental agencies. A total of 276 individuals attended the sessions, and 80 completed the survey for a 30 percent response rate.

A total of six meetings were held – one for stakeholders in each of the five DEMHS regions and one for state and federal agencies. The purpose of the meetings was to encourage input and participation in the plan development, measure the current level of interoperability, and promote a sense of investment for all stakeholders.

The survey served to identify common problems such as the lack of interoperable communications equipment, governance, training, and standard operating procedures. The survey results reported in the SCIP plan indicated some groups have purchased or received adequate equipment but do not use it regularly or completely understand how to use it, while other groups do not have the necessary equipment. Others noted that they did not have standard operating procedures and required help to develop them. Several also mentioned that training was insufficient.

Overview of Components of the Statewide Plan

As noted earlier, the SCIP is federally required to contain an overall strategic vision as well as steps to address specific issues such as training and exercises, standard operating procedures, and other components. The following provides an overview of some of these areas.

Strategic vision. The plan's stated vision is: *“By 2015 agencies and their representatives at the local, regional, and state level will be able to communicate (voice & data) using compatible systems, in real time, across disciplines and jurisdictions, to respond more effectively and timely to day-to-day operations and major emergency situations.”*

Once the statewide communications inventory is complete, the state interoperability plan's general approach is to phase out and replace existing and older technology and equipment with newer technology. The age, condition, and capabilities of the existing technology will determine the transition schedule. Various interfaces/gateways²⁵ such as STOC boxes will be installed and used to provide connectivity with different sets of equipment. This will continue until the existing equipment has reached the end of its lifecycle and new interoperable equipment will be purchased. The ultimate goal is to migrate all public safety practitioners to a common

²⁵ Gateways retransmit across multiple frequency bands providing an interim interoperability solution.

bandwidth (700 MHz) over time. Because funds in some localities have been recently expended for communications, it is not expected that such systems would immediately be replaced. All existing capabilities will be maintained until migration is complete.

Training and exercises. A required component of the SCIP is to identify the process by which the state will ensure that appropriate training and exercises are available to all practitioners across the state. *DEMHS has recently hired five regional trainers who will assist in the development and implementation of training programs for use of interoperable equipment and ensure federal NIMS compliance.* The trainers will ensure cross-discipline training by developing working relationships with representatives of municipal and tribal police, fire, EMS and emergency management agencies, and state agencies such as DOT, DEP, DPH, DPS, DOIT, and DEMHS.

One immediate recommendation of the plan is to hire a full-time interoperability coordinator. The coordinator's primary responsibility will be implementing all components of the SCIP in conjunction with the interoperability committee. The coordinator will be the main point of contact for incoming information such as changes in technology and usage.

The coordinator will also develop and coordinate statewide communications training and exercise programs. The new DEMHS regional training staff will collaborate on the training, exercises, and drills ensuring multi-jurisdictional/discipline partnerships on a regular basis. The coordinator will prepare and report results to the interoperability committee. It is expected that the coordinator position, along with the location and reporting structure, will be established and funded as requested.

Standard operating procedures. The SCIP survey results found that *standard operating procedures for communications are not consistent throughout the state.* Currently, each locality has varying levels of SOP documentation. While some cities and towns reported having formal written SOPs, other survey respondents indicated they have informal, unwritten agreements; others indicated they have no SOPs in place at all. The plan identifies this as an area requiring further attention.

DHS recommends that standard operating procedures must be established at the local level as well as jointly for planned events and emergency events. All SOPs must be written in a user-friendly format, follow NIMS guidelines, and training must be provided to all involved individuals. SOPs should also be designed on a regional level to ensure integration of NIMS. To address this, the plan proposes that the coordinator when hired will assist with the writing of joint SOPs to ensure that SOPs are written, understood, trained on, and complied with.

Tactical interoperable communications (TIC) plans. Another SCIP requirement is to identify any tactical interoperable communications plans in the state. TIC plans, which are federally required, outline the procedures and processes that will be used during a significant incident within a specified region. The development of TIC plans helps to identify specific problems, needs, and barriers to communications among the area's agencies and disciplines. It names potential partners and their roles and responsibilities. It inventories the area's

communications resources and details how those resources would be used to provide communications among all first responder agencies.

Tactical Interoperable Communications plans will be developed for all five DEMHS regions. The DEMHS goals state that all regional TIC plans are to be completed by January 2008. DEMHS reports that the goal date will not be met due to staffing limitations. *To date, only DEMHS Region 1 has been completed.* Given the number of towns in each region and the volume of information required, the coordination and time commitment involved in preparing TIC plans is considerable. The interoperable coordinator will provide assistance in this function. When completed, the TIC plans will be integrated into the SCIP.

