COUNTER-TERRORISM TASK FORCE

Chair:

Richard C. Alexander

Members:

Richard Brown
Duncan Campbell
Becky Carter
Dean Dordevic
Tim Greve
Erin Hubert
Jim Jeddeloh
Paul Lorenzini
Lucille McAleese
Peter Nickerson
John Parsons
Barbara Querin
David Simpson
Fred Stickel

Ex-Officio Members:

Greg Clark, Assistant Chief, Portland Police Bureau
Michael D. Schrunk, Multnomah County District Attorney
Julie Thornton, Supervisor, FBI, Portland, Oregon

Staff:

M. Ray Mathis, Executive Director, Citizens Crime Commission
Louise L. Grant, Associate Director, Citizens Crime Commission

LETTER FROM THE CHAIR OF THE CITIZENS CRIME COMMISSION

The Citizens Crime Commission's (CCC) Counter-Terrorism Task Force was formed as an Oregon business response to the terrorist attack on the United States September 11, 2001. Specifically, the CCC has examined the role of the business community in reducing the probability of terrorist attacks and assisting the public sector in preparing for attacks should they occur.

The Task Force greatly appreciates the participation of Multnomah District Attorney Mike Schrunk, FBI Supervisory Special Agent Julie Thornton, and Portland Police Assistant Chief Greg Clark. The following business leaders also gave valuable input into the research and recommendations of this report: Richard Brown, Owner, Richard Brown Photography; Duncan Campbell, President, The Campbell Group; Becky Carter, Security and Safety Initiative, Intel Corporation; Dean Dordevic, Principal, Ferguson Wellman Capital Management; Tim Greve, President, Carl Greve Jewelers; Erin Hubert, Executive Vice President, Portland Trail Blazers/Oregon Arena Corp.; Jim Jeddeloh, President, Perkins and Company., P.C.; Paul Lorenzini, retired Pacificorp Executive; Lucille McAleese, Owner, Kells Irish Pub and Restaurant; Peter Nickerson, Director, Growth-Link Overseas Company; John Parsons, Regional Chief Executive Officer, Lincoln Financial Advisors; David Simpson, Corporate Security Manager, Nike, Inc.; Fred Stickel, Publisher, Oregonian Publishing Co. and Barbara Querin, Sr. Vice President, Legacy Health System.

We especially appreciate the leadership of Task Force Chair Richard C. Alexander who continues to dedicate an enormous amount of time and resources to the betterment of our state and its citizens. His efforts on behalf of the Counter-Terrorism Task Force is another example of his outstanding citizenship and we are indeed grateful for his thorough and thoughtful leadership on this complex issue.

The events of 9/11 have forever changed our lives and it is the hope of the Citizens Crime Commission that this report will help diminish the threat and fear of terrorism for Oregonians.

James B. Jeddeloh
Chair, Citizens Crime Commission

THE COMMITTEE AND ITS CHARGE

The Citizens Crime Commission represents the business community on public safety issues and assists the public sector in becoming more effective and efficient in reducing crime and the fear of crime in our community. To this end, our membership formed the Counter-Terrorism Task Force in order to:

- gather data and testimony.
- define the terrorist threat to our state.
- identify critical infrastructure.
- determine what steps are being taken by government and business.
- make recommendations for prioritizing intervention strategies.
- advocate for recommendations.

OUR MISSION

Identify ways the private sector can assist the war on terrorism and make recommendations that enhance public safety.

INTRODUCTION

In the likelihood that terrorism against the United States will continue in the wake of September 11, the Citizens Crime Commission formed a Counter-Terrorism Task Force to study the optimal ways to prevent and prepare for catastrophic events. The potential targets for terrorist activity are many and varied ranging from military, political and civilian institutions to business and communications centers. While the Counter-Terrorism Task Force recognizes that all terrorist threats cannot be prevented, we believe that a thoughtful process that evaluates the threats and prioritizes the responses will go a long way to minimize the impact of terrorism on our state and nation.

The task force recognizes that there are numerous organizations and individuals on the national, state and local level who are working to identify and neutralize this threat to our freedom. The task force did not attempt to duplicate these efforts, but instead has sought to bring clarity and focus to the coordination and prioritizing of these efforts. Additionally, it is not possible to think of every possible terrorist threat to our nation, institutions and citizens. We can, however, identify potential infrastructure targets of terrorists and prioritize our response.

