Recommendations and Proceedings of the Joint Homeland Security Task Force

Volume I: Report

January 31, 2002

Table of Contents

I. INTRODUCTION

Oklahoma understands all too well the brutality of terrorism. The April 19, 1995 bombing of the Federal Building in Oklahoma City is seared into the state's consciousness and taught the nation that terrorism can originate within our own borders. The devastating consequences of international terrorism became a profound reality to the citizens of the entire country on September 11, 2001 when terrorists turned commercial aircraft into suicide weapons of mass destruction and executed the deadliest strike on American soil in our history.

Just as the nation dealt with the aftermath of the December 7, 1941 attack on Pearl Harbor, we now face a similar challenge to meet the threat of terrorism. In the war against terrorism, there may never be total, unconditional victory. Rather, we are in a protracted battle that will test our resolve and commitment as a people and a nation. There will be victories and setbacks, but we must have the will to sustain the pressure on our foes for the long-term in order to achieve measurable success.

The State of Oklahoma has a responsibility to its citizens, as well as an obligation to the nation, to review its security posture and take steps to enhance security as required. While federal law enforcement agencies and the country's national security apparatus will be paramount in deterring terrorist acts throughout the United States and in mounting our national defense, there has been and will continue to be a crucial role for state and local government. In the first instance, with appropriate intelligence and associated investigative resources, state and

local officials can act as a key force in preventing and deterring terrorism. In light of the level of danger posed by weapons of mass destruction, prevention must be our first priority. No matter how good the response capability is, it would likely be overwhelmed in the event of an attack on a massive scale. Should we fail to prevent or deter an attack, state and local governments will certainly lead the emergency response just as they did in the wake of the Oklahoma City bombing, and the two World Trade Center and Pentagon attacks. The first response to terrorist events is primarily the task of local government augmented by the state. Finally, the state must also play a critical role in the realm of investigating and prosecuting terrorists, and those who aid them, under Oklahoma law.

Recognizing that the people of Oklahoma have an important role to play in advancing the homeland security effort now underway throughout the nation, Senate President Pro Tempore Stratton Taylor and House Speaker Larry Adair established the Joint Homeland Security Task Force to help the state of Oklahoma consider changes in its laws, regulations and policies in order to meet the challenges brought about by the September 11 terrorist attacks. Specifically, the President Pro Tempore and Speaker charged the Task Force with an examination of specific changes needed in state law or in appropriations to assist Oklahoma in countering terrorism. The composition of the Task Force was bi-partisan, equally divided between members of the House and Senate, and inclusive also of expertise from outside the Legislature.

In order to meet the deadline set forth by the President Pro Tempore and Speaker, the Task Force immediately commenced a series of hearings that took

place in Tulsa and Oklahoma City. Just as the September 11 attacks united our country behind the cause of homeland security, the Task Force conducted its work in a completely non-partisan manner, meeting with a broad range of experts and officials that included state agency heads, private sector representatives, federal officials, and public interest groups. Due to the fact that homeland security raises issues bearing on important civil liberties concerns and therefore demands a careful balancing of security and civil liberty interests, the Task Force also met with representatives from the American Civil Liberties Union and the Oklahoma Press Association. Similarly, the Task Force cooperated closely with other committees related to security in the wake of September 11, including the Governor's Security and Preparedness Executive Panel and the Governor's Task Force on Security for State Employees, to ensure that the state's efforts were well coordinated and complementary across the Executive and Legislative branches.

The report that follows details a number of recommendations for legislative actions to prepare Oklahoma to help fight terrorism and be better prepared to respond should an attack take place. Many of these changes in law and recommendations for public investment can and should be made immediately; others represent changes in policy or are large investments to upgrade security and technology that may take several years to implement.

It is the strong recommendation of this Task Force that the attention of the state to the cause of homeland security be constant, extended and sustained. This should not be a short term effort. Long after this Task Force adjourns, it is our

view that the state will have an ongoing obligation to review its security and emergency response infrastructures to assess potential areas of vulnerability, and to take action to fill gaps in security through a constant process of review and enhancement of homeland security. For this reason, our first recommendation is to formally task an Oklahoma official with the responsibility of overseeing homeland security for this state.

Today, the United States is experiencing substantial success on the military and diplomatic fronts throughout the world as the nation goes to war against Al Qaeda and international terrorism. Yet, the threat of renewed terrorist activity in the United States is substantial. On an almost weekly basis, our national leaders provide information about credible threats against the United States. We, in Oklahoma, also understand that we cannot forget the continuing threat of domestic terrorist individuals and groups. The outbreaks of the anthrax virus and the ensuing panic further awakened America to the potential impact of terrorism on our economy and our way of life, as well as the enormous danger inherent in the possibility that weapons of mass destruction could be used to further terrorist goals.

Each of us bears responsibility to aid the country in the war against terrorism. This Task Force's review of Oklahoma's security posture and the landscape of current law clearly demonstrate that more can and should be done at the state level. The following report is submitted to assist the Legislature and the people of Oklahoma in advancing the important cause of homeland security—on behalf of our state and the nation.

II. EXECUTIVE SUMMARY

The Homeland Security Task Force recommends eleven significant legislative actions in response to the directive presented by the President Pro Tempore and the Speaker of the House. Those eleven recommendations are briefly introduced in this Executive Summary and elaborated upon in the next section of the report.

Additionally the report contains a variety of specific suggestions heard or discussed by the Task Force that may support the implementation of the major findings. Also provided are supporting documentation of issues discussed, information and individuals resourced, and a brief synopsis of the creation and proceedings of the Task Force.

RECOMMENDATION #1

Vest responsibility for coordinating Oklahoma's homeland security in one cabinet-level official.

RECOMMENDATION #2

Amend the Criminal Code to include, among others, crimes of terrorism, financial support to terrorist groups, terrorist threats and false terrorist threats.

RECOMMENDATION #3

Enhance the State's intelligence collection capabilities and devote resources to the currently existing joint task force on terrorism that unites state and federal law enforcement officials in Oklahoma who collect information about terrorist networks operating in this region.

RECOMMENDATION #4

Fund the Digital Driver License Initiative and make the necessary legislative changes to require nationality information obtained in the Oklahoma Driver License application process be made readily available to law enforcement.

RECOMMENDATION #5

Oklahoma should evaluate and consider legislation granting emergency health powers to the Governor and public health authorities in the event of a terrorist act or public health crisis to protect the health, safety and well-being of the citizens of Oklahoma.

RECOMMENDATION #6

Institutions of higher education and entities providing vocational training related to potentially dangerous activities should conduct risk management surveys and take measures to enhance security.

RECOMMENDATION #7

Minor modifications should be made to the Open Records Act and the Open Meetings Act to exempt official materials related to intelligence about terrorist activities, assessments of vulnerability, and counter-terror measures that could educate terrorists about targets to strike.

RECOMMENDATION #8

Develop and fund a rational plan to upgrade and integrate communications systems for governmental entities on the front line in responding to public health emergencies, law enforcement incidents and terrorist attacks.