Building redundancies. In addition to establishing an interoperable communications system, redundancies must be established to ensure tower sites, repeaters, antennas, and other communications assets are able to continue operations uninterrupted. *Currently, only the Connecticut State Police have redundant systems in place for catastrophic communications losses. All other communications systems have redundancies to a certain point.*

According to DEMHS and the chairs of the interoperability communications committee, different redundancy options exist. In addition to the CSP system, the state has mobile decontamination trailers with mountable communications towers that can be brought to any location to provide backup and redundancy during times of communications loss. Each DEMHS region has high band radio capability to communicate with towns and cities when other forms of communications fail. The state has access to military affiliate radio systems (MAR), which can run a cross-state repeater system as well as MEDSAT, a satellite enabled system. A network of amateur ham operators across the state is also available. Furthermore, the federal government has required each state, as a condition of receiving the grant money associated with SCIP, to purchase a cache of communications equipment known as strategic technology reserve (STR) to resolve catastrophic loss of communications assets. (Further explanation of STR is provided later in this section.)

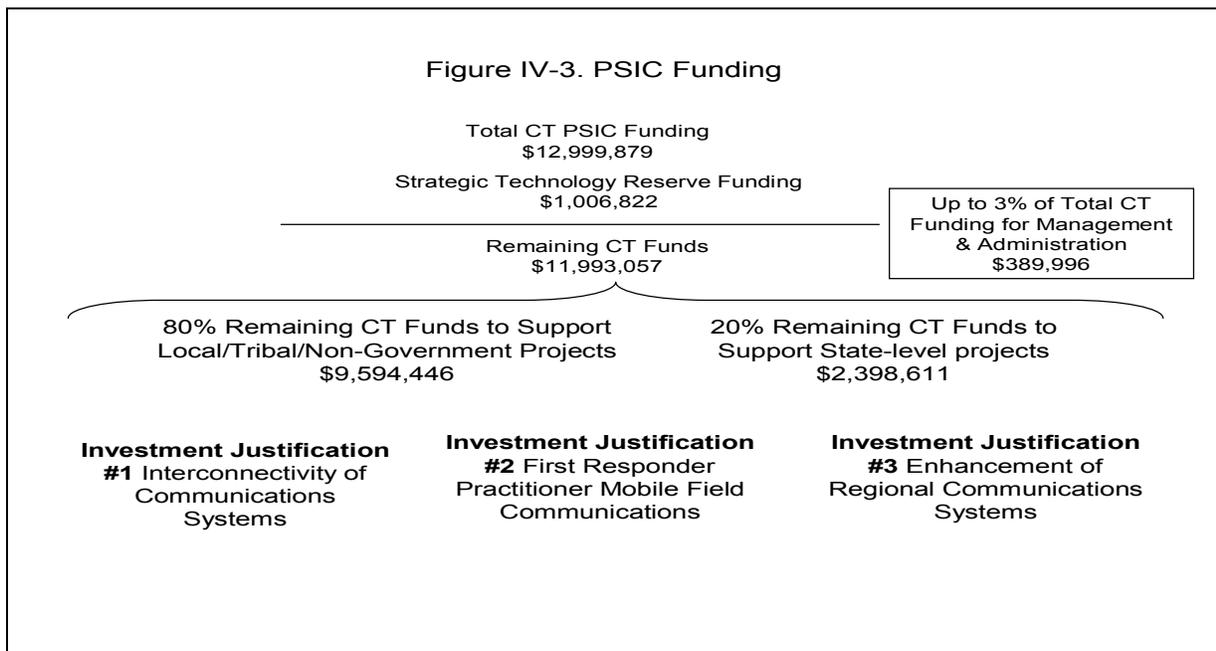
Data communications. The first SCIP priority is to establish voice communications interoperability. Although voice communications is a major component of the statewide communications system, it is not the only component. The ability to send and receive data and video to respond to an event must also be established. *The lack of voice and data communications interoperability continues to be a challenge.* Agencies often cannot communicate or exchange data information with other jurisdictions. To address this, SCIP will initiate an approach similar to the process outlined for voice communication interoperability. Existing systems and networks will be assessed for data communications, and efforts for data interoperability will commence.

Performance measures. The federal criteria for SCIP recommend that the statewide plans set performance measures to gauge the success of interoperability efforts and implementation of the plan. *Connecticut's SCIP states performance measures will be established as detailed project plans are developed for the various SCIP goals.* The long-term baseline measures will be:

- the ability and effectiveness of local, regional, state, federal, tribal nations, non-profit and private entities to communicate with voice data and video; and
- coordination with state agencies’ interoperable communications efforts.