COMMITTEE PROCESS

The Citizens Crime Commission Terrorism Task Force has been meeting since April 2002, studying ways that both the public and private sector can better prepare for terrorist and catastrophic events. To this end, the Task Force sought extensive advice and professional counsel from intelligence/security experts, both in committee sessions and in private meetings. Also of great benefit to the Task Force was input from the Oregon Office of Emergency Management as well as the Regional Office of Emergency Management. The Task Force ex-officio members included FBI Supervisory Special Agent Julie Thornton, Multnomah County District Attorney Mike Schrunk and Portland Police Assistant Chief Greg Clark. Testimony was given by numerous individuals including cyber threat assessment by FBI Supervisory Special Agent Will Hatcher from the New Orleans office of the FBI. Patrick Stewart, from the Oregon State Attorney General's office briefed the Task Force on legislative proposals that will assist in the war on terrorism. Additionally, Officer Dan Liu, Portland Police Bureau and FBI Special Agent in Charge Charles Mathews presented testimony on terrorist organizations known to be in Oregon.

Members of the Task Force were observers of a simulated emergency response exercise by the Regional Metropolitan Emergency Response system in Portland. Task Force members also attended a one-day terrorism seminar sponsored by Oregon US Attorney

Mike Mossman. Background information was obtained from numerous publications, many of which are listed in the appendices of this report.

TERRORISM

It is helpful to begin our discussion of terrorism with the FBI's definition as follows:

> *Terrorism is a use of force or violence against persons or property in violation of the criminal laws of the United States for the purposes of intimidation, coercion or ransom. Terrorists often use threats to create fear among the public, to try to convince citizens that their government is powerless to prevent terrorism and to get immediate publicity for their causes.*

Additionally the FBI categorizes terrorism in the United States as one of two types… domestic terrorism or international terrorism.

Domestic Terrorism involves groups or individuals whose terrorist activities are directed at elements of our government or population without foreign direction.

International Terrorism involves groups or individuals whose terrorist activities are foreign-based and/or directed by countries or groups outside the United States or whose activities transcend national boundaries.

WEAPONS OF TERRORISTS

Terrorist weapons come in many shapes and forms. The committee has chosen to focus on those that offer the greatest threat of mass casualties and disruption to society. We did not include for example, individuals using pistols, knives or other weapons that may cause individual loss of life, but are less likely to disrupt society as a whole. Furthermore, the Task Force has tried to be careful in its report to avoid giving potential terrorists ideas for obtaining weapons of mass destruction. With this caveat in mind, the list of threats can be broadly placed in five categories:

1) conventional explosives
2) chemical, biological and nuclear weapons
3) cyber attacks
4) eco- terrorism
5) agri-terrorism

Conventional explosives are easily obtained and made in the United States. For example, the federal courthouse in Oklahoma City was bombed with the use of fertilizers and explosives which caused a large loss of life and enormous damage to a community. The federal government, through the Bureau of Alcohol, Tobacco and Firearms (BATF), is doing a much better job of tracing and protecting conventional explosive materials. However, this remains the most likely form of attack because of the large volume of explosives and components accessible in the United States.

Chemical, biological and nuclear threats are arguably the area that is causing the most consternation for all levels of government. The potential loss of life and damage to infrastructure from such attacks is almost unlimited and unimaginable. However, we must imagine these events if we are to prevent terrorist attacks, as well as our response if prevention fails.

Cyber attacks have occurred for many years in the United States, primarily by hackers motivated by thrill, challenge and prestige. Considerable intelligence has been gathered indicating that our enemies are also attempting to use the Internet as a means of attacking our institutions. FBI cyber expert Supervisory Special Agent Will Hatcher shared with the Task Force that numerous attempts have been made to enter and compromise the computer systems of businesses, military and national agencies charged with security. He strongly recommends that the region develop a local computer forensics laboratory such as those in San Diego and Dallas and proposed in San Francisco, Chicago and Kansas City.

Eco-terrorism - According to Officer Dan Liu, the **Animal Liberation Front** (ALF) and **The Earth Liberation Front** (ELF) are the two primary eco-terrorist organizations in Oregon. The ALF formed a radical militant group in the mid 1970's and ELF, which was founded in England by members of the Earth First organization, appear to have started working together in 1993. On June 13, 2001 ALF and ELF jointly claimed responsibility for attacks on five banks in New York facilities. While the mainstream philosophy of animal rights and ecological issues is in keeping with the American tradition of lawful protest in achieving change through education, advocacy and public awareness, the ELF and ALF have sought to bring about change through criminal acts and have gradually escalated their tactics.