RECOMMENDATION #9

Take steps to dramatically increase security of the State's critical information systems and coordinate with the private sector to ensure preparedness for the threat of cyber terrorism.

RECOMMENDATION #10

Increase security at the Oklahoma State Capitol Building.

RECOMMENDATION #11

Require periodic assessments of the safety of ranching and agricultural enterprises, and of food processing. Develop plans for remediation in conjunction with the private sector to combat potential attacks on Oklahoma's food production and processing systems and operations. Fund the animal carcass digester project as recommended by the Governor's Advisory Panel and the Joint Legislative Task Force on Food Safety.

III. RECOMMENDATIONS

RECOMMENDATION #1

Vest responsibility for coordinating Oklahoma's homeland security in one cabinet-level official

Homeland security requires close cooperation and detailed coordination amongst a wide variety of governmental entities across all levels of government – federal, state and local. At the state level alone, critical agencies and officials include:

the Commissioner of Public Health,

the Commissioner of the Department of Public Safety,

the Director of the Office of Civil Emergency Management,

the Adjutant General of Oklahoma,

the Secretary of Transportation,

the Secretary of Agriculture,

the State Epidemiologist,

the State Bioterrorism Preparedness to Response Coordinator,

the Attorney General,

the Corporation Commission, and

the Director of the Oklahoma State Bureau of Investigation.

This list could be much longer in that it does not enumerate the large number of county and municipal officials who are essential to the task of preventing and responding to terrorist incidents. With this in mind, the Task Force believes it is imperative that one high-ranking Oklahoma official—the State Director of

Homeland Security--be given the authority and responsibility to develop and coordinate the state's homeland security efforts.

The Task Force recommends that the Director of Homeland Security should be appointed by the Governor for a term of six years, subject to confirmation by the Senate. The appointment should be made by the Governor from a slate of well-qualified nominees selected by a legislative nominating commission. The Director should be charged with reporting to the people of Oklahoma on the status of security within Oklahoma by providing the Legislature an annual report on the state's comprehensive security program. This person would also be charged with serving as Oklahoma's principal representative for interacting with the federal office of Homeland Security and in securing federal support for Oklahoma's Homeland Security program.

The Task Force spent considerable time discussing the particular structure required for the coordinating role of this official and the position's appropriate place in state government. We concluded that the Director should be a cabinet-level officer and tasked solely with homeland security duties, at least for the immediate future. In our opinion the State Director of Homeland Security needs to be a very high-level official who has:

The clear mandate to coordinate, review and evaluate state and local agencies responsible for Homeland Security.

The necessary funding and staff to carry out the mission. Although this task should not call for an exceedingly large outlay of funds or

staff, it should nonetheless be large enough to allow the Director to act as an integrator of state and local efforts.

The Task Force concluded that an initial budget of approximately $400,000 should be sufficient for the cabinet position recommended, and that appropriate legislative oversight of and interaction with this official is imperative.

After much discussion the Task Force agreed that in order to adequately coordinate homeland security efforts, a single individual with responsibility for directing the state's efforts was needed. The Task Force also agreed that this individual should not only have the responsibility over assets to be used in implementing the stated goals, but should also have commensurate authority in achieving them. It is recognized that the process for selecting a Director of Homeland Security poses both administrative and political challenges. The available options for such a process run the gamut from a direct appointment of a cabinet-level position by the Governor with confirmation by the Senate, to a selection by an independent Board or Commission for a specific term with removal from office only for cause.

Qualifications of the Director

The qualifications of the individual chosen should include a broad range of skills and talents. At the very least the individual should have:

An understanding of intelligence gathering, analysis, and distribution.

Knowledge of the function of state, federal, and local governments.

Knowledge of resources available, such as law enforcement, medical, and other first responders.

Substantial communication and managerial skills.

Leadership skills.

Ability to function in a political environment.

A dedication and enthusiasm for the task at hand.

After reviewing the political and logistical parameters associated with selecting a Director, the Task Force suggests consideration of the statutory creation of a Homeland Security Nominating Commission, whose sole role would be to evaluate applicants for the position and submit three to five names to the Governor for his consideration. The Governor would choose from that list in the same manner as judicial nominees are submitted and chosen. The Governor's choice would then be subject to Senate confirmation. It is further recommended that the term of the Director should be six years, and that the Director be subject to removal for cause only. This six-year term is modeled after the term of years structure that exists for the head of the FBI and is designed to insulate the position from politics to a great extent and to ensure that the state can recruit an outstanding individual to fulfill this role. Finally, during the hearings and discussions of the Task Force, a consensus was reached that the proposed State Director of Homeland Security should have no other responsibilities in state government. Specifically, the Task Force recommends that the Director should be precluded from being an agency chief administrator.

Legislation

It is a relatively simple task to delineate the responsibilities of an office of Homeland Security. It is a much more difficult matter, however, to establish authority for such an office. Given the fact that the Director of Homeland Security will be utilizing assets within state, federal, and local agencies, the Task Force believes it is imperative to require the cooperation and assistance of agencies over which the state has jurisdiction. We would recommend that language be crafted directing all agencies of the state and its subdivisions to render assistance and cooperation to the Office of Homeland Security. The Task Force further recommends that failure to render such assistance and cooperation may result in removal from office.

(Additional discussion of Task Force issues, resources utilized, and additional recommendations heard by the committee can be found in Section 4.1 of the Proceedings section of this report.)

RECOMMENDATION #2

Amend the Criminal Code to include, among others, crimes of terrorism, financial support to terrorist groups, terrorist threats and false terrorist threats.

Several states around the country have acted rapidly to amend their criminal codes to include new crimes related to the offense of terrorism. The State Attorney General provided the Task Force with a number of recommended

additions to the criminal laws of Oklahoma in light of the September 11 attacks and the continued threat that exists.

In sum, the Task Force recommends that the Legislature adopt the Attorney General's suggested amendments to the criminal code, including his suggestions to:

Criminalize the offense of terrorism.

Criminalize material support – including funding support – to terrorists.

Criminalize the making of terrorist threats, as well as the making of false threats or perpetrating hoaxes related to terrorism.

List terrorism as a predicate crime under the racketeering statutes.

In conjunction with the above amendments to the criminal law, the Task Force recommends increased civil remedies under forfeiture powers related to investigation or prosecution of terrorist activities.

(Additional discussion of Task Force issues, resources utilized and additional recommendations heard by the committee can be found in Sections 4.2 and 4.4 of the Proceedings section of this report.)

RECOMMENDATION #3

Enhance the State's intelligence collection capabilities and devote resources to the currently existing joint task force on terrorism that unites state and federal law enforcement officials in Oklahoma who collect information about terrorist networks operating in this region.

