

# MEETING THE CHALLENGE OF HOMELAND SECURITY

Second Edition, October 2003



**B | A | S | I | C**

**BAY AREA SCIENCE AND INNOVATION CONSORTIUM**

Advancing the Bay Area's Leadership in  
Science,  
Technology  
and Innovation

# MEETING THE CHALLENGE OF HOMELAND SECURITY

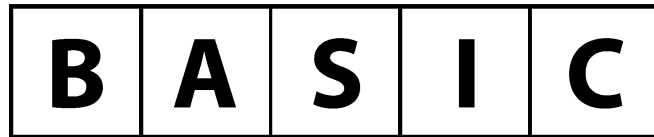
Second Edition, October 2003

This report was produced through the contribution and support of BASIC members and other public and private sector leaders in the Bay Area.

BASIC (Bay Area Science and Innovation Consortium) is a program of the Bay Area Economic Forum, co-sponsored by the Bay Area Council and the Association of Bay Area Governments (ABAG).

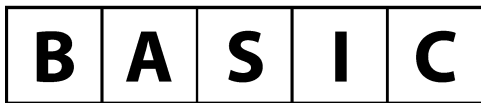
*Project Manager*  
Sally DiDomenico  
Vice President  
Bay Area Economic Forum and BASIC

*Cover photo courtesy of Sandia National Laboratories*



BAY AREA SCIENCE AND INNOVATION CONSORTIUM

Advancing the Bay Area's Leadership in  
Science,  
Technology  
and Innovation



BAY AREA SCIENCE AND INNOVATION CONSORTIUM

200 Pine Street, Suite 300  
San Francisco, CA 94104  
Phone: (415) 981-7117  
Fax: (415) 981-6408  
Email: [basic@bayeconfor.org](mailto:basic@bayeconfor.org)  
[www.bayeconfor.org/BASIC](http://www.bayeconfor.org/BASIC)

# TABLE OF CONTENTS

Message from the Chairman

Executive Summary ..... i

## SECTION I ESSAYS ON THE CHALLENGES OF HOMELAND SECURITY

### TERRORIST THREATS

**Today’s Terrorist Threat: Weapons of Mass Destruction** ..... 3  
*by Roger W. Werne, PhD, Chief Engineer, Nonproliferation,  
Arms Control, and International Security Directorate,  
Lawrence Livermore National Laboratory*

**Cybersecurity** ..... 7  
*by Joe Raguso, Vice President of Strategic Partnerships,  
SRI International*

### RESOURCES FOR REGIONAL PREPAREDNESS

**The Role of National Laboratories and Universities  
in Bay Area Preparedness** ..... 9  
*by William A. Barletta, PhD, Coordinating Director,  
Homeland Security and Non-Proliferation Programs,  
E.O. Lawrence Berkeley National Laboratory  
and Jody R. Westby, President, The Work-IT Group, Denver*

### FIRST RESPONDER CONCERNS

**Meeting New Challenges:  
Building on Lessons from Natural Hazards Response** ..... 13  
*by Jeanne Perkins, Principal, Earthquake Program,  
Association of Bay Area Governments*

**A Public Sector Perspective  
on Meeting the Challenge of Homeland Security** ..... 17  
*by Frances Edwards-Winslow, PhD, CEM Director,  
Office of Emergency Services,  
City of San Jose*

TECHNOLOGY AND PLANNING FOR FIRST RESPONDERS

**Technology Development for First Responders** .....[21](#)

*by Peter Friedland, PhD, Special Assistant to the Director,  
NASA Ames Research Center*

**Integrated Planning and Response:  
A Systematic Approach to Homeland Security** .....[25](#)

*by Ronald E. Stoltz, PhD, Manager, Government Relations,  
Sandia National Laboratories*

A CRITICAL INFRASTRUCTURE

**Cargo and Seaport Security** .....[29](#)

*by Joseph N. Miniace, President and CEO,  
Pacific Maritime Association*

PUBLIC-PRIVATE COLLABORATION

**The Private Sector and the Public Sector:  
Homeland Security Calls for Unprecedented Collaboration** .....[35](#)

*by Sunne Wright McPeak, President & CEO,  
Bay Area Council*

PRIVATE SECTOR ISSUES

**Pursuing Counterterrorist Technology:  
Private Sector Interests and Public Policy** .....[41](#)

*by Nicholas Imparato, PhD, Professor of Management,  
University of San Francisco and Research Fellow, Hoover Institution,  
Stanford University*

**Positioning Security Technologies for the Future** .....[47](#)

*by Robert J.T. Morris, PhD, Chairman, BASIC, and Director of the  
IBM Almaden Research Center*

POLITICAL AND ECONOMIC CONSIDERATIONS

**The Political Economy of Protection:  
Appreciating the Political and Economic Aspects  
of Investments in Homeland Security** .....[53](#)

*by Jay Stowsky, PhD, Executive Director, UC Berkeley Project on  
Information Technology and Homeland Security*

**SECTION II**  
**BAY AREA TECHNOLOGICAL CAPABILITIES**  
**TO ADDRESS THE CHALLENGES**  
**OF HOMELAND SECURITY**

Introduction.....[59](#)

**EXAMPLES OF BAY AREA TECHNOLOGICAL CAPABILITIES**  
**RELATED TO THE CRITICAL MISSION AREAS**  
**OF HOMELAND SECURITY**

Intelligence and Warning.....[61](#)  
Border and Transportation Security.....[67](#)  
Domestic Counterterrorism.....[71](#)  
Protecting Critical Infrastructure .....[73](#)  
Defending Against Catastrophic Terrorism .....[79](#)  
Emergency Preparedness and Response .....[85](#)

**EXAMPLES OF BAY AREA**  
**UNIVERSITY RESEARCH PROGRAMS**  
**BENEFITING THE NATION’S SECURITY**

Stanford University.....[91](#)  
UC Berkeley.....[93](#)  
UC Davis.....[95](#)  
UC San Francisco .....[96](#)  
UC Santa Cruz .....[97](#)