According to the chairs of the state interoperability committee, the performance measures will be used in tandem with an annual self-assessment based on an interoperability continuum developed by the federal DHS. This tool was established to depict the core facets of interoperability. These elements include governance, standard operating procedures, technology, training/exercises, and usage of interoperable communications. A copy of the continuum is provided in Appendix E.

PSIC funding. It is anticipated that Connecticut will receive approximately \$13 million to begin implementation of the statewide interoperability plan. According to DEMHS, three key “investment justifications” or goals have been developed. The breakdown of the PSIC funding is presented in Figure IV-3.



To receive the PSIC grant funds, *the state must establish a strategic technology reserve of deployable communications equipment in the event of an emergency or major disaster.* This requirement allows for a cache of extra communications equipment (e.g., land mobile radio equipment, cellular and satellite enabled equipment, self-contained mobile communications sites, backup power, and IT equipment) in case of a catastrophic failure or surge in needs. This cache is considered supplemental to day-to-day communications equipment. This requirement is satisfied by some of the purchases made under the second investment justification described below. Another PSIC grant requirement is that 80 percent of the funds must directly benefit local and regional interoperable communications and 20 percent must support state projects.

The first goal or investment justification, expected to consume a significant portion of the PSIC funds, is to connect PSAPs, communications systems, and identified public safety facilities (e.g., fire, law enforcement, EMS, and local public health facilities) on a proprietary resilient network with fiber optic redundancy. These funds would supplement the equipment purchase for a wireless network and for 700 MHz connectivity. It is anticipated that 911 surcharge monies (about \$3 million in matching funds) will also be used.

The second goal or investment justification is actually three projects to improve mobile field equipment, training, and coordination. The first project is to purchase hardware and stockpile equipment that satisfies the STR requirement. The second proposal is to purchase six rapid response mobile interoperable communications vehicles (one each for the five DEMHS regions and one for statewide use) that enable cross-communications with state agencies and regions as well as the capacity to connect entities that are not commonly linked. Memoranda of understanding will be developed to strategically house these vehicles at different secure localities and outline the provisions for vehicle deployment to different localities and EOCs as needed. According to DEMHS, this mobile communications approach is used by New York and the National Guard. These funds will also provide training to personnel authorized to operate these units. The third project is to purchase the necessary equipment to set up a mobile Emergency Operations Center. This would provide a portable temporary operating environment during incidents and would be similar to a local area network. It will have the capacity to set up radios, 20 phone lines, and laptops.

Through the third goal or investment justification, DEMHS will determine gaps in regional communications systems and prioritize needs. DEMHS will identify whether funding should be expended to maintain an existing communications system or to upgrade and migrate to a common bandwidth (700 MHz). For example, this could include an evaluation of the aging CMED system to determine if and how it should be maintained until the 700 MHz build-out is complete. These funds would procure and install equipment to fill regional gaps. According to DEMHS, no determinations have been made as to which systems would be initially evaluated.

Summary

Achieving interoperability on a statewide basis is a complex process. *Interoperability is a challenge that cannot be addressed by one entity but rather must involve multiple entities.* A partnership among local, state, and federal public safety organizations and industry is required. Several initiatives, as outlined in the statewide communications interoperability plan, are needed to provide a coordinated approach to resolving long-standing inadequacies in public safety communications systems.

The plan's primary mission is to provide for a statewide telecommunications infrastructure and protocol that will allow for timely, efficient, and cost-effective communications (voice, data, and video) for all public safety and other public agencies (state, regional, and local). As a result, the state will be able to provide an appropriate coordinated response to any and all emergencies involving multi-jurisdictional, multi-disciplinary agencies.

To accomplish this, existing legacy systems will need continued support as an ongoing migration plan allows all practitioners to operate on a common bandwidth enhancing interoperability. Although the statewide strategy will require the procurement of new technologies, adequate and appropriate technology is just one solution to the interoperability problem. Unless emergency response agencies routinely use interoperable equipment, establish standard operating procedures, and train, they will not be prepared to use the equipment in infrequent large scale incidents. *Once approved, the statewide communications interoperable plan will be a significant initial step toward public safety communications interoperability, improving system coverage and operations, information sharing, and partnering for governance.*

Mass Emergency Notification

The dissemination of emergency information and instructions in a threatened or actual emergency is defined in the state's Emergency Alert System (EAS) plan.²⁶ EAS defines the procedures for designated government officials as well as the broadcast and cable services. The purpose of the plan is to provide a single source of qualified information and instructions regarding any emergency situation to all broadcasters and cable systems in the state.