Terrorists have a wide constellation of prospective targets from which to choose. It is impossible to fully secure every building and mitigate all vulnerability. Therefore, a primary objective of counter-terrorism strategy must be to identify and apprehend terrorists and their supporters before they execute their plans. Historically, the states have ceded anti-terrorism investigations to the federal agencies. Yet, the network that perpetrated the September 11 attacks demonstrates the deep roots certain terrorist cells have planted within the United States, thereby highlighting the important role that state and local law enforcement authorities have in monitoring potential terrorist cells and their supporters.

In order to strengthen intelligence capabilities at the state level, the Task Force recommends that the Oklahoma State Bureau of Investigation Intelligence Enhancement Program be funded. This program would provide new and enhanced "all source" services in the area of terrorism intelligence, including field training on collecting, analyzing and disseminating intelligence, and would provide more than a dozen professionals in the area of criminal intelligence. Included in the twelve new positions would be four special agents assigned to the Oklahoma Joint Terrorism Task Force—a team made up of both state and federal officials, including the Federal Bureau of Investigation. The Oklahoma

Joint Terrorism Task Force is fully devoted to the cause of counter-terrorism and has responsibility for coordinating intelligence efforts at the federal and state level under the sponsorship of the FBI. It also serves as a mechanism for the increased sharing of intelligence among state, local and federal agencies that is so vital to homeland security. Under the proposed plan of the OSBI, senior criminal intelligence analysts would be tasked to analyze intelligence reports on terrorism from all sources and to maintain the Statewide Intelligence Network database. This plan would also train two special agents in the arena of cyber terrorism, an emerging threat against the information systems of the government and the private sector.

The cost involved to fully fund the program as proposed by the OSBI is $1.2 million. The decision concerning full or partial implementation of this important initiative should be made with the input of the newly created Director of Homeland Security, who could best determine the appropriate level of investment in this specific program and how it relates to the state's total effort.

(Additional discussion of Task Force issues, resources utilized and additional recommendations heard by the committee can be found in Section 4.1 of the Proceedings section of this report.)

RECOMMENDATION #4

Fund the Digital Driver License Initiative and make the necessary legislative changes to require nationality information obtained in the Oklahoma Driver License application process be made readily available to law enforcement.

The Task Force heard testimony from various witnesses in the law enforcement arena about the need to digitize driver license information in Oklahoma. Witnesses indicated that this effort has been underway for some time but has never been fully funded. The members of the Task Force concluded that this is an important step in equipping the law enforcement community with the sophisticated tools necessary to pursue a robust counter-terrorism strategy.

Oklahoma, like several other states, collects information on applicant nationality and the jurisdiction of any previous driver license issued. This data is collected upon application for an Oklahoma driver license. The Task Force recommends that nationality information obtained during the driver license application process be provided in a form readily available to law enforcement. This step, in conjunction with the digitization initiative and improved monitoring of immigration procedures at the federal level, should help in the national effort to better monitor the legal status of foreign nationals and improve enforcement of visa restrictions—both of which have been identified in the wake of the September 11, 2001 attacks as seriously deficient.

It is estimated that an initial $250,000 is required to fund this initiative, with the ultimate cost totaling $5 million by completion in 2004. Because of prior action

taken by the Legislature to create a funding stream for this project, no ongoing appropriations will be necessary. The Task Force further suggests that including additional biometric data on Digital Driver Licenses remain under review during this process.

(Additional discussion of Task Force issues, resources utilized and additional recommendations heard by the committee can be found in Section 4.2 of the Proceedings section of this report.)

RECOMMENDATION #5

Oklahoma should evaluate and consider legislation granting emergency health powers to the Governor and public health authorities in the event of a terrorist act or public health crisis to protect the health, safety and well-being of the citizens of Oklahoma.

Emergency health threats, including those caused by bioterrorism and epidemics, require the exercise of extraordinary government functions. The legislation proposed to the Task Force by the Commissioner of the State Department of Health grants specific emergency powers to the Governor and public health authorities. These powers could only be activated in the event of a declared public health emergency upon advice of public health officials and subsequently deactivated after the emergency passes. In the event of a public health crisis, such as an incident involving bioterrorism, the Act would confer upon the Governor the authority to collect certain data and records, as well as authority to utilize property for the care, treatment and housing of patients and for

the destruction of contaminated materials. Additionally, analogous legislation could expedite state bidding processes in a time of true emergency so that, for example, purchases of lifesaving equipment could be made with great speed.

This proposal clearly raises fundamental civil liberty concerns, especially when the highly complicated issue of quarantine is raised. Also of concern is the use of emergency powers in tandem with the line of succession to the Governor's office. The succession question is further complicated by the fact that the Lieutenant Governor or other surrogate of the Governor may not have the federal security clearance and hence the ability to learn certain information to make judicious decisions in this regard. At the same time, the devastating consequences of a successfully executed biological or chemical attack could be aggravated to an extreme degree in the event that such powers and/or security clearances are not in place. Therefore, the Task Force recommends that this issue receive additional scrutiny. The exercises planned for April 2002 in which state and local agencies will react to a mock bioterrorism event should be used to assess the necessity for legislation along the lines of the Emergency Health Powers Act.

(Additional discussion of Task Force issues, resources utilized and additional recommendations heard by the committee can be found in Section 4.5 of the Proceedings section of this report.)

RECOMMENDATION #6

Institutions of higher education and entities providing vocational training related to potentially dangerous activities should conduct risk management surveys and take measures to enhance security.

Institutions of learning are vulnerable to exploitation by terrorists. The use of flight training schools to prepare for the September 11 attacks should serve as a wake-up call for similar training facilities as they impart valuable skills that, in the wrong hands, can be put to sinister uses. However, the threat of terrorist exploitation goes beyond training institutions and includes the full panoply of higher education. Some of these vulnerabilities are as obvious as poor security in buildings that house dangerous chemicals or store sensitive technologies. Other vulnerabilities are far more complicated, such as the question of poor monitoring of foreign national students who may be in violation of visa requirements. While the federal government is seeking to better enforce current immigration law and to tighten controls on student visas, there is a role for educational institutions in assisting the immigration and naturalization services so that better monitoring of foreign national students for compliance with visa requirements can be achieved.

The Task Force spent considerable time hearing from witnesses concerning the dangers that exist related to educational institutions. At the very least, the Task Force recommends that every higher education institution in the state be required to submit risk assessment evaluations related to terrorism along with the institution's plans for remediation of those risks. All training facilities related to

flight training or commercial vehicles should also be required to conduct similar assessments and remediation studies. It is further recommended that all such assessments be submitted to the proposed Director of Homeland Security as soon as possible.

(Additional discussion of Task Force issues, resources utilized and additional recommendations heard by the committee can be found in Section 4.3 of the Proceedings section of this report.)

RECOMMENDATION #7

Minor modifications should be made to the Open Records Act and the Open Meetings Act to exempt official materials related to intelligence about terrorist activities, assessments of vulnerability, and counter-terror measures that could educate terrorists about targets to strike.