ELF and ALF operate in small semi-autonomous cells independent of one another. There is no identifiable (provable) membership list, leaders, members, payroll, etc. Anonymous claims of direct actions are sent by a communiqué spokesperson who disseminates information to the media. Their targets have been fur farms, department stores, research labs, residence of researchers, cosmetic companies, meat and poultry processors, circus shows, rodeos, restaurants, logging, milling facilities, resorts, government buildings, financial and administrative organizations, hybrid research farms, car dealerships, etc. These terrorist acts include arson to buildings, equipment and facilities, sabotage of

resources, monkey wrenching, destruction of research material and records, the release of animals and the use of electronic means, such as email saturation against their targets. They have used crude to sophisticated incendiary devices and have thus far caused millions of dollars of property damage in Oregon.

Terrorist acts, which have occurred in our region, attributed to ELF and ALF, have not yet resulted in loss of human life. However, they have caused serious property damage and put people at risk. Future acts may have more serious consequences. The FBI Joint Terrorism Task Force (JTTF), with the assistance of the Portland Police Bureau and other agencies, is currently working to develop successful cases against individuals in these organizations.

Agri-terrorism is the malicious use of plant or animal pathogens to cause disease in the agricultural sector. Animal pathogens were actually used in World War I and many nations possess weaponized biological agents, such as the former Soviet Union and Iraq. It is reasonable to assume that with the disintegration of the Soviet Union and the unemployment of many of the scientists engaged in their bio-weapons program that the knowledge and ability to produce such weapons may have spread to other nations/states. Moreover radical Palestinian groups have used food contamination as a weapon against Israel. In several instances since the 1970's, Israeli citrus fruit and eggs were intentionally contaminated. The U.S. is especially vulnerable to agri-terrorism. Because of limited bio-security and surveillance in the food processing and animal rendering industry, as well as at other points in the food chain, the introduction of harmful pathogens is relatively easy.

From the terrorist perspective, agri-terrorism is almost risk free. Most are safe to produce, easy to transport, and particularly in the case of animal pathogens, easy to disseminate. Plant pathogens are harder to spread as they are highly sensitive to environmental conditions, but both present a low risk of detection for the terrorists. The relative ease of weaponizing biological agents against live stock or plants, coupled with the largely risk free nature of this form of attack, increases the likelihood of their use.

CRITICAL INFRASTRUCTURE

Those structures, facilities or services, which are essential to the function of a region and without which there would be great risk of loss of life and/or disruption of public services and the economy, are considered to be critical infrastructure. It is logical to conclude that terrorists are likely to direct resources against targets that will cause the greatest disruption to our society.

The U.S. has become the world's most successful, open, highly industrialized information-age nation. Growth in key areas of service has provided reliable electrical power, clean water, adequate and low cost supply of gasoline and fuel oil, good medical

services, abundant food choices as well as other benefits of a highly evolved way of life.

The infrastructure which supports the production and delivery of these services was designed and built in a relatively threat-free environment. No one anticipated that someone might one day want to disrupt these products and services or use them as a weapon against us.

We must now assess the threats to vulnerable infrastructure, prioritize risk and take appropriate steps to reduce the likelihood of having that which benefits us - turned against us.

Key Regional Infrastructure

Water supply system
Electrical generation and distribution
Hospitals
Schools
Natural gas storage and distribution
Gasoline and oil storage and distribution
Telecommunication
Public buildings and continuity of government
Transportation/Airports
Emergency services--Fire, Police, Medical, Rescue
Bridges and tunnels
Harbor and port facilities
Information or communication components that control critical infrastructure and finance

There is no perfect defense against acts of terrorism. The likelihood of a terrorist attack against any given target is small. The impact of such an attack, however, can be very large.

The threat cannot be ignored. A calm thoughtful approach to assessing risk, setting priorities and carefully listing equipment, improvements and practices required to minimize the likelihood or impact of a catastrophic event is the strongest defense available to us. Once such a listing of essential needs is determined, funding sources should be identified. Among these sources might be a public safety levy. A levy, properly presented and restricted only to essential needs, would likely gain strong public support.

PREPAREDNESS

An emergency preparedness plan for terrorist attacks has four essential elements, most of which apply to other catastrophic events.