With the use of encoders, EAS can be activated directly by DEMHS, CSP, and the National Weather Service. The EAS can be activated to provide warning to specific portions of the state. Local authorities may also request local EAS activation through the Connecticut On-line Law Enforcement Telecommunications (COLLECT) system through the CSP.

The EAS encoder allows authorized entities to record an emergency message for where and when residents can tune for emergency information including actions taken by state and/or local governments. If necessary, the EAS message can direct attention to public information briefings, that may be carried on radio stations, television stations, and cable systems. Television stations and cable systems will also transmit video crawl explaining the emergency interruption. The FCC requires monthly testing of the EAS by DEMHS and CSP to assure the successful operation of the system. Broadcast stations and cable systems must randomly test at least once a week. In addition to EAS, the use of outdoor warning devices such as sirens or public address systems may be used for incidents related to nuclear power facilities or involving hazardous materials.

Reverse 911. In addition to EAS, local authorities are permitted to pursue other mass emergency notification systems at their level. In March 2007, the Connecticut Department of Information Technology awarded Reverse 911, an Indianapolis-based organization, a contract as the state approved emergency notification software provider. The contract allows cities and towns to pay for the Reverse 911 system with either state homeland security funding or standard budgetary funds. The cost depends on the options purchased. Towns may either purchase the

²⁶ The plan is prepared through the Connecticut State Emergency Communications Committee (SECC), a collaboration of federal, state, and local entities including: DEMHS, DPS, FEMA, the Federal Communication Commission (FCC), the National Weather Service, the Connecticut Broadcasters Association, and the broadcasters and cable systems of Connecticut.

Reverse 911 system and related software to run the program themselves, or they may select a service-based option whereby the system is operated for them. According to DEMHS, the operating costs are based on the number of calls dialed plus approximately \$2,500 to purchase the telephone database which needs continuous updating.

Reverse 911 assists towns to obtain phone number databases, but it is up to the towns to decide how the information in the calling system should be used and protected. The database is a mix of listed phone numbers, cell phone and unlisted numbers, as well as numbers that residents have voluntarily given to the town. If an individual does not want to be part of the database, they can opt out.

Reverse 911 combines the calling data and utilizes GIS mapping technology to geographically target and notify affected individuals. Towns outline the targeted area on the online map and then record and launch a voice message. Simultaneously, Reverse 911 dials all phone numbers in the designated calling zone.

If phone lines are busy, the system will attempt to redial those numbers a predetermined number of times to make contact. If an answering machine picks up the call, the emergency message will be left on the machine. In addition to land lines and cell phones, Reverse 911 can also send notifications to phone numbers registered to pagers, fax machines and TTY/TDD devices for the hearing impaired. Notification results that provide call session statistics are immediately available. This can assist localities during door-to-door evacuations.

Among the potential uses for Reverse 911 are emergency evacuations, natural disaster alerts, hazardous material leaks, homeland security alerts, search and rescue operations, missing person alerts, wanted person alerts, neighborhood emergency incidents, and special community notifications.

The implementation of Reverse 911 at the local level is expected to enhance communication abilities during crisis situations and improve emergency response with fast delivery of mass notifications to citizens and first responders. This technology is considered a valuable tool for local officials to use to notify residents of a pending or ongoing incident without over-reliance on news media for information.

According to DEMHS, more than 40 municipalities in the Hartford region and about a dozen in the Fairfield region are using federal homeland security money to buy emergency calling systems from Reverse 911. Almost half of the state's 169 municipalities should have the system by 2008 which would cover approximately 70 percent of the state's population. Appendix F provides a listing of towns that have purchased Reverse 911 with homeland security funds.²⁷

System limitations. As noted, Reverse 911 does not notify unlisted numbers or cell phones unless manually added to the database. Cell phones may be entered in a database. However, the cell number is linked to a specific address then the location of the cell phone becomes fixed to that location. Therefore, a situation may arise where the cell phone user is

²⁷ According to DEMHS, there may be towns that purchased mass notification systems from other vendors. However, this information is not regularly tracked.

mobile and in the affected area, but is not notified because the fixed location of the cell number is in an unaffected area. In addition, the calling system may become less effective as the geographic area gets larger due to the outgoing call capacity of the system and reception capacity of the towers in the affected area. DEMHS acknowledges the system still has some issues to be resolved.