In many Task Force hearings, witnesses presented testimony reflecting a concern—particularly in the private sector and among some federal officials—that sharing sensitive information with state officials about terrorism or specific vulnerabilities to terrorist attack might result in those officials ultimately disclosing that information pursuant to current "open records" and "open meeting" statutes. The Task Force found that it was unclear whether state law truly puts that type of information at risk. However, in light of the ambiguity of the statutes, the Task Force recommends that minor modifications be made to clarify that information about potential terrorist attacks or information relating to vulnerability

assessments and counter-terror measures should definitely be exempt from the disclosure regimes of these statutes.

(Additional discussion of Task Force issues, resources utilized and additional recommendations heard by the committee can be found in Section 4.2 of the Proceedings section of this report.)

RECOMMENDATION #8

Develop and fund a rational plan to upgrade and integrate communications systems for governmental entities on the front line in responding to public health emergencies, law enforcement incidents and terrorist attacks.

The Task Force heard testimony from witnesses across state government who identified the need to transform the communications infrastructure used by police, fire and public health officials so that the systems could be interoperable and integrated with one other, especially in emergency situations such as a terrorist attack. The Task Force fully understands the critical role of reliable and compatible communications in dealing with emergencies of all kinds. Numerous plans have been presented over the years to accomplish a part of this task, including a $52 million proposal to develop an 800 MHz system. The Task Force shares the view that such a communications upgrade for our public health and safety response infrastructure is critical. Yet, despite years of proposals on the shelf, it appears the state has not looked into this matter from a holistic, comprehensive perspective, and that there may well be better and cheaper ways to accomplish the basic objective. For this reason, the Task Force recommends

that the Legislature require the proposed Director of Homeland Security to develop a comprehensive proposal to address this issue and to present it to the Legislature as soon as possible. This proposal should make every effort to identify ways to meet, in a cost effective manner, the objectives proposed in earlier discussions of the issue. Clearly this is a critical and complicated issue. For this reason, it is the opinion of the Task Force that this must be addressed by an expert in order to leverage what has already been done and to best determine the next steps.

(Additional discussion of Task Force issues, resources utilized and additional recommendations heard by the committee can be found in Section 4.5 of the Proceedings section of this report.)

RECOMMENDATION #9

Take steps to dramatically increase security of the State's critical information systems and coordinate with the private sector to ensure preparedness for the threat of cyber terrorism.

The effort to protect our state and nation will not be adequate unless we recognize the degree to which critical aspects of our health, security, welfare and way of life currently rely on the security of our computers, internet connections, and other types of connectivity. It is imperative that the state recognizes the need to protect against this threat. Specifically, the Task Force recommends that the state's cyber-terror detection capabilities be enhanced by increasing the

number of personnel within the OSBI who are trained in this area and by requiring them to interact with federal officials in this field. The state should also invest in trained cyber-security personnel to assist state agencies in auditing their information systems to assess vulnerability to attack and to evaluate cost-efficient ways to safeguard their systems. Particular emphasis should be placed on those agencies which, if its information systems were undermined, would have serious adverse public consequences. In order to achieve maximum effectiveness, it is crucial that any efforts undertaken in this area must be coordinated with the private sector, including internet service providers, telecommunications companies, and major corporations.

(Additional discussion of Task Force issues, resources utilized and additional recommendations heard by the committee can be found in Section 4.3 of the Proceedings section of this report.)

RECOMMENDATION #10

Increase security at the Oklahoma State Capitol Building.

The Task Force received a briefing concerning security at the Capitol and discussed the findings of the Task Force on Security for State Employees. Enhancements to the security posture of the State Capitol are essential as the Capitol is the heart of Oklahoma government and a public space of central symbolic importance to the people of the state. Modest investment in the security of the Capitol, along with minor changes in procedures, would yield

significant security improvement. It is the recommendation of this Task Force that such investment and such changes should be made.

(Additional discussion of Task Force issues, resources utilized and additional recommendations heard by the committee can be found in Section 4.6 of the Proceedings section of this report.)

RECOMMENDATION #11

Require periodic assessments of the safety of ranching and agricultural enterprises, and of food processing. Develop plans for remediation in conjunction with the private sector to combat potential attacks on Oklahoma's food production and processing systems and operations. Fund the animal carcass digester project as recommended by the Governor's Advisory Panel and the Joint Legislative Task Force on Food Safety.

The Task Force heard considerable testimony concerning the protection of livestock, agricultural production and food processing. The vital nature of the food production chain, as well as the importance of food production to the state's economy, has led the Task Force to single this area out as a high priority for the proposed Director of Homeland Security. The Task Force believes that a comprehensive plan is needed to coordinate all levels of governmental resources with farmers, ranchers, food transportation middlemen, suppliers of fertilizer and pesticides, crop dusting operators, food storage companies and grocers. Such a plan is necessary in order to adequately protect the safety of food grown or

processed in the state, not only for the sake of Oklahoma consumers and producers, but for the consumers of Oklahoma food products throughout the nation and the world. The cost of the animal carcass digester is $1.5 million. This item was identified by the Oklahoma Food Safety Task Force as a “highest priority” item. The digester is necessary to dispose of highly infectious materials that cannot be destroyed in the incineration process.

(Additional discussion of Task Force issues, resources utilized and additional recommendations heard by the committee can be found in Section 4.5 of the Proceedings section of this report.)

IV. PROCEEDINGS OF TASK FORCE

On November 9, 2001 Senate President Pro Tempore Stratton Taylor and Speaker of the House Larry Adair created the Joint Homeland Security Task Force. The Task Force was charged with:

Reviewing existing security and emergency response infrastructure.

Assessing potential shortcomings and points of vulnerability.

Developing strategies for strengthening security and response efforts.

Recommending specific law changes or appropriations to assist Oklahoma in meeting the terrorist threat.

Interacting with executive branch Task Forces as necessary to accomplish its tasks.

The members of the Joint Task Force on Homeland Security are:

Citizens:

Mr. Ken Levit (Chair)
President of the University of Oklahoma-Tulsa

Dr. Sujeet Shenoi
Professor of Computer Science, Tulsa University

General Dennis J. Reimer (Ret.)
Director of the National Memorial Institute for the Prevention of Terrorism

Senate Members:

Glenn Coffee

Billy Mickle

Jim Reynolds

Dick Wilkerson

House Members:

John Nance

Bill Paulk

Dan Webb

Dale Wells

Task Force Hearings

The Task Force met 10 times between November 13, 2001 and January 31, 2002 in a combination of public and executive sessions. The meetings took place at the State Capitol and University of Oklahoma's Schusterman Center in Tulsa. Following is a listing of the wide variety of experts who gave testimony to the Task Force:

First Meeting: November 13, 2001

Bob Ricks
Cabinet Secretary of Safety and Security, and Commissioner of Public Safety