The experts who have counseled us and printed material from many credible sources identify those key elements as:

1) Intelligence -- The gathering of information which can be used to prevent attacks from occurring.

2) Mitigation -- Identify the most likely targets. Prioritize risk. Take steps to protect highest risk targets and "harden" facilities in such a way as to reduce exposure and minimize damage.

3) Emergency Response -- Provide for well equipped, trained personnel and facilities for response to terrorist acts.

4) Remediation -- Plan for recovery and continuation of services.

Many groups, representing national, state, county and municipal interests are working - hard and together - toward the development of preparedness plans. Much has been accomplished -- but all would agree that much remains to be done. Following are recommendations and points of interest deserving of further emphasis.

PUBLIC SECTOR RECOMMENDATIONS

1) Intelligence

- Renewed emphasis should be put on the gathering and sharing of good intelligence. **The best way to counter terrorism is to prevent it**. This is our most effective means of preventing loss of life and property damage. It requires all citizens to become more vigilant; i.e., report suspicious activity and objects.

- Review statutory and regulatory authority for appropriate changes.
  The Task Force received testimony from Pete Shepherd, State Attorney General's Office, on a number of changes to Oregon laws which will enhance the ability of law enforcement to respond and investigate terrorists.
  There are two laws in particular that the committee wants to see changed. The first one addresses the problems faced this past year by the Portland Police Bureau responding to the request by the U.S. Attorney General to interview individuals who might have information pertaining to the 9/11 attacks. They

were advised by the Portland City Attorney that Oregon law would not allow the Portland Police Bureau to participate in these interviews. This opinion was in direct conflict with the interpretation of the law by the State Attorney General and the Multnomah County District Attorney. This situation should not be allowed to occur again and appropriate changes to the state law should eliminate multiple interpretations.

Secondly, under current Oregon Law, ORS181.850, local law enforcement cannot inform the local Immigration and Naturalization Service (INS) when they learn that an individual's only crime is that he/she is in the United States illegally. The restriction this statute places on local law enforcement in cases where an individual may be a suspected terrorist is obvious and should be revisited by the Oregon Legislature.

- All public officials should support the participation of the various police agencies in the Joint Terrorism Task Force headed by the FBI, which is coordinating the response to terrorism. These task forces exist in practically every major city in the U.S and are absolutely essential if we hope to prevent terrorist events. **All law enforcement agencies need to be at the table sharing information during this very important time.**

- Maintain a secure, Internet-based, single source web page system, so that appropriate counter terrorism information is available to all appropriate parties.

(2) Mitigation

- Continue to assess risk to critical infrastructure. Determine which elements of infrastructure are most crucial to public safety. In some descending order, identify the action, if any, required to reasonably protect or harden the resource. From this analysis a list of needed improvements and equipment can be made. **Such a listing of needs should reflect a balanced evaluation – a weighing of risk versus costs and represent only the essential needs required to prudently address risk levels.**

  It is likely that such an assessment will determine that there will be varying degrees of protection required with some elements of infrastructure being fully protected, i.e. water supplies, while some others may receive more limited protection and be responded to based on specific threats.

- Remove the address of Emergency Operations Centers and 911 centers from the buildings, property, letterhead and telephone directories. Request that the media not use specific addresses when referring to emergency operation centers.

- Operation centers and 911 centers should be hardened, protected and have back-up facilities and equipment in place for immediate use. This back-up facility might be fixed or mobile.

- Avoid housing the Emergency Operations Center and 911 Center in the same facility.

- Eliminate or restrict public parking adjacent to Emergency Operation Centers.

- Airport and air transportation security was addressed in the Portland Security Task Force Report of February, 2002. There is no question that the disruption of air travel remains a favorite terrorist target and deserves the highest level of protection and cooperation from the various heads of government. Copies of this report are available upon request.

- Approximately 6,000 shipping containers enter the Port of Portland each year and less than 2% are physically inspected. The containers then move by rail or truck to their final destination. These containers, arriving from points around the world, provide a means for introducing terrorist weapons into our region. While the Coast Guard and local ports (including ours) can establish practices leading to improved security, the experts assert that maritime security must be seen as an international issue, requiring the cooperation of all nations. To achieve a higher level of container security, without disrupting the movement of goods, will require the integration of several steps, including the following:

    1) **Push the border back**. Prevent weapons from getting to the U.S. by inspecting and protecting cargo at the time it is loaded into the container or before embarkation. Provide incentives to manufacturers, distributors and shipping lines that comply with strict loading and sealing requirements. Incentives might include a higher clearance rating expediting the movement of their cargo -- to the benefit of all parties involved -- manufacturer, shipper, port and user.