## **APPENDICES**

APPENDIX A: Bay Area Corporations with Expertise Related to Homeland Security (Companies Contributing to This Report) .....	<u>101</u>
APPENDIX B: Bay Area Leading Research Universities .....	<u>111</u>
APPENDIX C: Bay Area National Research Laboratories and Independent Research Institutions .....	<u>113</u>
APPENDIX D: Bay Area New Research Complexes .....	<u>117</u>
APPENDIX E: Authors of Section I Essays.....	<u>119</u>
Appendix F: BASIC gratefully acknowledges the financial contribution of Reed Smith Crosby Heafey supporting the production of this report.....	<u>131</u>
APPENDIX G: BASIC Board of Directors.....	<u>133</u>

## Message from the Chairman

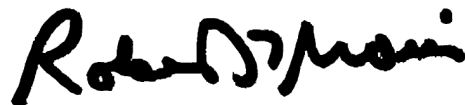
The nine-county Bay Area of Northern California—which encompasses Silicon Valley and the cities of San Francisco, Oakland and San Jose—is world-renowned as a center of R&D expertise and innovation, as well as an economic engine for the country. It is, therefore, only natural for our region to play a key role in homeland security, both as a key scientific and technological resource for countering terrorism and other disasters, and as a critical asset that must itself be protected.

It is this challenge that the members of the Bay Area Science and Innovation Consortium (BASIC) address in this second edition of our homeland security report. Bay Area companies and research labs have significant assets and innovations that can be used worldwide to enhance security. This report is intended to be a resource to those seeking such technologies.

We also consider this report to be a “call to action” for Bay Area leaders to initiate efforts to become a model for regional preparedness, response and recovery planning. BASIC strongly supports the view of Administration and Congressional leaders that regions of our country should independently develop local homeland defense programs to augment the federal government's initiatives.

Our region is already well-positioned to lead innovative collaborative, public-private efforts benefiting the security of the region, state, nation and beyond. To achieve this mission, we must carefully analyze potential threats to us and to our critical infrastructure. We must also develop the tools and techniques for implementing preventive measures and for facilitating a rapid and targeted response to mitigate potential damages. Finally, we must communicate our findings and solutions to homeland security agencies both near and far.

This is the challenge to the Bay Area’s leadership. BASIC is committed to assisting the region in achieving this goal.

A handwritten signature in black ink, appearing to read "Robert J. T. Morris". The signature is written in a cursive, flowing style.

Dr. Robert J. T. Morris  
Chairman





# MEETING THE CHALLENGE OF HOMELAND SECURITY

## EXECUTIVE SUMMARY

Terrorism is a major challenge to humanity and our nation, and a direct threat to our region. From sensors to computers, analytical instruments to databases, new and proven technologies alike can play critical roles in preventing terrorist acts, minimizing damage from them and locating those responsible.

The Bay Area's world-renowned research universities, national research laboratories, public and private research and development institutions and companies are making vital contributions to the scientific and technological advances required to enhance our security. This report—prepared by the Bay Area Science and Innovation Consortium (BASIC) as a planning resource for homeland security and anti-terrorism agencies and planners throughout the country and the world—highlights many of these important homeland security technologies and capabilities.

This report is divided into two sections. The first presents thoughtful essays by experts from the Bay Area's public and private sectors. These essays describe the:

- impact of weapons of mass destruction,
- needs of first responders,
- concerns related to protecting ports,
- Bay Area's wealth of public and private sector technological resources to address these needs,
- issues facing the private sector as it conducts business in this dynamic operating and policy environment,
- challenges to—and the potential of—increasingly sophisticated information technologies,
- difficult political and economic questions that may arise in defending the nation's critical infrastructure.

Most importantly, the authors of these articles emphasize the need for a collaborative approach by all sectors in order to ensure the security of any region.

The second section of the report highlights some of the technologies developed or being developed in the Bay Area to address the six critical mission areas identified by President Bush in his recommendation last year to establish the national Homeland Security Department:

1. ***Intelligence and Warning***  
System, data, communication and privacy protection; threat assessment and surveillance
2. ***Border and Transportation Security***  
Border, seaport, cargo and airport surveillance and security
3. ***Domestic Counterterrorism***  
Weapons, explosives, truck and car bomb detection, forensics and physical identification
4. ***Protecting Critical Infrastructure***  
Cybersecurity, structural analysis and entry security
5. ***Defending Against Catastrophic Terrorism***  
Chemical, biological, nuclear detection, and building decontamination
6. ***Emergency Preparedness and Response***  
Data and IT systems response and recovery, public alert and communication networks

Public agencies and private companies alike can take advantage of these technologies to enhance homeland security and to help protect their own assets from the potential impacts of terrorism.

Moving forward, BASIC will focus its efforts on promoting the use of Bay Area technologies in homeland security. It is convening a regional Homeland Security Team to collaboratively develop and implement an action strategy to match the needs of first responders with the appropriate technologies and unique capabilities of Bay Area companies, universities and laboratories. BASIC will also serve as a forum through which the region's scientific and technological leaders can identify and collaboratively address new regional and national homeland security challenges and the policy implications of innovative technological approaches.

## **SECTION I**

# **ESSAYS ON THE CHALLENGES OF HOMELAND SECURITY**



# **Today's Terrorist Threat: Weapons of Mass Destruction**

*by Roger W. Werne, PhD, Chief Engineer, Nonproliferation,  
Arms Control, and International Security Directorate,  
Lawrence Livermore National Laboratory*

Weapons of mass destruction (WMD) including chemical, biological, radiological and nuclear weapons, represent a direct threat to the United States and its allies should they come into the hands of terrorists. More than 20 countries, some of them hostile to the U.S., are suspected of or known to be developing WMD, and some of these are clear supporters of terrorism against the U.S. Cyber-terrorism is an additional concern that parallels the WMD threat, given this country's vital dependence on the unrestricted flow of information.