Dr. Robert Petrone
Oklahoma State Department of Health

Second Meeting: November 27, 2001

Dr. Stephen Sloan
University of Oklahoma, Political Science Department

Drew Edmondson
Attorney General for the State of Oklahoma

DeWade Langley
Director of the Oklahoma State Bureau of Investigation

Richard Marquise
Special Agent in Charge, FBI

Third Meeting: December, 3, 2001

No Witnesses

Fourth Meeting: December 11, 2001

Leslie M. Beitsch
MD, JD, Commissioner, Oklahoma Department of Health

General Robert A. Goodbary
Director, Office of Military Relations, OSU

Fifth Meeting: December 14, 2001

Howard Barnett
Chief of Staff, Office of the Governor

Sixth Meeting: December 18, 2001

Albert Ashwood
Director, Department of Civil Emergency Management

Sujeet Shenoi
Ph.D., University of Tulsa

Drew Edmondson
Attorney General for the State of Oklahoma

Seventh Meeting: January 4, 2002

JoAnn Bell
Executive Director, Oklahoma ACLU

Mark Thomas
Executive Vice President, Oklahoma Press Association

Bob Ricks
Cabinet Secretary of Safety and Security, and Commissioner of Public Safety

Eighth Meeting: January 11, 2002

Robert M. McNamara, Jr.
Managing Director, Manatt Jones

Tom Holland
Manager, Phillips Global Security

Major General Stephen Cortright
Adjutant General of Oklahoma

Representative James Covey
Chair of the Oklahoma Food Safety Task Force

Ninth Meeting: January 18, 2002

Curt Hopfinger
Vice President, Regulatory, Southwestern Bell Oklahoma

John Howle
Director, Central Office Operations, Southwestern Bell Oklahoma

Lance Thomason
Area Manager, SBC National Security Preparedness, Michigan

Kerry Wagnon
Program Director, Capital Safety Projects in Oklahoma City

Danny George
Executive Director, Oklahoma Municipal League

Meeting notices and agendas of the Task Force hearings are included in the appendix of this report in addition to handouts and resource materials provided to the Task Force.

Part of the charge of the Joint Homeland Security Task Force was to work with other state government groups that are addressing security issues. One of these groups, the Task Force on Security for State Employees, was charged by the Governor with the task of recommending security measures for the Capitol building, the Capitol complex, and other state facilities. The Joint Homeland Security Task Force heard testimony from the Chair of the Task Force on Security for State Employees, Bob Ricks. Another member of that Task Force, Senator Dick Wilkerson, is also a member of the Joint Homeland Security Task Force and served as liaison between the two groups.

Another group dealing with state security issues is the Governor's Security and Preparedness Executive Panel, which was given the much broader task by the Governor of developing, coordinating and implementing a comprehensive state strategy to protect the citizens of Oklahoma from the threat of terrorist attacks. The Joint Homeland Security Task Force heard from the Chair of that panel, Howard Barnett, regarding its work. Both prior to and following that testimony, the Chair of the Joint Homeland Security Task Force, Ken Levit, and Howard Barnett met on several occasions to discuss the findings of their respective groups in an effort to coordinate the state's response to terrorism. Additionally, a member of the Joint Task Force, General Reimer, also serves on the Governor's Executive Panel.

Discussion of Issues

4.1-Vesting Responsibility for Homeland Security in One Office

The Task Force reviewed a number of different accountability models in the course of its hearings and discussed the pros and cons of different approaches. The review included an overview of how other states are addressing the homeland security accountability problem. Some states, such as New Jersey, have set up a permanent statutory homeland security commission to provide ongoing coordination and oversight. Other states, such as Massachusetts, Missouri and North Dakota, have appointed homeland security "czars" to vest powers. Much of the Task Force's discussions centered on this issue of how best to vest accountability in the homeland security arena. One participant made the point by simply stating that there was a need to "put someone in charge."

The discussions of the Task Force pointed out that Oklahoma's situation is relatively unique in that the Oklahoma Constitution disperses power not only among the three branches of government, but also within the executive branch. Many key agencies involved in homeland security report to governing boards that do not have direct accountability to their cabinet secretary or even the Governor. In fact it was pointed out that Oklahoma's cabinet system is overlaid on a system of agency boards, and has very little real day-to-day management or budgetary authority.

This dispersal of authority makes it difficult to put a single individual in charge of activities that, by their very nature, cross multiple lines of authority. Recognizing

that such challenges existed, the Task Force was nonetheless adamant in its recommendation to vest authority in one person. It was suggested that the Governor name the Director of Homeland Security, but that confirmation by the Senate also be required. Another suggestion, which was ultimately put aside, was to name an existing, relevant, cabinet official as the Director of Homeland Security. However, the discussion of the Task Force ultimately concluded that the Director's office should reside in the Governor's Office. Its location there was perceived to have a two-fold benefit. First, during an actual emergency the Director of Homeland Security would be directly available to advise and coordinate the response of the Governor's staff along with the rest of the executive branch. Additionally, during non-emergency periods a location in the Governor's office would provide a degree of legitimacy to the Homeland Security Director's planning efforts.

There was significant discussion of how the Director would be appointed and for how long. Some Task Force members believed the Governor should be presented with a slate of potential candidates from which he would choose. It was argued this would help insulate the Director from politics. Such a process would mirror the judicial nominating process. Others felt that the Director should be chosen directly by the Governor, with the advice and consent of the Senate. Only in this manner, it was argued, would the position have the requisite authority of the Governor's Office.

There was also considerable discussion as to whether the Director of Homeland Security should have a term co-terminus with the Governor's term, or whether

the position should be similar to that of the FBI director on the national level, who has a term of ten years. In either case it was felt that the new Governor elected in November of 2002 should have the right to be involved in the selection of the first Homeland Security Director. This would mean that anyone appointed to this position prior to January, 2003 should be an interim appointment.

4.2-Enhancing Intelligence Gathering Capacity: Issues and Discussions

The Task Force spent a significant amount of time discussing the merits of enhancing Oklahoma's intelligence gathering resources. Numerous experts told the Task Force that enhanced intelligence information is a key component in preventing terrorist activities. This position was expressed not just by law enforcement officials, but by other witnesses as well, such as Professor Stephen Sloan from the University of Oklahoma and the former General Counsel of the CIA, Robert M. McNamara, Jr. Unfortunately, intelligence capacity at the state level has been somewhat neglected, for a variety of reasons, since the mid-1970s. Growing distrust of the intelligence gathering capabilities of law enforcement agencies, spurred on by the events of Watergate and revelations of inappropriate and illegal use of such intelligence by the Hoover-era FBI, made many justifiably suspicious of such operations. The events of September 11, however, have made it necessary for intelligence gathering capacity to be enhanced once again. There was much discussion regarding this capacity and the role of legislative oversight, as well as the need to consider the dynamic tension between enhanced intelligence gathering activities and safeguards to civil liberties. The Task Force spent significant time listening to testimony from the Oklahoma Civil Liberties Union and the Oklahoma Press Association regarding concerns about open information and infringement of constitutional rights. The recommendations in this report attempt to strike the right balance between protecting our citizens and protecting the civil liberties that make us a great nation. Nonetheless, the challenge we face is unique, and fresh thinking is required to ensure we remain "safe and free".