    2) **Require tamper-proof seals on all containers**. Certain high risk cargo should be further protected through use of more sophisticated security devices containing electronic components that signal an alert if the container has been opened or access gained in other ways.

    3) **Continue to support enhancement of the Coast Guard's Ship Arrival Notification System** and its logical extension to broad electronic tracking of individual containers, shippers, consignees and gathering of other essential information. Provide a record of chain of custody and content.

4) **Increased use of drive-through screening at foreign and domestic ports** using x-ray and radiation detection technology. Radiation detection devices have been installed on cranes handling containers at some ports. Hand held radiation detectors are also being used.

5) **Continue the development of better intelligence**. Become more aware of threats and risks before they arrive in the U.S. Improved intelligence can help determine who poses a threat and who does not -- thereby reducing targets to a more manageable level.

Better use of technology, human and electronic intelligence and incentives to conform to best practices by manufacturers, shippers, ports and users will significantly improve container security without disrupting the flow of commerce.

- Protect computer files from cyber attack.

- Provide back-up electrical power sources for critical areas of operation.

- Our elected officials should prepare a plan for the continuance of government and essential administrative and support services in the event of an attack on existing public facilities.

- Provide safe, off-site storage for critical records, documents and other data so as to facilitate more orderly continuation of government.

(3) Emergency Response

We have learned that it can be very difficult to anticipate and prevent terrorist acts. However, with a heightened focus on the gathering of intelligence, more attacks will be thwarted. Others will not be stopped. The many experts who have met with our Task Force are in agreement that **it is not a question of whether we will experience additional terrorist attacks -- just where and when.**

We must accept the reality of the situation and place a major emphasis on our ability to respond to an event in such a way as to minimize casualties and property damage.

We must provide for fast, coordinated, effective response on the part of our Fire, Police, Medical and Rescue resources. While terrorist threats and targets are many and varied -- our response, in most instances, will be the same.

- When our committee discussed essential needs with experts in the field of Emergency Response – be it Fire, Law Enforcement or Medical - one term rises quickly to the top of all lists: IMPROVED COMMUNICATION.

Every individual who appeared before the committee pointed out the communication problems existing between agencies. The lack of inter-agency communication in the World Trade Center catastrophe between police and fire directly resulted in greater casualties. Good communication capability requires good equipment and technology, redundancy, communications discipline and a sound communication plan. Communication must flow up, down and laterally. No amount of emergency response resources can be effectively brought to bear without coordinated inter and intra agency communication capability.

- Continue training and simulation exercises at all levels of government. Task Force members observed a clinical training exercise that was conducted on a regional basis. These exercises take an enormous amount of time and effort, yet are essential to the protection of our citizens. At a minimum, these exercises should be conducted on a quarterly basis and include senior elected leaders.

- Continue to seek out best practices in all areas of emergency response. **Share ours -- learn from theirs.**

- Program/Response capabilities should be objectively evaluated on an ongoing basis with weaknesses identified and corrective action agreed upon -- and taken.

- Business and government leaders should support the establishment of the "National Center for Disaster Decision Making" (NACDDM) in the Portland Metropolitan area. This center will assist senior leaders in public safety, public health and other government officials in developing sophisticated skills necessary to make critical decisions during disasters. (See Appendix C)

  It is suggested that NACDDM consider, at a future date, developing a syllabus and curriculum for private sector leaders through which they could gain knowledge in how to prepare for and deal with the terrorist threat as it relates to their enterprise.

- Emergency response personnel, responding to a disaster, should have priority access to communication channels/frequencies.

- Communication with the public during a crisis via print, radio or television should be official -- by a designated senior official -- (mayor) and be updated on a regular basis. Other official communications might include a web page with maps and instructions as well as other event-related information.

  Good, straightforward communication with the public will reduce the level of anxiety and concern and help to avoid overwhelming communication and medical facilities unnecessarily.

- Provide proper protective clothing and equipment to all first responders. Emergency response persons should be protected in a self-contained environment and equipment readily available to identify the type of threat, severity and area requiring containment.