Committee staff discussions with DEMHS and DOIT representatives regarding the Reverse 911 system raised a few issues. First, a mass notification system is a voluntary purchase for municipalities. Second, towns are being charged by the telephone companies to supply the telephone number database in their communities despite the fact that the Office of Statewide Emergency Telecommunications (OSET) within DPS already pays the companies to manage a statewide database for PSAPs to operate the Enhanced 911 system. Finally, DEMHS has maintained no role in managing the contract or tracking which towns have acquired it.

The program review committee believes *this method of mass notification while not perfect does provide a valuable tool for emergency management*. As such, program review committee recommends that **a mass notification system, such as Reverse 911, should be a required homeland security fund purchase for municipalities**. This is not unprecedented. In the past, DEMHS has required municipalities to purchase certain communications equipment with homeland security funds. Of course, a concern would be the ongoing operating cost of maintaining such a system if federal funds diminish. To that end, **DEMHS should work with OSET to ensure the cost to towns for databases is minimal**. Program review staff was told that DEMHS is considering legislation to address the purchase cost of the database. Finally, **DEMHS, along with DOIT, should have a role in managing the mass notification system contract and tracking who has acquired it**.

Public relations and awareness. As noted in the briefing report, DEMHS' public communications consists of public service announcements, news releases and briefs, media interviews, an electronic newsletter and website, and a public inquiry phone line. In early 2007, DEMHS commissioned a statewide survey of Connecticut residents to assess the effectiveness of its awareness campaigns and overall public knowledge of emergency preparedness. The Center for Survey Research and Analysis at the University of Connecticut conducted the study and made the following verbatim marketing insight statements:²⁸

- “There is room for improvement regarding familiarity. Promotional campaigns to increase awareness are warranted.”
- “Updated campaigns might specifically target younger adults, who tend to be less concerned about emergency preparedness.”
- “Continue use of slogans, which are effective in increasing awareness of emergency preparedness. Focus on increased familiarity with the tips hotline, perhaps reaching out to school-age children who will share the information in households.”

²⁸ Center for Survey Research & Analysis, *Department of Emergency Management and Homeland Security*, (March 2007).

- “There is clearly a great deal of interest in obtaining information online. DEMHS will be tapping into a population that is used to and interested in obtaining information online.”
- “Television, newspapers, and radio are also important media for disseminating information.”

Currently, DEMHS does not have a public information officer. These duties are presently being handled by the DEMHS deputy commissioner. This includes handling of public awareness campaigns such as “See Something, Say Something.” The deputy commissioner reports several new initiatives are being developed or considered with the assistance of the Federal Emergency Management Agency. Many are aimed at reaching school-age children.

The program review committee finds *the function of a public information officer is an important component for DEMHS and should be an ongoing responsibility for a permanent position.* Therefore, the committee recommends **a DEMHS public information officer position should be authorized and filled. Public service announcements and campaigns should be developed and revamped when necessary.**

Other Issues and Top Concerns

During the course of the study, program review staff noted various issues related to selected management practices of the department. This section covers findings and recommendations regarding miscellaneous areas including: the development and reporting of goals and objectives; the use of administrative agreements; and an alternative site for the State Emergency Operations Center. In addition, this section includes a discussion of the DEMHS and DPS “top concerns” requested by program review committee members.

Goals and Objectives

DEMHS has engaged in an elaborate planning process that includes stakeholders from a wide variety of disciplines throughout Connecticut. In addition, the multi-disciplined Emergency Management and Homeland Security Coordinating Council (EMHSCC) also plays a key role in reviewing and commenting on major initiatives and strategic goals. In examining the strategic goal setting and planning process, along with the various planning documents and federal grant applications, the program review committee makes the following findings:

- *Some DEMHS goals tend to be short-term and/or do not convey a vision of where the department wants to be in the future.*
- *DEMHS objectives do not always have an expected date of accomplishment and do not usually have associated performance measures.*
- *DEMHS does not systematically track and report progress made on goals and objectives.*
- *Various federal and state documents contain an assortment of goals for DEMHS. The department does not provide a unified reporting system so that stakeholders, policy makers, or the general public can know the status of the goals.*

Goals are intended to provide an indication of the broader outcome of what is to be achieved. Objectives are more refined steps necessary to achieve the goal, while performance measures are ways to assess program results. Long-term goals can be found in the SHSS, the DEMHS internal strategic goal document, and in federal grants. In reviewing DEMHS’ goals, there is not always a clear vision or anticipated picture of success in any particular area.