Oversight of Intelligence

As it is a new and sensitive area for state legislatures, the issue of intelligence oversight was important for the Task Force, but one which did not result in any ironclad conclusions. Recognizing that intelligence is a key factor in preventing acts of terrorism on U.S. soil, the Task Force also understood that domestic intelligence is a sensitive issue and requires the utmost care to ensure a balance between the rights of citizens and their safety. Several different ideas were put forth to allow for effective oversight of intelligence activities while maintaining necessary confidentiality:

> Allow the presiding officers of the State Senate and the State House of Representatives to designate three members to serve on a Joint Oversight Committee on Intelligence. Two members from each body's majority party and one member from the minority party (with selection input from the minority leader) would be appointed. This Joint Committee would meet whenever necessary, but at least twice a year, and would receive briefings in private. During those briefings members would have access to confidential documents which would remain in the room.
>
> Another alternative that was discussed was the use of existing committees of the House and Senate---such as the new House standing Committee on Homeland Security---as oversight bodies. Appropriations subcommittees and/or standing committees such as the Judiciary Committee could also be used.

Open Records and Open Meetings

There was significant concern expressed by a number of witnesses testifying to the Task Force that modifications were needed to the Open Records and Open Meetings Acts to protect sensitive information and intelligence. Some of these concerns included:

> Private sector organizations are currently reluctant to share certain information with the state for the purposes of threat assessment and response plans because they fear the information will become public. Such proprietary information includes descriptions of power generation grids, computer systems, pipelines, and company security systems.
>
> Potentially sensitive public sector information about assets such as college laboratories, Grand River Dam Authority facilities, OneNet, and water supplies were also reported to be subject to disclosures associated with Open Records and Open Meetings laws.

The task force understands these concerns and believes there is validity to them. Recent information provided by the National Conference of State Legislatures (NCSL) indicates that other states are also struggling with such issues. NCSL reports that administrators are particularly concerned about sunshine laws that require public access to security assessment information or asset vulnerability data. Furthermore, water systems, dams, power systems, and computer systems are all vulnerable to cyber terrorism with knowledge of system

configurations. Such system configuration data may also need protection when associated with a critical state asset.

The OSBI provided a specific recommendation to amend the Open Records Act to exclude terrorism vulnerability assessments, investigations and related materials from disclosure. The Oklahoma Press Association counseled that they would prefer a specific list of documents that would be excluded from the Act, rather than wording that dealt with "related materials." One approach would be to add a "laundry list" of the types of documents necessary to be excluded. It was suggested by one committee member that this provision should mirror federal law.

The Open Meetings Act already has broad language in it that could be used to conduct hearings on intelligence in closed session. This language, however, is subject to interpretation. Discussions in the Task Force indicated that the members believed further clarifications of the Act to specifically include discussions of homeland security, security assessments and terrorism investigations would be useful.

Existing Intelligence Resources

The Task Force recognizes that the State of Oklahoma already has many intelligence gathering resources. The chief concern of the group, however, is that those resources are properly coordinated and utilized to prevent terrorism within our boundaries. Experts explained to the Task Force that the intelligence gathering process is already used in dealing with gangs, drug cartels, and other

forms of organized crime and can therefore be modified to fit terrorist cell activity. The Task Force received information that local law enforcement will need training in the techniques of gathering critical intelligence, particularly in rural areas that may contain vulnerable assets such as pipelines, electric generating plants and transmission lines.

Experts in this area recommended, and the Task Force agrees, that additional training be provided to state and local law enforcement agencies in both the metropolitan areas and rural parts of the state. The issues of intelligence gathering and additional training were thought to be essential by the Task Force. Moreover, they are issues that must be done correctly and with considerable dispatch.

Intelligence Recommendations

State intelligence gathering is a law enforcement function. Therefore, a key premise in developing a homeland intelligence function is to criminalize terrorism and terrorism-related activities. Although such acts are oten already illegal under federal law or perhaps under a related state provision, the Oklahoma Attorney General clearly indicated that enhancement of the criminal law would better enable the law enforcement community to monitor persons and activities that have a nexus to terrorism. In this vein, the Attorney General and other law enforcement officials asked the Legislature to:

> Enact new statutory language in Oklahoma State Statute, Title 74, Section 150.2 that would add terrorism to the list of crimes which

the OSBI may collect information on. This recommendation would allow OSBI to appropriately apply enhanced intelligence gathering methods to the prevention of terrorism as well as the apprehension of terrorists. The Attorney General recommends making this crime punishable by any term of years up to and including life imprisonment. (See 4.4-Criminal Law Amendments sections.)

Further strengthen intelligence and investigative powers by adding terrorism to the list of crimes that fall in the category of "racketeering." (See 4.4-Criminal Law Amendments sections.)

Include carrying a weapon as a licensed security guard in the gun permit prohibitions for foreign nationals on work or student visas;

Enhance OSBI capabilities by adding eighteen FTE (10 special agents, 4 senior intelligence analysts, 2 MIS programmers, 1 training officer, and 1 grant administrator). Additional details of the OSBI plan are provided in the agency's Intelligence Enhancement Program Business Plan (see appendix). Total cost estimated by the OSBI for their program was $1.2 million. The Task Force feels this enhanced capability is necessary, but would leave the exact funding amount to be determined by the Director of Homeland Security.

The Legislature should require intelligence training as a part of CLEET Basic Academy education. This would ensure that all local law enforcement personnel would have a basic understanding of the purposes and techniques of intelligence gathering and would

provide a foundation for further training. The exact curriculum should be developed by OSBI and validated by the Homeland Security Director.

Provide resources for the OSBI to develop the capabilities to undertake cyber terrorism investigation in mainframe and/or networked computer systems. Although the OSBI currently does not have this capability, experts testifying before the Task Force indicated that this is a likely target for future terrorist activity. This capability would be in addition to 6 FTE currently allocated by the Legislature for a computer crimes unit.

Expedite funding for digitalized driver license photographs. Such a system would make licenses more difficult to duplicate and help law enforcement identify altered licenses. Unlike traditional cards currently in use in Oklahoma, the photos on digitalized licenses are printed right into the card itself and cannot be altered without being destroyed. A similar system implemented in 1999 in Arkansas cost $10.4 million.

4.3-Cyber and Campus Terrorism Issues

The Task Force was fortunate to have as one of its members a leading expert on cyber terrorism, Dr. Sujeet Shenoi. Dr. Shenoi's presentations to the Task Force on cyber terrorism were illuminating and highlighted a threat arena that needs further attention by the state and nation.

The growth of the internet and its convergence with communications networks has produced extraordinary opportunities -- we are connected wherever we are, whenever we want. But our vital systems are likewise connected -- computers that control our power grid, vast segments of our public telephone networks, process control systems in our oil refineries, computers aboard U.S. Navy vessels, and even critical FAA systems.