- Fire, Police and Medical agencies should develop and maintain a roster of back-up personnel; i.e. recently retired and experienced personnel, who would be available for back-up in a mass casualty event.

- Continue the planning for a five-county regional terrorist response plan through which regional resources can be coordinated and focused. The planning should include a regional heavy rescue team.

- The National Guard should participate in planning sessions and exercises so as to be better prepared to assist in a mass casualty event and its aftermath.

- Senior elected public officials should anticipate certain critical public policy decisions which must support effective, coordinated response to a terrorist attack and provide appropriate directives to Fire, Police and Emergency Services -- **Now.**

- Support public health officials in their efforts to provide medical response to varied terrorist threats -- including mass decontamination capability.

- The medical community should have in place a "surge" plan to accommodate a mass casualty event to the extent that existing facilities and resources make possible. Public policies should be in place that provide for protection of medical facilities and resources from being overrun by a frantic public.

(4) Remediation

Recovery from a terrorist act or natural disaster can occur faster if certain key planning elements are in place prior to the occurrence of the event. One very important element, mentioned earlier under mitigation, is off-site storage of critical records, documents and other data essential to continuing operation.

- Site clean up and/or decontamination.

- Public/private partnerships focused on all aspects of recovery, i.e. rubble removal, repair or reconstruction, easing of regulations, expediting materials and human resources.

- **Remain positive -- unbowed -- communicate well -- move forward.**

BUSINESS RECOMMENDATIONS

Business overall, is poorly prepared for a catastrophic event – be it earthquake or terrorist attack. Business has placed major emphasis on doing it better, faster and at lower cost – an emphasis dictated by a competitive environment. This competitive environment provides the public with excellent products and services, reasonably priced and readily available. Most businesses are not yet convinced of the need for physical security or incident response planning. Unfortunately this is likely to change.

Business security plans will differ by type of business, size, location(s), products or services offered and material utilized in the business process, as well as other factors. Each plan will be different and respond to the security risks associated with that particular enterprise. Law enforcement agencies can provide some material or advice in developing a plan. There are also capable consulting services which can assist in all phases of plan preparation. There are some things that can be done at little or no cost, while others have cost associated with their implementation. Regardless, all business should develop a basic physical security plan and an incident response plan. These plans might include, but should not be limited to the following:

- All businesses should conduct an inventory of current security features, note weaknesses, and develop a physical security plan. This plan would include usual review of locks, lighting, alarm systems, set-back areas, perimeter fencing, entry lights and security controls.

- Discuss the need for enhanced awareness with all employees. Enlist their support in spotting suspicious people or objects.

- Control access to property. Limit visitor/customer access to selected entrances.

- In some instances – eliminate or limit parking or driveways adjacent to structures. Restrict visitor parking to areas away from structures.

- Establish clear lines of authority. Determine who speaks publicly for the business.

- Develop a back-up inter-company communication plan.

- Provide for good communication with employees in the event of a catastrophic event. Set up a dedicated telephone line (or lines) to provide a recorded message stating the company's condition and plan for continued operations. Email and/or a company web site may also be used to provide information to employees. These communication measures are important whether or not the business was directly involved in the catastrophic event.

- Subject all newly hired employees to a through background check.

- Establish a plan and process for communicating business status to vendors, customers, and other interested parties. Ensure that key vendors have compatible business continuity plans.

- Work with law enforcement to develop an appropriate response to a bomb threat. Police assistance may be available to help you review your property and provide assistance in developing your physical security plans -- one section of which should be how to deal with a bomb threat.

- Protect computer files from cyber attack. The local office of the FBI has informational material available to assist in this effort.

- Secure, behind locked doors all explosives, flammables or biological agents. Maintain strict inventory controls over all these materials. Restrict access to these areas.

- Establish clear lines of authority for dealing with a threat or major event. Let it be known.

- Attempt to quickly obtain a public service assessment of the threat and affected area of a chemical or biological attack and provide employees with such information as is available in the event of an evacuation of your business.

- Know how to quickly turn off outside air and water intake systems.

- Provide employees with copies of The American Red Cross recommendations for maintaining a three-day supply of food, water and essential supplies for each person in an employee's family. Employees who are better prepared are safer, more effective, and less distracted and more available to assist in mitigation or remediation efforts.

- Business must concentrate on the same following key areas of preparation as does the public sector:

  -Human intelligence – Be observant, report suspicious activity, objects or persons.