## **Chemical Weapons**

Chemical weapons deliver toxic agents as a gas or aerosolized liquid which debilitate or kill upon inhalation or skin contact. Because these chemicals can be widely dispersed, they can rapidly injure or kill large numbers of people. Nerve agents, such as sarin and blister agents like mustard gas, are of particular concern. Chemical weapons have been used in warfare as recently as the 1980s, in the Iran-Iraq war, and the psychological barrier against terrorism use of WMD was broken in 1995, with Aum Shinrikyo's attack on the Tokyo subways.

Because of the near-immediate effects of chemical weapons, the collapse of affected people is often the first indication of an attack. And unless first responders are equipped with protective suits and respirators, they will end up as victims as well.

## **Biological Weapons**

Biological weapons typically use bacteria or viruses that cause illness or death in infected humans, animals, or crops. Pathogens such as *Yersinia pestis*, *Bacillus anthracis* and *Variola major* (the causative agents, respectively, of plague, anthrax and smallpox) are major sources of concern. After initial infection, there is an incubation period of typically several days to two weeks before clinical symptoms appear. Some biological agents such as the smallpox virus are highly communicable, whereas others like the anthrax bacterium are less contagious. All of these diseases are highly debilitating and typically deadly if untreated. However, effective treatments are available if infection is promptly diagnosed. Technologies and tools for early detection of a bioattack and rapid identification of infection can greatly improve defense against bioterrorism.

## **Radiological and Nuclear Weapons**

A radiological dispersal device (RDD) or dirty bomb uses conventional high explosives to disperse radioactive material over a wide area. Because no nuclear yield occurs, physical damage and casualties are limited to the zone directly affected by the high explosive. However, extensive, costly and time-consuming cleanup is required to restore the contaminated area to normal usage. Thus, RDDs cause more psychological damage than actual casualties.

On the other hand, an improvised nuclear device (IND) is a crude nuclear bomb capable of nuclear yield. It is expected that a nuclear device manufactured by a terrorist group would be crude compared to the nuclear weapons of the declared nuclear states. As high school students demonstrate every few years, the information necessary for the design of a nuclear weapon is available in the open literature. However, the actual manufacture of a weapon is technically very challenging. In addition, the International Atomic Energy Agency (IAEA), together with the U.S., Russia and other concerned countries, have extensive safeguards in place to keep weapons-usable nuclear materials out of the hands of proliferators and terrorists.

It is conceivable that terrorists could acquire a stolen nuclear weapon. Terrorist use of such a weapon would cause enormous casualties and damage; most modern nuclear weapons are tens to hundreds of times more powerful than those used to end World War II. However, terrorist acquisition of a stolen nuclear weapon is considered highly unlikely, since the U.S., Russia and other nuclear weapon states have their weapons under very strict security.

## **Cyber Attack**

The U.S. and other developed countries have become highly dependent on interlinked information systems and infrastructures. The rapid and unrestricted flow of information is critical for controlling such activities as power generation and distribution, banking and finance, transportation, manufacturing and healthcare. These activities are necessary for the conduct of everyday life and essential to the maintenance of our democratic society. Wide-spread or long-term disruption of any of these infrastructures could significantly damage our welfare and economy. The disruptions caused by repeated hacker attacks and the recent electrical blackout in the Northeast hint at the widespread economic damage that could result from a concerted cyber attack by terrorists.

## **Defending Against the WMD Threat**

The formation of the U.S. Department of Homeland Security (DHS) is an important first step in developing a national defense against terrorist threats. The DHS will tap the vast scientific and technological resources of the nation to develop and deploy systems throughout the country to detect the development and respond to the use of WMD by terrorists against the U.S.

Within the Bay Area we have unique research and development (R&D) assets that can be leveraged to meet this challenge, including the Lawrence Livermore National Laboratory (LLNL) and Sandia National Laboratories (SNL), two of the nation's premier national security R&D institutions. Among its many capabilities, LLNL operates the National Atmospheric Release and Advisory Center (NARAC), which is on call 24 hours a day to track and predict the dispersal of chemical, biological, radiological, or other hazardous materials released into the atmosphere from anywhere in the world. This system has been called upon multiple times to respond to regional incidents, including smoke from burning tires and chemical releases from area refineries.

For biodefense, LLNL, together with the Los Alamos National Laboratory, developed the Biological Aerosol Sentry and Information System (BASIS). BASIS has been deployed at the 2002 Winter Olympics in Salt Lake City and other venues around the country. Sandia has developed a suite of novel sensor systems for detecting chemicals and high explosives. The national laboratories work closely with various response agencies, including the U.S. Customs, the Coast Guard, and state and local law enforcement, to ensure that the technologies and systems they develop meet real-world operational needs.

Lawrence Livermore, Sandia and the other national laboratories are an important resource for the country and the Bay Area. Laboratory personnel are eager to work with Bay Area public officials and first responders to understand the challenges they face and to bring the resources of the national laboratories to bear in assisting the region to prevent, detect, respond to, and recover from WMD. However, as extensive as these capabilities are, we must not rely on the federal government alone to address and solve regional problems.

The Bay Area's public and private sectors must work together to cooperatively leverage the region's many resources and develop an effective defense against terrorism.





# Cybersecurity

*by Joe Raguso, Vice President of Strategic Partnerships,  
SRI International*

The threat of terrorism in the United States is largely understood in the context of the terrible tragedy of 9/11. The attack on the World Trade Center seared into our collective consciousness massive loss of life, physical damage, and financial damage to the United States. Our public and private sectors are now reviewing all key infrastructures and response systems to improve the security and safety of our citizens. Less well understood, and especially difficult to defend, is a terrorist attack via the Internet, where a devastating attack could cause little physical damage, but permanently harm key segments of the U.S. economy by disrupting information and eroding confidence. Simple examples include:

- Shutting off access to—or providing misleading information about—financial data: “My 401(k) disappeared.”
- Wiping out or interrupting prescription records: “I can’t get my insulin.”
- Causing massive uncertainty and lack of trust in the stock market: “I didn’t buy that stock.”