For example, the goal statement in the SHSS for communications is to “enhance the existing statewide communications system.” Similarly, the DEMHS internal goals document contains the following goal for infrastructure: “continue the development of critical infrastructure plan for the State of Connecticut.” Perhaps a more informative goal for communications is actually found in the recently developed Statewide Communication Interoperability Plan, which states, “By 2015 agencies and their representatives at local, regional, and state level will be able to communicate (voice and data) using compatible systems, in real

time, across disciplines and jurisdictions, to respond more effectively and timely to day-to-day operations and major emergency situations.”

Typically, management literature emphasizes that well-designed goals and objectives are the product of five characteristics known by the acronym “SMART.”²⁹ That is they are: Specific (well defined); Measurable (know when it is achieved); Achievable (have stakeholder consensus); Realistic (acknowledge resource constraints); and Timely (have enough time to achieve goal). Most objectives have a date of accomplishment but not all do. For example, the expansion of CTIC has no date of accomplishment. Further, except for some general measures in the SHSS (which are not tracked or reported on – as discussed below), most objectives do not have any performance measures. It should be noted that DHS asks the department to provide a status of its SHSS goals and objectives. The federal monitoring report is the result of a self-evaluation that is reviewed by DHS. The results are considered “for official use only” and are not shared publicly by the department.

In addition, the accomplishment of goals and objectives is not systematically tracked and reported. The SHSS states that the department will, “at least biannually brief the EMHSCC in order that they may review the strategic goals, objectives, and implementation steps of Connecticut Homeland Security Strategy.” This has not been done. The council does assist in the creation of the goals and the department usually gives topical updates about its activities to the council and to the legislature, through its annual report. In the last few months and in response to program review inquiries, the department has begun to provide the council with a limited idea as to how the department’s activities relate to the accomplishment of the goals.

Basic notions of government accountability require that there be sufficient, credible, useful, and timely information about the effects of agency activities. Monitoring of performance is the only way to know if the resources and activities entrusted to government agencies are being managed efficiently and effectively, having the desired impact, and providing the highest possible quality service.

Therefore, the program review committee recommends **DEMHS should, when revising its state homeland security strategies and internal strategies, ensure that the goal statements provide a clear picture of what the department is trying to achieve and make certain all objectives have dates of accomplishment and meaningful performance measures. In addition, on at least an annual basis, DEMHS needs to develop a unified goals document that communicates the status of its goals and the results of its performance to the Emergency Management Homeland Security Coordinating Council and the legislature.**

Memorandum of Understanding

A memorandum of understanding between DEMHS and the Department of Public Safety has not been executed as required under law. In January 2005, DEMHS was created as a result of a merger of the Military Department’s Office of Emergency Management and the Department of Public Safety’s Division of Homeland Security. Under Public Act 04-219, the act that created

²⁹ George T. Doran, *There's a S. M. A. R. T. Way to Write Management Goals and Objectives*, Management Review (AMA Forum), November 1981, pps. 35-36.

DEMHS, the assigned personnel from DPS and the Military Department were under the sole direction of the DEMHS commissioner.

This authority was amended in the next legislative session by Public Act 05-256. This act specifies that the personnel assigned from those departments are under the “direction” of the DEMHS commissioner, but the public safety and military departments retain “administrative control” over state police officers and military personnel they assign to work in DEMHS. The act further requires that the DEMHS commissioner enter into an interagency memorandum of understanding with the other departments to provide for the temporary assignment and retrenchment rights of the DPS and military department employees and for interagency information sharing. The act limits personnel assignments under the memorandum to temporary assignments. DEMHS absorbed the employees from the military department obviating the need for an MOU. However, an MOU with public safety has not been executed.

The committee recommends that **the Department of Emergency Management and Homeland Security with the cooperation of DPS shall implement the provisions of C.G.S. Section 28-1a (e) relating to the creation of interagency memorandums of understanding.**

Notification of Federal Grant Award Reductions

DEMHS does not notify the legislature or seek additional state funding when federal grant funding is denied or reduced. Program review committee members have expressed concern that DEMHS has not received the full federal funding for which it has applied and demonstrated a need. In 2006, for example, DEMHS applied for \$30 million in federal funding and received \$13.5 million. Spending was reduced on all its initiatives, and one initiative was eliminated. In 2007, the department requested \$27 million and was awarded about \$10 million. Moreover the total amount DEMHS has received annually in federal funding has been reduced over the years. The department states that it prioritizes its initiatives and eliminates those it cannot afford. The department will also try to stretch existing resources to fill any gaps. DEMHS maintains that it does ask the legislature for funding to meet its most urgent needs.