  -Tighten security, harden your building – i.e. locks, lights, alarms, fencing, controlled access. etc.

  -Develop a physical security plan and an incident plan. Provide an effective response to threats. Prepare a response to bomb threats.

-Provide for remediation. Minimize business interruption – protect critical files. Communicate well at all times with all interested parties.

- Once your plan is in place, conduct drills to assure that your planning is sound and response appropriate and orderly. Assess the outcome of the exercises and implement corrective action as required.

- Provide Emergency Medical Training (EMT) to selected employees.

- Have appropriate protective clothing and equipment available for selected employees who may be called upon to work with First Responders in pointing out hazardous material storage areas or guide them to points of access to damaged structures.

- Maintain back-up copies of classified documents, discs, proprietary information and critical records essential to the operation at a secure location off-site.

- Instruct maintenance and security personnel who move about all areas of the organization to be particularly alert to anything out of the ordinary.

As regional planning progresses and matures, **areas of public sector-private sector cooperation should be explored**. The public sector leadership may overlook the private sector resources because it is harder to control and direct. Furthermore, there may exist a public sector perception that, " it's our job – our responsibility –fund us adequately and we will do it." However, the Task Force concluded that business could provide equipment and manpower to assist in rescue efforts, redundancy in some areas of communication, technical and maintenance support, assistance in remediation including environmental clean-up and assist in many other ways. The private sector has enormous resources and capabilities, much of which could be redirected in a crisis toward community protection.

CONCLUSION

Some may assume that since our attack in Afghanistan the threat of terrorism has abated and we can de-emphasize preparation for future terrorist acts. This would be a mistake. The war on terror has not been won. The international threat is evolving. Certain terrorist organizations have become more sophisticated in structure, organization, planning and communication capabilities. Terrorist networks, in which several smaller terrorist groups may work together to plan and coordinate attacks collaboratively, are being formed.

The U.S. is a uniquely compelling target for terrorists – our lifestyles, freedoms, quality of life and conflicting international involvements raise issues of envy and anger within some people. More states/nations are likely to use terrorist groups as an extension of their foreign policy. **The risk of terrorist acts is likely to be with us for years to come. We must accept that fact.**

Based on information provided our committee by terrorism experts, our region is certainly not exempt from threats. **It is now time for us to move forward calmly, but with purpose, to determine the essential requirements for defense and response and provide the funding needed for implementation. We believe the public would support it – and not expect less.**

TESTIMONY

Darmel Benshoof, Inspection and Control Unit
Portland Police Bureau
Office of the Chief of Police
1111 SW 2nd Ave.
Portland, OR 97204

Becky Carter
Security & Safety Initiative
Intel Corporation
JF2-16
5200 NE Elam Young Parkway
Hillsboro, OR 97214-6497

K. Dean Gubler, D.O., MPH
West Wing ICU Medical Director
Trauma & Surgical Critical Care
Associate Trauma Medical Director
Legacy Emanuel Trauma Program & Shock Trauma Institute
2801 N. Gantenbein Ave., MOB 130
Portland, OR 97227

Will Hatcher, Supervisory Special Agent, FBI
Computer Crime Squad
2901 Leon C. Simon Blvd.
New Orleans, LA 70126

Greg Hendricks, Captain
Portland Police Bureau
Office of the Chief of Police
1111 SW 2nd Ave.
Portland, OR 97204

Randy Kane, Lieutenant
Criminal Intelligence Unit Joint Terrorism Task Force
1500 SW 1st Ave., Suite #401
Portland, OR 97201

Alison S. Kelley, JD, Adjunct Professor
Program Coordinator
Executive Leadership Institute
Hatfield School of Government
494 State Street, Suite 220
Salem, OR 97301-3654

Daniel C. Liu, Officer
Criminal Intelligence Unit
FBI Joint Terrorism Task Force
1500 SW 1st Ave., Suite #401
Portland, OR 97201

Charles Mathews, SAC FBI
1500 SW First Ave., Suite 400
Portland, OR 97201

Steven Muir, Battalion Chief, Emergency Management Coordinator
City of Portland, Bureau of Fire, Rescue & Emergency Service
55 SW Ash
Portland, OR 97204

Kenneth D. Murphy, Deputy Director
Oregon Emergency Management
595 Cottage St., NE
Salem, OR 97301

Bruce W. Prunk, Deputy Chief
Portland Police Bureau
111 SW 2nd Ave.
Portland, OR 97204