The technology exists today for terrorists to attack via the Internet—our “electronic highway.” The attacks can be accomplished with the electronic equivalent of “box cutters”—simple tools available to everyone. Individual hacker attacks on the Internet, primitive as they were, have already caused billions of dollars of losses. In 1999, the “Melissa” virus caused \$1 billion in damage. In 2000, the “Love Bug” cost \$15 billion. In 2001, “Code Red” cost \$1.2 billion. In 2003, “Slammer” was able to reduce the performance of the top 40 U.S. sites by an average of 50% for at least one hour.

A well-organized terrorist cyber attack can dwarf these hacker attacks, and cause a massive explosion of network damage by, for example, attacking repeatedly, and at will, specific industry sectors and the Internet backbone.

Defending against a well-organized attack through the Internet is very difficult. Our networks are open to all, controlled by none, and designed with “trust” as an implicit assumption. An attack can start from anywhere, anonymously, and create massive damage to millions of computer systems within fractions of a second. “Safe computing” practices can help raise the bar for attack, but will never eliminate it. Attacks can occur on entire industry segments, with individual victims never being aware of the attacks on others, let alone being able to warn them.

The challenges are significant:

- How can we continuously discover and eliminate existing and evolving vulnerabilities in real-time given the dynamic nature of network configurations and applications?
- How can individuals and organizations share information to mitigate risks?

Neither individuals nor companies wish to share personal or competitive information with each other or the government. Yet most solutions or methods to improve security and protect against cyber attack require massive information sharing. This dilemma has been frequently noted in the press, with literally dozens of articles discussing this subject, pitting “big brother” against freedom and privacy.

As articulated in the National Strategy to Secure Cyberspace, President Bush asked the best and the brightest in the IT industry, the cybersecurity research community and information infrastructure practitioners to develop solutions to this challenging problem. Elements of this strategy include creating a real time early warning system, response plan, mitigation strategy and recovery capability while maintaining individual and corporate privacy.

As a world leader in IT innovation, the Bay area is responding to the need to immediately reduce our cyber vulnerabilities. This region has the largest number of organizations addressing this challenge through research, development, or deployment of critical technologies. The list includes: Stanford University, UC Berkeley, Lawrence Livermore National Laboratory, Lawrence Berkeley Laboratory, SRI International, Symantec, NASA Ames, UC Santa Cruz, Sun, Oracle, Cisco, Microsoft, IBM, HP, Network Associates, Silicon Graphics, Novell, Lockheed, Verisign, Sanctum, Arcsight, Cylink, and Wells Fargo among others.

As the magnitude of the problem continues to come into focus, it is clear that the solution will require a public-private partnership between government and industry, and is certain to include a significant portion of representatives from the Bay Area.

# **The Role of National Laboratories and Universities in Bay Area Preparedness**

*by William A. Barletta, PhD, Coordinating Director,  
Homeland Security and Non-Proliferation Programs,  
E. O. Lawrence Berkeley National Laboratory*

*and Jody R. Westby, President, The Work-IT Group, Denver*

Viewed from Washington, the Bay Area's national laboratories offer an enormous resource for meeting the scientific challenges that underlie enhanced domestic security. The Department of Energy's weapons laboratories have a long history of supporting defense and intelligence agencies both in threat analysis and in developing low profile detection, prevention, and response technologies. Even before the September 11th attacks, technology R&D efforts focused on detecting the proliferation of nuclear, chemical and biological weapons of mass destruction had become major enterprises at the weapons labs and, in certain cases, even at the open science laboratories. As the Department of Homeland Security (DHS) moves toward establishing a Homeland Security Advanced Project Research Agency and the designation of regional centers of technical excellence, we can expect accelerating efforts to develop and field test numerous technical resources, such as:

- Non-intrusive, stand-off detection and imaging systems;
- Methods and materials to control, track, and reduce the availability of hazardous materials;
- Light-weight protective and barrier equipment and materials, filtration systems and explosive containment structures, and other methods to protect people, animals, crops, and public spaces;
- Means to predict the fate and transport of toxic and infectious materials, pre-symptomatic medical diagnostics, and methods to immobilize and neutralize hazardous materials.

Regional stakeholder associations can encourage DHS investment in the DOE national laboratories and user facilities, which complement private sector research and provide an ideal environment to carry out this highly collaborative work.

At the regional level, uncertainty about how the new DHS will function, combined with the lack of funding for state/local initiatives, has led to a lack of focused action. The reality is that local and regional governments will be the first to respond to terrorist attacks. They, therefore, have the responsibility to create new risk management plans to ensure public safety. Public emergency management plans have traditionally been based on potential incidents or events, rather than directed attacks. Some of these events may be disasters such as earthquakes. Yet even extensive natural disasters are not aimed at civilian targets and do not have the same psychological effect. Also, they do not have the same impact on the credibility of local, regional and national authorities.

Chemical, biological or radiological attacks will engender a persistent level of fear in the public that is not usually present in natural occurrences. Consequently, many municipalities have not developed response plans that address the complex correlation of vulnerabilities in the face of multiple, asymmetric attacks. Such attacks will require coordinated public-private sector action that is likely to involve federal, state, and local responders, government officials, and private sector stakeholders acting on an urgent timeline.