Therefore, in theory at least, anybody with the knowledge and a satellite phone -- even someone hiding in a cave in Afghanistan -- can cause power and telephone outages, to adversely impact refinery operations, or potentially launch missiles from Navy ships. Compromising FAA systems makes it possible to affect -- not four aircraft -- but 400, perhaps even 4,000 at one time. After September 11, 2001 we cannot underestimate the intelligence, malice and determination of the adversary.

Indeed, cyber attacks, because of their massive force multiplier potential and the fact that they can be dispatched from a distance, can be launched individually, in conjunction with traditional attacks, or with chemical and biological attacks to wreak more death and destruction. Cyber attacks are also appealing to adversaries because of their diversity, ease of use, and low cost. Moreover, the asymmetric nature of cyber attacks makes it impossible for a highly “wired” country like the United States to respond to these attacks in kind.

Ultimately, all of American society is vulnerable to cyber attacks. The federal government is hard pressed to protect and defend its own electronic assets, let

alone provide security for assets belonging to state and local governments or the private sector. It is therefore imperative that the Legislature take serious steps to protect the state's vital electronic assets.

The Joint Homeland Security Task Force heard the following recommendations from Dr. Shenoi:

Provide additional computer security personnel and resources to OSBI and law enforcement agencies.

Require all state agencies to conduct internal audits, identify vulnerabilities, and develop countermeasures and back-up plans.

Foster cooperation and information sharing between state agencies, the private sector and universities about critical information systems.

Promote "best security practices" and proactive rather than reactive efforts in this field.

Create a state "Director of Homeland Security."

Create a state "Director of Cyber Security."

Create a "Standing Committee" dealing with terrorism and cyber terrorism.

Create a framework for confidentiality between the private and public sectors in the arena of technology and telecommunications.

Continually assess system vulnerabilities.

Develop countermeasures and back-up plans to the threat of cyber terrorism.

Promote science/technology/ethics education.

Foster the ideal of service to state and country within the technology community.

Campus Security

The Task Force heard a presentation from General Al Goodbary, Director of Military Relations at Oklahoma State University. General Goodbary pointed out that student populations and university research and development and laboratory facilities are all potential areas of concern for state governments. Recommendations heard by the Task Force relating to campus security include:

Require the Oklahoma State Board of Regents to direct each campus to develop a security plan that deals with student safety, laboratory safety, evacuation plans, and coordination with local municipal officials.

Require Oklahoma Colleges and Universities to monitor and report the status of foreign students to the OSBI.

Develop a student security registry.

Develop and enforce course entrance requirements for sensitive courses.

Enhance laboratory security on campuses.

Secure computer systems from potential attack.

In addition to developing campus response and security measures, colleges and universities can also serve as general resources to the state in combating terrorist attacks. For example, improvements to a sophisticated, level-three

bioscience laboratory at the University of Oklahoma could greatly assist the state in heading off serious consequences associated with a bioterrorism attack by quickly evaluating the relevant substance and determining its dangerousness. A specific proposal and budget for such laboratory improvements are included in the appendix. Similarly, support to the substantial sensor technology work now underway at Oklahoma State University could provide additional safety to the citizenry of Oklahoma and the country.

4.4-Criminal Law Amendments

Attorney General Drew Edmonson addressed the Task Force twice. The Attorney General recommended the following law changes to the Task Force members to deal with security issues:

> Criminalize the activities of knowingly raising, collecting, or soliciting funds or other material support for a terrorist organization. Criminalize knowingly providing support with the intent that material support or resources will be used to plan, prepare or carry out, or avoid apprehension for committing terrorism. Make such crimes punishable by up to twenty years in prison.
>
> Proscribe the act of communicating a terrorist threat which one knows to be false. Make it punishable by up to twenty years in prison.
>
> Prohibit the manufacture, distribution, use, attempted use or possession of fraudulent identification documents, including

passports, driver licenses, and biometric data. Strengthen the requirements to obtain a copy of such documents.

Require background checks, including fingerprinting, in order to obtain a HazMat driver license.

Enhance criminal penalties for injuring or killing a first responder in an emergency caused by a terrorist act.

Subject to civil forfeiture any property used or intended to be used in an act of terrorism.

The Attorney General also voiced a number of concerns regarding attempting to expand the state's role in immigration issues, explaining that immigration powers rest almost solely with the federal government.

4.5-Response Recommendations

The Task Force heard testimony in this area from numerous experts. The Task Force learned that a number of modifications to the public health laws may be needed to update Oklahoma's public health response in the face of potential terrorist attacks. At issue are Oklahoma specific amendments to the proposed Emergency Health Powers Act developed by the Association of State and Territorial Health Officials. The Task Force asked Dr. Leslie Beitsch, State Commissioner of Public Health, to provide specific guidance on the necessary areas for amendment to public health law. Dr. Beitsch indicated during his testimony to the Task Force that a number of areas of Oklahoma Health Code needed to be amended to deal with terrorist-related health threats. Dr. Beitsch

specified the following aspects of the Emergency Health Powers Act that should be pursued in Oklahoma. These provisions included:

> A state of public health emergency shall be declared by the Governor if the Governor finds an occurrence or imminent threat of an illness or health condition, caused by bioterrorism, epidemic or pandemic disease, or novel and highly fatal infectious agents or biological toxins.
>
> Health Care providers, coroners, or medical examiners shall report all cases of persons who harbor any illness or health condition that may be caused by bioterrorism, epidemic or pandemic disease, or novel and highly fatal infectious agents or biological toxins and might pose a substantial risk of a significant number of human fatalities or incidents of permanent or long-term disability. In addition, pharmacists shall report any unusual or increased rates of prescriptions or unusual trends, which could be related to bioterrorism or an epidemic.
>
> The public health authority may exercise, for such period as the state of public health emergency exists, powers over dangerous facilities or materials. These powers shall consist of controlling accesses to facilities and property, ensuring the safe disposal of infectious waste and corpses, control of health care supplies, and destruction of property.
>
> During a state of public health emergency, the public health authority shall use every available means to prevent the

transmission of infectious disease and to ensure that all cases of infectious disease are subject to proper control and treatment. Their authority shall extend to establishing and maintaining places of isolation and quarantine and requiring isolation of any person by the least restrictive means necessary to protect the public health. All reasonable means shall be taken to prevent the transmission of infection among the isolated or quarantined individuals.

Neither the State nor its political subdivisions, except in cases of gross negligence or willful misconduct, nor the Governor, the public health authority, or any other State official should be liable for the death of or any injury to persons, or damage to property, as a result of complying with or attempting to comply with the Emergency Health Powers Act.

The Legislature may also need to modify workers compensation laws, liability laws and "good samaritan" laws to accommodate the need for first responders who are providing aid from outside the affected jurisdiction.