Mike Swinhoe, Special Agent FBI
1500 SW First Ave., Suite 400
Portland, OR 97201

Books used as research sources:

Heymann, Philip B., Terrorism and America, The MIT Press, Cambridge 1998

Stern, Jessica, The Ultimate Terrorists, Harvard, Cambridge, 1999

Lesser, Ian; Hoffman, Bruce; Arguilla, John; Ronfeldt, David; Zanini, Michele and Jenkins, Brian Michael, Countering the New Terrorism, Washington, 1999

Butler, Richard, former Chairman of United Nations Special Commission – Public Affairs, The Greatest Threat, New York, 2001

Bergen, Peter L., Holy War, Inc., Simon and Schuster, New York 2002

Holmes, John Pynchon; Burke, Tom, Terrorism – Today's Biggest Threat to Freedom, Kensington Publishing Co., New York, 2001

Osterholm, Michael T.; Schwartz, John, Living Terrors, Dell Publishing, New York, 2000

Netanyahu, Benjamin, Fighting Terrorism, Farrar, Straus and Giroux, New York 2001

Articles, Reports and Periodicals used as research sources:

Brookings Review, After September 11, Summer 2002, the Brookings Institution, 2002

Backgrounder, Terrorism, The Center for National Security Studies, Washington, ND

The FBI Domestic Counter- Terrorism Program, Center for National Security Studies, Washington, ND

Countering the Changing Threat of International Terrorism, A Report of the National Commission on Terrorism, Pursuant to Public Law 277, 105th Congress

Combating Terrorism: In Search of a National Strategy, Testimony of Dr. Bruce Hoffman, Director, RAND Washington office before the Subcommittee on National Security, Veterans Affairs and International Relations, House Committee on Government Reform, ND

Terrorism in the United States 1999, U.S. Department of Justice, Federal Bureau of Investigation, 1999

Counter the New Terrorism: Implications for Strategy, Ian O. Lesser, RAND, Washington, ND

Strike at the Roots of Terrorism, by Ian O. Lesser, RAND, Washington, ND
Terrorism, Infrastructure Protection and the U.S. Food and Agricultural Sector, Peter Chalk, RAND, Washington, Testimony before Senate Sub-committee on Oversight of Government, Management, Restructuring and the District of Columbia, ND

Improving Functional Capabilities, Chapter Three, Report of Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction for U.S. Congress and the President of the United States.

Before Disaster Strikes, American Red Cross, ND

Counter Terrorism Coordination, The Inman Report – Report of the Secretary of State's Advisory Panel on Overseas Security. ND

Backgrounder: Terrorism, Federal Emergency Management Agency, ND

The Best Homeland Defense is a Good Counter-Terrorism Offense – Ambassador Michael A. Sheehan, Coordinator for Counter-Terrorism, US State Department, The ANSSER Institute for Homeland Security, ND

Defending the American Homeland's Infrastructure by Phil Lacombe and David Keyes, ND

Combating Terrorism: Assessing Threats, Risk Management and Establish Priorities, Statement of John V. Parachini, Monterey Institute International Studies, Center for Non-proliferation Studies, before the House Subcommittee on National Security, Veterans Affairs and International Relations, ND

Testimony on Eco-Terrorism by U.S. Congressman Greg Walden before the House Resource Sub-committee on Forests and Forest Health, ND

When Trade and Security Clash, The Economist, April 6, 2002

Certifying the User, Traffic World Magazine, June, 2002

Container Security Improvements Needed to Prevent Terrorist Acts Through U.S. Ports, according to Maritime officials, transportation reporter on testimony before U.S. House Coast Guard and Maritime Transportation Sub-committee. ND

Maritime Briefs, Traffic World Magazine, May 20, 2002

The U.S. Agricultural Sector: A New Target for Terrorism? Peter Chalk, RAND Corporation, Washington, ND

Planting Fear – How real is the threat of Agricultural Terrorism? By Gavin Cameron, Jason Pate & Kathleen M. Vogel, ND

Terrorism: How Vulnerable is the United States? By Stephen Sloan, The Strategic Studies Institute of the U.S. Army War College, May, 1995

Statement of Harold J. Creel, Jr. Chairman, Federal Maritime Commission, Washington D.C. Submitted to the Committee on the Judiciary, U.S. House of Representatives, June 5, 2002.