Especially in the case of chemical, biological or radiological attacks, responders need to know what technology and which experts they require to contain and mitigate damage and to minimize loss of life. As seen in the Oakland Hills fire, effective, timely response can be seriously handicapped by incompatibilities in existing infrastructures such as communications, and inconsistency in operational rubrics across our Bay Area communities. In addition, local decision-makers who must handle attack situations may not have sufficient knowledge or a guiding framework regarding the vast legal and policy issues that must be factored into response situations.

Response plans need to address numerous, critical interfaces between the public and private sectors. For example, a dirty bomb or other radiological terrorist attack in the Port of Oakland would impact numerous other private sector entities, such as shipping companies, container operations, dock crews, fishing operations, trucking companies, catering and restaurant facilities, ship repair services, etc.

An effective response to a terrorist attack demands that public sector responders interface quickly and effectively with the private sector. An attack is not a time for gadgets and devices; it is a time for solving complex human and technical problems rapidly in an incisive manner. As public institutions, the Bay Area's national laboratories and universities have a special opportunity and concomitant responsibility to serve as resources to the region and utilize their vast expertise to help develop a response plan that will take into account all risks and issues. The areas in which the laboratories and universities can and should assist local and regional stakeholders include:

- Assisting municipalities in assessing their vulnerabilities as part of developing appropriate response and training plans;
- Assessing how the consequences of an attack may propagate outward from the primary target;
- Analyzing legal, policy and public health matters and weaving these into response planning, training, and decision management;
- Assisting municipalities in developing models for public-private sector cooperation and coordination between federal, state, and local responders;
- Identifying, developing, and making available our region's best science and technology relevant to multi-prong attack scenarios, so responders have the best information and tools when seconds matter;
- Developing self-healing or self-mitigating infrastructures (such as energy and communications networks) and technical systems to assure continuity of governance and economic vitality.

Because security threats require a multi-disciplinary response, technological solutions will continue to dovetail with policy issues. It is a truism that modern societies depend upon the goodwill of the entire population to function smoothly; the more technological the society, the more fragile the structure is with respect to random malicious acts. In no arena is this maxim truer than that of information infrastructure—a hallmark technology in the Bay Area. As information networks and processing systems become more broadly interconnected with critical physical infrastructure, and the dependency upon these systems becomes more complex, risks associated with malfunctions increase dramatically. Scientists and technologists have important roles to play in each phase of consequence management: assessment, planning, prevention, training, detection, and response.

The dramatic and rapid developments in electronics, biotechnology, robotics and information technology for research and commerce raises the bar for keeping pace in the areas that are most vital to assuring homeland security. The greatest strength of our research community, including both national laboratories and universities, is free and open inquiry combined with the ability to engage the very best minds regardless of their country of origin. For example, in the Bay Area, applied genomics, proteomics, and biotechnology that are vital to future bio-defense are developing at a rapid pace. Rapid sequencing of bacteria is already available in open, government-supported, and commercial laboratories. Information technology is vital to the rapid application of developing science and technology. Data mining will be crucial in providing law enforcement and intelligence agencies with early warning of dangerous groups and in providing supporting forensic information. Nanoscience and the associated technology of designer materials will permit novel imaging and spectroscopic techniques for cargo inspection, forensics, and material tagging.

Our local and state governments, law enforcement, intelligence and defense agencies must actively engage the academic and commercial worlds if they are to be at their most effective in combating international terrorism. The mode of that engagement must respect the open environment at the heart of scientific creativity and economic vitality.

# **Meeting New Challenges: Building on Lessons from Natural Hazards Response**

## **A Perspective on Local Governments as First Responders from the Association of Bay Area Governments (ABAG)**

*by Jeanne Perkins, Principal, Earthquake Program,  
Association of Bay Area Governments*

Cities and counties around the nation face a daunting challenge—to be the first line of defense in response to terrorist attacks. The Bay Area’s public sector, however, may be in a better position than many other regions to respond to this challenge. Just as the businesses, universities, and research laboratories in the San Francisco Bay Area have been leaders in research and technology development, the cities and counties in the region have been leaders in dealing with natural and man-made disasters.

Bay Area cities and counties not only deal with the emergencies within their communities, but also are responsible for elements of the critical infrastructure in their jurisdictions. The Cities of San Francisco, Oakland, and San Jose administer three international airports; Oakland and San Francisco host two international seaports. Numerous counties in the region administer extensive public health programs, medical support systems and major hospitals. Many cities are responsible for wastewater systems and treatment, and some for water supply distribution and treatment for multiple cities and counties. The protection of these public services is critical.

### **Lessons Learned**

The importance of coordinated emergency response capabilities was vividly demonstrated to the region in two Bay Area natural disasters—the 1989 Loma Prieta earthquake and the 1991 Oakland Hills firestorm. These two events drew attention to the need for better coordination among local government, fire and police departments, water and power utilities, and State of California agencies.

Experience in responding to disasters provides the Bay Area with a solid foundation for developing the expanded plans required for responding to terrorist threats. The Association of Bay Area Governments (ABAG), as the regional council of governments and planning organizations owned and operated by the region’s cities and counties, can play a key role in coordinating this effort.



## **Ongoing Programs**

### ***The Standardized Emergency Response System***

Since 1993, the Standardized Emergency Response System (SEMS) has been used to provide a clear and consistent organizational structure modeled after the *Incident Command System* developed to respond to wildland fires. It incorporates a mutual aid system for obtaining emergency resources from other cities and counties not affected by a specific disaster. SEMS offers standardized approved training to all users. All State government agencies are mandated to use SEMS and all local government agencies responding to multi-jurisdictional emergencies must use SEMS to be able to receive State reimbursement of response-related personnel costs. SEMS is now a model for managing emergencies nationally.

### ***Personal Preparedness***

Many cities and counties in the Bay Area are using the Federal Emergency Management Agency (FEMA)'s Community Emergency Response Team (CERT) training programs to improve the preparedness of their residents. Bay Area cities were among the first to use the program and many have expanded the CERT program to develop a forum for sharing information and to incorporate business continuity planning in the effort through *BayNet*. Meetings of *BayNet* also include business continuity planning and have become a model forum for public-private collaboration.