The Task Force learned that the state of Oklahoma maintains and annually updates a State Emergency Operations Plan. It has been utilized many times in response to large disasters, such as the Christmas 2000 ice storm, the May 1999 series of tornadoes, and the April 1995 Oklahoma City Murrah Building bombing. This plan mirrors the Federal Response Plan, which is maintained and updated by the Federal Emergency Management Agency (FEMA). The plan breaks the operations functions into functional groups called Emergency Support Functions

(ESFs), such as communications, transportation, and health and medical. The plan provides a basic framework in each ESF, identifying the lead agency and its support agencies. An example is the State Department of Health, which serves as lead agency in the Health and Medical ESF. Numerous other state agencies support the Department of Health in its decisions involving health and medical response to an emergency.

It should be noted, however, that both the State Emergency Operations Plan and the Federal Response Plan are strictly support plans to actual operations performed at the local level of government. When an emergency occurs, local first responders will be the first on the scene, and their capabilities must be exceeded before the state or federal plan is implemented. While recognizing this fact, the Task Force was informed that it is also important to have a smooth transition from a strictly local effort to assistance that is provided in conjunction with state and federal jurisdictions. This requires an adequate degree of coordination and a detailed plan for such coordination.

At the state level, Oklahoma has maintained a standing committee, made up of various state agencies, to address increased capabilities for state response. Locally, representatives of first responder associations, as well as the Municipal League and the Association of County Commissioners, have been asked to do the same.

The Task Force heard testimony that there is a need for additional equipment and training for first responders at the local level. With respect to fire department

readiness, the Task Force learned that most of our state is covered by volunteer firefighters. These departments perform their jobs with little public financial support. There are hundreds of volunteer fire departments across the state which receive little more than $2,000 annually each from state appropriations. Their equipment is typically obtained through a surplus property process. A similar situation exists for the state's local emergency managers who are, for the most part, volunteers.

Currently, there are major gaps in our ability to train and finance all fire departments to reach a hazardous materials certification level. This is the type of response needed for an event involving chemical or biological substances. One solution discussed by the Task Force is to implement the Department of Public Safety's strategy to create regional Hazardous Materials Teams, which could be used as local assets or activated for state duty. It has been noted that urban and suburban jurisdictions with such capability could also be used on a regional basis.

The Task Force also discussed longer-term solutions to response needs. Such solutions could entail research and development investments at state universities to utilize, for example, the sensor technology being developed at Oklahoma State University and the Meso-Net system at the University of Oklahoma to provide a sophisticated, early warning system for air-borne bio- or chemical terrorism attacks. Such technology could become useful globally, making Oklahoma a leader in the fight against terrorism.

Food Safety Recommendations

On two separate occasions the Task Force heard from witnesses who emphasized the importance of protecting the state's livestock, agricultural production and food processing industries. Because of the infectious nature of certain diseases, it is imperative that the state have a response and remediation plan to deal with potential terrorist attacks on livestock, agriculture or the food supply.

Representative James Covey, Chair of the Oklahoma Food Safety Task Force, addressed the Homeland Security Task Force and provided a summary of his group's work on this subject. The Food Safety Task Force focused on the upgrading of the Animal Disease Diagnostic Laboratory, consolidation and upgrading of laboratories at the Oklahoma Department of Agriculture, and funding of additional epidemiologist and microbiologist positions at the State Department of Health.

One of the highest priority recommendations of the Food Safety Task Force was the funding of an animal carcass digester. The Governor's Chief of Staff, Howard Barnett, also briefed the Task Force on the work of the Governor's Advisory Panel in the area of food safety. He too recommended that the state purchase the carcass digester, which is estimated to cost $1.5 million. The digester would allow the state to safely dispose of animal materials that have become infected with highly infectious diseases, such as bovine spongiform encephalopathy, commonly known as "mad cow disease." Such diseases cannot

be destroyed through common incineration and the digester is the recommended method of disposal.

(A complete copy of the Food Safety Task Force's findings is available in the appendix of this report.)

Communications

One critique of Oklahoma's readiness to deal with terrorist attacks that was raised repeatedly before the Task Force is the state's current lack of interoperability in communications. Simply put, fire officials are not always able to talk to police, who may or may not be able to talk with emergency management, who cannot always talk to emergency medical. Without compatible communications response to any type of emergency event, such as a terrorist incident, is made more difficult, and the risk of increased lethality is heightened significantly.

The Task Force heard testimony regarding a number of potential solutions to the problem of communications interoperability. The longest standing and most discussed was the proposed statewide 800 MHz Trunked Radio Communications System. The total cost of such a system is approximately $52 million. with recurring annual costs of $3 million. According to the Department of Public Safety, eighteen other states have taken this type of approach, including neighboring states of Arkansas and Colorado. Although the 800 MHz system has been much discussed in the past, it has always been sidelined due to cost considerations.

Other approaches to the interoperability issue include a military style, more incremental approach to interfacing different types of communications systems. This type of approach, referred to by the Task Force as the military approach, would assess current capabilities against a future objective system. An incident communications matrix could be established that would identify those stations that must have compatible communications to deal with a terrorism incident. Based upon that analysis a determination could be made as to how best to achieve a solution with available resources. Such an approach would provide a road map that could ultimately lead to a more comprehensive system.

Other suggestions to the communications dilemma ranged from exploring new wireless technology solutions, one of which had a price tag of approximately $100 million, to using a communications consultant to provide an expert view of how to achieve the desired goal.

It is the recommendation of the Task Force that one of the first duties of a newly appointed Director of Homeland Security be to employ a communications consultant and present the Legislature with options to solve this problem. The solutions should each have fiscal notes attached, along with the advantages and disadvantages of each solution detailed. These recommendations should be available within ninety days of the hiring of the consultant.

4.6-Capitol Security

Recommendations for security of the State Capitol are contained in the preliminary report of the Task Force on Security for State Employees (November 20, 2001), which undertook its work in accordance with Executive Order 2001-32. The preliminary report is based in part on the results of security surveys completed on the State Capitol by the U.S. Marshall's Office and a private security consultant. Following are the major recommendations for security of the State Capitol in the Task Force's preliminary report:

Training programs for state employees to increase employee awareness and create an office "neighborhood watch."

Increased Capitol Patrol visibility at the entrances of the Capitol.

Emergency phone number stickers distributed at all Capitol Complex phones.

Installation of additional video cameras.

Upgrading of existing video cameras.

Installation of intrusion alarm systems.

X-ray of all incoming mail and packages.

Installation of magnetometers and x-ray machines in the State Capitol and select state buildings.

Restriction of hours and accessible entrances to the State Capitol.

Creation of an off-site delivery point for all mail and packages.

The working group on these issues estimated the total cost of the recommendations to be $3.3 million over a two-year period. Of that amount, $1.2 million is for equipment, and $2.1 million is for additional personnel. The view of

the Task Force was that the security requirements of the State Capitol need to be addressed due to the essential functions and symbolic nature of the building. Furthermore, the Task Force reached the view that even a minimal systems upgrade would significantly improve the current level of security at the Capitol.