The program review committee recommends **DEMHS shall notify the appropriations committee and the appropriate committees of cognizance in a timely manner of the status of federal grant funding when grant awards are less than what the department had applied for.**

Alternative Emergency Operations Center

As noted in the briefing report, *the state does not have an alternative site for the EOC.* The state EOC, located just west of the State Capitol, occupies the basement floor of the State Armory Building. This location currently accommodates spaces for the Governor’s office, a conference room, computer rooms, a media center, a communications center, a weather center, and other support areas.

Any alternative EOC facility would require emergency backup power, emergency fueling, secured perimeter, video surveillance and special air-handling equipment for security

reasons. It needs to provide seating for approximately 112 people with computer workstations and television monitors to operate as a command center in the event of an emergency.

In 2005, the Department of Public Works (DPW) developed a plan for alternate uses of the Connecticut Juvenile Training School (CJTS). Among the potential plan options considered was the use of the CJTS campus as a site for DEMHS offices and for the state EOC. However, the DEMHS commissioner reports that discussions for this site have ceased.

In his written testimony, the DEMHS commissioner mentioned the procurement of a mobile communications solution (discussed in the previous section) that allows first responders and emergency managers to establish a mobile emergency operations center wherever it is needed, or wherever it can be sustained during an emergency. DEMHS is also currently consolidating much of its staff into one centralized building in Hartford, which DEMHS reports will give the agency another work center in addition to the EOC. Other alternative sites that have been mentioned are Rentschler field in East Hartford or the former Southbury training facility that will soon house the DEMHS Region 5 offices.

The program review committee recommends **DEMHS, through a sub-committee of the coordinating council, should develop a plan to address the need for an alternative EOC no later than January 2009. In particular, the plan should outline all necessary EOC specifications and requirements and whether the alternatives currently being considered (e.g., mobile command center, Rentschler, Southbury) are viable and reasonable options. Once site requirements are determined, DEMHS, in conjunction with DPW, should identify potential alternative methods and/or locations available for the EOC.**

DEMHS and DPS Homeland Security Proposals

At the September 25, 2007 program review public hearing, some committee members asked that the commissioners of DEMHS and DPS provide the committee with a list of items needed to address the top concerns of their respective agencies regarding homeland security in Connecticut. Their responses are discussed below, and a copy of their formal written submissions is provided in Appendix G. Although committee staff met with each commissioner to discuss the proposals, the meetings could not be scheduled until late into the study process. As a result, committee staff was not able to fully evaluate these options and subsequently recommendations have not been made. Therefore, the following is provided for informational purposes.

DEMHS Response

DEMHS reported three priority funding issues. The first priority is funding for the local emergency relief account established by statute. The second priority is funding for continuous stockpiling of supplies such as generators and water. The third priority is funding for improvements to the five DEMHS regional offices.

Local emergency relief account. Under C.G.S. §7-520, the state has established a local emergency relief account. Account funds, when available, are provided to municipalities that apply to a 12-member local emergency relief advisory committee, which is headed by the

DEMHS commissioner. Municipalities must use the funds as reimbursement for emergency response costs for situations that posed an unusual and serious public safety threat and required immediate municipal spending, or as matching funds to qualify for federal aid.

Since 2001, the local emergency relief account has had little to no funding available. DEMHS officials did not know the reason for the historical lack of funding for this account. Nevertheless, DEMHS believes this account may serve an important function for localities experiencing events that do not quite satisfy federal requirements for emergency financial assistance. For example, funds may be available to a municipality for repair of public buildings after a flood, even if the total damage region-wide does not meet the thresholds under the federal Stafford Act for federal relief.³⁰ DEMHS' initial estimate for funding this account is \$1 million.

Stockpiling of supplies. Under C.G.S. §28-16, the DEMHS commissioner is empowered to purchase and maintain a stockpile of medical supplies, blankets, food and provisions, fuel, equipment, and any other supplies necessary to afford emergency relief and assistance to the residents of the state. The most recent DEMHS effort in this area was the purchase of sheltering cots. However, DEMHS believes *further stockpiling efforts for items such as medical supplies and personal protection devices such as masks are needed and must be maintained on an ongoing basis.* DEMHS suggests approximately \$1 million could be used towards this effort.

Funding for DEMHS regional offices. The third funding initiative DEMHS proposed was for improvements for the regional offices. DEMHS believes the current regional office locations are physically inadequate and advocates for relocation. As noted in the briefing report, the DEMHS Region 5 office is in the process of relocating to the former Southbury training school. DEMHS offices in Regions 1 and 4 are located in the lower levels of different state police barracks. DEMHS Region 2 occupies space in the Department of Public Safety headquarters in Middletown while the Region 3 office is located in the Department of Veteran Affairs complex in Rocky Hill.