### ***Transportation Systems***

ABAG has been a national leader in identifying the critical role of functional infrastructure, particularly transportation systems, not only in emergency response, but also in ensuring rapid economic recovery. ABAG's efforts have included modeling of road and airport closures, as well as developing innovative outreach strategies. These programs complement the work of the region's Metropolitan Transportation Commission (MTC) and Caltrans in their planning to identify routes that are critical for life safety and emergency response, to examine routes that serve major roles in the economic recovery of the Bay Area, and to evaluate performance level needs for these routes and their structures. MTC has also developed a *Trans Response Plan* for a multimodal transportation response that is integrated into the overall emergency response for the nine-county area.

## **Next Steps**

### ***Need for Improved Emergency Communications***

Because of the large number of independent cities, counties, utilities, and special districts in the region, as well as the vulnerability to natural hazards, the need for coordinated emergency communications became obvious here earlier than in many other metropolitan areas. Some cities have taken major steps to enable all first responders to talk with each other at the scene of an emergency. But for many other local jurisdictions, the costs and technical complexity of integrating police, fire and other first-responder communications and mapping systems have prohibited them from making the necessary improvements. In addition, the present efforts in most cities do not include communication with relevant regional organizations nor with state and federal agencies. These are critical response issues and must be addressed.

### ***Need for Improved Field Equipment***

The Bay Area is home to one of the highest concentrations of Metropolitan Medical Response Systems (MMRS) and Metropolitan Medical Task Forces (MMTF) in the country. These systems include police, fire, emergency services, emergency medical services, public health, emergency medical transportation, hospitals, private medical providers and the medical examiner/coroner as partners in developing and exercising response plans for terrorist events. This preparedness has led to dual use capabilities that enhance the response to hazardous materials accidents, epidemics, and civil unrest events.

However, while the training and exercise programs have been very beneficial, better field level equipment is needed to enhance the speed of response to dangerous incidents. Most critical is the need for an affordable and easily maintained community alert and warning system with multi-hazard capabilities. In addition, handheld detectors with higher levels of sensitivity are needed for chemical materials and biological materials. A partnership between the city-based MMTF's and the research and development community in the Bay Area could lead to important innovations in these areas.

We also need a better medical surveillance and intelligence/information handling system. Algorithms need to be developed for baseline data, and automated processes integrated to evaluate data that is entered into the system in real time to determine illness patterns or syndromes that could indicate a terrorist attack or severe epidemic in the earliest stages.

## **Conclusion**

The experience of Bay Area cities and counties can provide valuable insight in developing a public-private collaborative approach to a regional plan for homeland security.

ABAG has been a leader in performing research to improve earthquake mitigation and preparedness by local governments and businesses, an expertise that can be used to develop and test ways to increase terrorism preparedness for the region.

## **A Public Sector Perspective on Meeting the Challenge of Homeland Security**

*by Frances Edwards-Winslow, PhD, CEM Director,  
Office of Emergency Services,  
City of San Jose*

For many years, Americans considered terrorism an activity that takes place in the Middle East or Europe. The attack against the World Trade Center in 1993, the 1995 destruction of the Murrah Federal Building in Oklahoma, and the horror of the 9/11 attack in New York City sent the clear message that domestic terrorism is a real probability that must be faced by cities across the U.S.

The public sector is faced with some very sobering facts: terrorist attacks are no longer limited to bombing buildings or vehicles; instead civilian authorities must respond to terrorist events that could involve the use of weapons of mass destruction (WMD)—military chemicals and weaponized biological agents with the power to affect thousands of people. Within the designation of WMD are three broad categories: nuclear, biological and chemical. These WMD agents have the potential to create chaos within the civilian community and disable large numbers of police, fire and emergency medical personnel—a city’s “first responders.”

Adding to the burden of cities and counties is that these awesome challenges must be faced at a time of decreasing budgets and decreasing staff. However, since the challenges must be met, the public sector must integrate training and equipping for WMD with its daily work. This “dual use” approach maximizes the benefits of training and equipment to the community, while enabling the first responders to sharpen their skills. This approach is effective because a biological attack is really a very bad epidemic, and a chemical attack is really a very bad hazardous materials event.

There are a number of federally funded programs to assist cities and counties in the training of first responders and in developing appropriate plans. However, the cost of participating in such training may be an obstacle. While the instruction is generally offered free of charge, the cost of the students’ time to attend the classes must be borne by the receiving agency, usually at overtime rates. For example, in the first year of San Jose’s WMD training, the Police Department alone spent \$1 million in overtime to ensure that all personnel received the basic training.

Regardless of the difficulties, cities must develop an adequate internal response capability since help from outside sources takes too long to arrive. Cities must develop a dual use approach to WMD planning and training, building on their own knowledge and taking advantage of the resources available within the region.

## **Recommended Actions**

### ***Cooperative Efforts on Training***

Cities could assist other cities in the training of first responders. As part of the designation as a Metropolitan Medical Task Force city, San Jose received five DOD training courses designed to equip local government first responders with the knowledge to respond safely and to save the maximum number of victims of a WMD event. San Jose has provided first responder training to other cities in Santa Clara County and would be willing to work with other cities around the region to provide train-the-trainer courses for their first responder organizations.

### ***Realistic Assessment of Threat Level***

All cities do not face the same level of threat—a metropolitan city with an important economic infrastructure is at a higher level of threat than a small, residential city. Each city needs to assess its individual threat level, as this would determine the level of preparedness necessary for that community.

### ***Adequate Emergency Response Plan***

Most cities have an existing Emergency Operations Plan based on response to earthquakes and other natural disasters. The plans should be upgraded to the necessary level of preparedness to address a terrorist attack using biological, chemical, or radiological materials, and involving multiple casualties. Considerations would include recognition of a terrorist event, methods for decontamination of patients when appropriate, triage and basic and advanced life support actions at the field level, emergency medical transport considerations, and communications with hospital resources. Plan elements for tracking illness in a community and for the administration of appropriate vaccinations or antibiotic prophylaxis are also essential. Planning must be followed by appropriate training for employees and exercises of the plan to ensure its usefulness.

### ***Adequate Analysis and Response Equipment***

Responding to a terrorist attack using weapons of mass destruction requires the rapid identification of the agent used. First responders must have analysis equipment in the field that provides information on the agent quickly to ensure that the proper medications are administered, and the proper precautions are taken. For example, persons suffering from exposure to nerve agents require immediate thorough decontamination and atropine, while someone exposed to pepper spray only requires removal of contaminated outer clothing and eye wash.

Dealing with biological materials is even more complex, as the rash of “white powder” calls in the fall of 2001 demonstrated. Public safety resources were consumed managing the cleanup of common household substances because there was no rapid method for determining whether a substance was anthrax or something benign. A sophisticated tool for analyzing the composition of a biological agent’s DNA is necessary in a lab, but at an emergency scene, a first responder needs a simple, easily interpreted instrument that provides immediate confirmation as to whether a particular substance is a living organism. This “rule in”/“rule out” approach would allow most such calls to be handled with a rapid wipedown of the surface and reassurance for the concerned caller that the item was not anthrax. The few test results recognizing a living organism could then be tested at the county health laboratory for additional characterization, and only those few potential victims would have to be tracked to await a decision on the necessity for treatment.

### ***Adequate Communication Tools***

Communication tools must be operable in any environment and across city and county boundaries. First responders have long expressed concern that police, fire and emergency medical transportation services used different frequencies. The World Trade Center tragedy was exacerbated by lack of communications interoperability. Technology can be part of the solution, enabling existing frequencies to be used more broadly, and creating one instrument that can reach a variety of spectra.

### **Closer Coordination with the Private and Public Sector Labs and Technology Companies**

The public sector must understand the type of assistance they can receive from the region's national labs and they must clearly define their technology needs to the private sector. A close coordination with the labs and with the private sector will be an important foundation for building effective regional preparedness. Opportunities for information sharing should be enhanced so that channels are created for first responders to register needs, and for inventors to find test beds for their products, once they have been proven effective scientifically.

### **The Bay Area Could Become a National Model of Public-Private Sector Response to Homeland Security Challenges**

The Bay Area has the creativity and resourcefulness to become a center for excellence in the development of technologies to support homeland security. A partnership between the public and private sectors would ensure that scarce R&D resources are invested in the most productive way, assisting first responders and boosting the local economy.

# Technology Development for First Responders

*by Peter Friedland, PhD, Special Assistant to the Director,  
NASA Ames Research Center*

The tremendous wealth of scientific and engineering expertise embodied in the Bay Area's federal research laboratories, research universities and institutes, and corporations (both large and small) positions the region to be one of the nation's premier resources for homeland security. This is true for both the short-term development of technology to meet the immediate needs of first responders as well as in building a scientific research program that will provide greater security to our nation over the long term.

One particularly efficient way to combine both endeavors is through the creation of collaborative research centers which bring together in one physical location the combined expertise of governmental, industrial, and academic partners. A prime example is the NASA Research Park (NRP) in which NASA Ames Research Center (ARC) partners and collaborates with the broader academic and corporate research and development (R&D) community. This approach of combining historical technological expertise with the thinking of other sectors will be important in rapidly developing the technologies required for homeland security.

ARC's over thirty years of experience in advancing space research has become directly relevant to homeland security, particularly in the areas of Information Technology, Human Factors, Aviation Safety and Security, Biomedical Instrumentation and Detection, and Unmanned Aeronautical Vehicles (UAVs).

In addition, ARC is the official designee for both NASA and the State of California in search and rescue (and the only federal center outside of the Federal Emergency Management Administration with this responsibility). Since 1985, the 120-person Disaster Assistance and Rescue Team (DART) has participated in search, rescue, medical work, and damage control for all major urban disasters. DART also serves as a technology testbed for such problems as search within collapsed structures and development of hazardous-response vehicles. ARC conducts training for rescue teams throughout the entire United States.



## **New Technologies Needed for First Responders**

The initiation of a comprehensive technology development program for the vital needs of first responders is likely to lead to a rapidly useful and steady stream of practical products broadly applicable throughout the nation. The development of these new essential technologies is a priority challenge to the public and private research laboratories. Among the important areas of research and development proposed at ARC are:

### ***Protective Clothing***

Protective clothing is vital for use in physically (high temperatures, sharp objects, etc.), chemically, or biologically dangerous environments. The clothing must be able to monitor vitals, precisely track locations, be wearable for extended periods of time, provide both audio and video communications, and be cost-effective for routine use. Expertise in information technology, materials (such as those already used in NASA-developed space suits), and human factors is particularly important as is the practical experience and test subjects provided by the DART team and associated agencies.

### ***Victim Location***

Technology is needed to rapidly locate victims of disasters, particularly in collapsed structures. This includes work in listening and thermal sensing devices, as well as Information Technology to model the physical characteristics of the structure and the disaster to predict void spaces that might contain survivors. Such technology should also give rescue teams a comprehensive view of their search environment, informing them of the specific location of power lines, hazardous materials, etc.

### ***Vehicles to Access Hazardous Areas***

The right mix of autonomous and manned vehicles, equipped with robotic manipulators and monitoring devices, is important to rapidly and safely gain access to hazardous areas. The clear goal is expeditious location and immediate (without causing further injury) removal of victims with minimization of potential risk to rescuers. Expertise in robotic mobility, sensors, and effectors, UAVs (for rapid site assessment), and bio-instrumentation is critical here. One of the major NRP tenants, Carnegie Mellon University, was key in developing robots for disaster amelioration at such locations as Three Mile Island and Chernobyl.