Program review committee staff visited the DEMHS regional offices and agrees that *space limitations at DEMHS regional offices exist, considering the recent and anticipated expansion of DEMHS regional staff.*

DPS response

DPS submitted three long term proposals.³¹ One proposal would allow for a proactive response to possible bombing risks related to mass transit. Another proposal is the construction of a new Emergency Support Unit/Canine facility centrally located in Cheshire. The third proposal is an expansion of the truck inspection squad.

Mass transit squad. *DPS currently operates a mass transit squad on a limited basis.* DPS believes the squad delivers an efficient and effective method of providing enhanced security

³⁰ The Stafford Disaster Relief Act is the law that authorizes federal assistance when the President declares a state to be a disaster area. Financial assistance determination is based on a cost threshold that changes annually.

³¹ DPS reports that the cost estimates submitted in the DPS written response (see Appendix G) were prepared two years ago. The costs noted in this section are updated figures prepared by DPS.

and detection at mass transit locations such as train stations, bus depots, and airports. The DPS proposal would increase the number of canine detection teams and allow the agency to conduct more frequent, unscheduled sweeps of various mass transit locations within the state as well as at large public events. The sweeps would be of rail, bus, and ferry services looking for suspicious activities, packages, devices, substances, and individuals. DPS believes other identified key assets could be included in this program.

The Connecticut State Police now has four K-9's at Bradley Airport and six for statewide use. The DPS proposal would add 12 bomb dog teams to the existing contingent. Each team is composed of two troopers (one dog handler/one bomb technician). The enhanced unit would consist of 24 troopers in the field plus two additional K-9 trainers. The unit would operate on a full-time basis and use existing bomb technicians from around the state. DPS estimates the cost of this proposal to purchase equipment, dogs and hire additional troopers is approximately \$3.9 million. This proposal would increase CSP staffing above the authorized statutory level of 1,249 troopers.

Emergency Support Unit (ESU)/Canine facility. Built in 1967, the Emergency Support Unit is now located in a 5,000 square feet bay garage in Colchester. According to DPS, approximately 14 pieces of equipment must be stored outside, exposed to weather conditions significantly reducing their service lives. The equipment includes a bomb disposal truck, prisoner vans, weapons of mass destruction trailers, and riot equipment trailers.

In 1999, CSP was allocated \$7.2 million to design and build a new ESU facility in Cheshire. Plans for a new ESU facility call for a 14-bay garage that will provide approximately 25,000 square feet of space. It will also contain a K-9 training facility and a 30-dog kennel. DPS believes this facility could also centralize training locations that can be used for homeland security issues, such as Urban Search and Rescue, and it could serve as a center for regional training.

Earlier this year, an additional \$1.65 million was added by the legislature and the governor's office to cover inflationary costs. At the time the program review committee asked DPS for its top proposals, the bond money associated with this package had not been released, prompting DPS to submit this proposal as a top priority. However, the bond package containing the funding for this project was recently released, and the project is expected to continue.

Commercial enforcement staff. Pursuant to state law, DPS, in conjunction with the Department of Motor Vehicles, is responsible for conducting commercial vehicle inspections with specific staffing levels for enforcement activity. DPS has approximately 20 full-time troopers and nine weight and safety inspectors dedicated to commercial enforcement duties and responsible for meeting the statutory obligations of P.A. 98-248. There are an additional 50 troopers statewide conducting commercial enforcement duties as part of their patrol duties. According to DPS, general violations are found in approximately a third of truck inspections.

The squads are trained to inspect hazardous material vehicles and are equipped with personal radiation pagers and sophisticated radiological equipment that can detect the presence of nuclear material. During heightened security alerts, these squads may be required to work a

continuous rotation. The DPS proposal would add eight troopers specifically assigned to commercial vehicle inspection. According to DPS, this proposal would allow motor carrier safety assistance inspections to be conducted on a full-time, everyday basis as opposed to the manner in which current staffing levels permit. *Deployments of additional commercial enforcement personnel would permit inspections to occur statewide with emphasis on secondary roadways and would be separate and distinct from continuing weigh station operations.*

DPS believes that an enhancement of the squad could provide a greater measure of protection against the transportation of radiological and/or unauthorized explosive materials through the state as well as increase criminal enforcement and general public safety. DPS anticipates the fiscal impact associated with the hiring of eight troopers would be approximately \$1.2 million. This proposal would exceed the DPS authorized statutory staffing level of 1,248.