### ***Intelligent Assistants***

The extension of over 15 years of NASA research on computational tools to aid astronauts and mission controllers can provide direct assistance to rescue specialists that incorporates recommended procedures for all likely-to-be-encountered situations during response to a disaster, and provides for planning and scheduling of response activities, even during communications failures. The Bay Area, through such companies as Palm Computing and Palm Source, has been the world's leading innovator in Personal Digital Assistants (PDAs), the likely platform for widespread proliferation of these systems.

### **Public-Private Collaboration**

The Bay Area's national research laboratories, research universities and public and private research labs, through their specific expertise and in collaborative programs, can make important contributions in the research and development of technologies to assist cities across the nation in protecting their people.



## **Integrated Planning and Response: A Systematic Approach to Homeland Security**

*by Ronald E. Stoltz, PhD, Manager, Government Relations,  
Sandia National Laboratories*

Preparing for a possible terrorist event can quickly overwhelm individual agencies or localities. The number of targets, the concentration of our population, the means of delivery and the kind of attacks seem so large as to be almost intractable. However, there has been extensive preparation and thinking about other large disasters that provide some guidance. The Bay Area and California have developed responses to earthquakes (mirroring terrorist explosive attacks), disease or epidemic outbreaks such as influenza, hanta virus, plague and now SARS (similar to bio-terrorist attacks), and major industrial chemical releases (mirroring chemical attacks). Radiological events have not been as thoroughly rehearsed, but there are still those in the response community that remember the efforts to prepare for radiological/nuclear events from civil defense preparedness days.

To be sure, terrorist attacks entail a special set of circumstances. The concentration of lethality and choice of single or multiple attack locations is an issue. Secondary attacks must be considered as well as the fear among the population that malicious attacks engender. Also, forensics and the need to identify those responsible change the way we deal with the early and later stages of an attack.

While planning for and responding to an attack on our homeland is daunting, Sandia National Laboratories, along with Lawrence Livermore and Los Alamos National Labs have developed comprehensive approaches, with specific themes and concepts of operation, as well as targeted technologies. While Sandia focuses on large scale, weapons of mass destruction attacks, the approaches, concepts and technologies are widely applicable. The keys to success, i.e., reducing casualties and disruption, are a systems approach to the problem and a focus on the interdependencies that help our society function.

## **Facility Operators and Business Owners: The First, “First Responders”**

Modeling and simulation of terrorist attacks using weapons of mass destruction targeted at airports, subways and major office and government buildings has shown that the first five to fifteen minutes are critical if one is to reduce the number of casualties. The responsibility thus falls to facility owners and operators to take the first actions and to prepare for the arrival and assistance of fire, police and emergency medical personnel.

Sandia and its partners have worked extensively with the San Francisco Airport and the Washington Area Metro to analyze airflow, movement of people and equipment, performance of existing monitoring systems (both visual and chem/bio detectors) and their emergency response plans. Two lessons emerge from these exercises. First, even without an operational detection system, passive protection can reduce casualties. Improvement to physical security can reduce the likelihood of successful attacks. Passive systems can be set in place to contain the event and preplanned evacuation has been shown to be very helpful in limiting exposure both inside and outside the facilities. Secondly, commercially available chemical sensors can be modified to operate continuously and in compromising environments like subways and airport ramp areas. Biological sensors are improving, with systems now available to detect the presence of bio-active materials and new systems in prototype stage to identify specific pathogens. Sandia and the other defense national laboratories are working with the Department of Homeland Security’s Science and Technology directorate to be sure the right technologies are being developed, tested and deployed.

Sandia has long expertise in architectural safety and design, dealing with explosive attacks to buildings and critical installations. The Lab has performed blast damage assessments of facilities that provide owners and operators with guidance as to mitigation and remedial actions. Many of the safety barriers and access restrictions, especially to underground parts of major buildings, were installed using guidance developed by Sandia.

Once fire, police and emergency medical personnel arrive on scene, a more complex and sophisticated set of technologies and approaches can be employed. Sandia has developed, based in part on the needs of the DoD, a hand-held “micro-ChemLab” that can analyze and determine specific chemical and biological agents. Sandia has entered into cooperative arrangements with a large chemical analysis equipment company to commercialize this device. Sandia has also commercialized and deployed a decontamination foam for use with biological agents. This technology is now used by the military, facility owners and some fire companies and can be used to decontaminate personnel, equipment and buildings. The foam is highly effective and does not leave a residue or produce side effects in treated individuals. It was used extensively following the anthrax attacks in late 2001.

Sandia also has a decade of experience with technology and training for explosives and bomb disposal operations. A patented technology allows bomb disposal units to neutralize unexploded ordnances without destroying the forensic evidence needed to both track and prosecute terrorists. The technology, along with other tailored devices and robotic systems, has been installed during major entertainment and public events and was successful in dealing with the Unabomber case in the late 1990's. Sandia also holds frequent training sessions, under the label *Operation America*, where bomb disposal units from the military, police and special security forces are trained in using the latest technologies.

### **Assessing Complex, Critical Infrastructures**

Two complex components of our civilian infrastructures that have received special attention are municipal water districts and the nation's seaports. Sandia scientists and engineers have developed an analysis and planning guide for operators of water systems. This guide allows operators to determine their potential vulnerabilities, to begin to plan for appropriate monitoring systems and locations and to develop remediation plans to deal with both terrorist and naturally occurring events. The methodology is published and widely available. Lawrence Livermore scientists are now assisting regional water operators to implement the approach, which is now required by the EPA.

In order to reduce the likelihood of disruption to seaports and container facilities and prevent terrorist attacks, a comprehensive approach must be taken. Sea-going cargo analysis, information technologies, perimeter and boundary protection, WMD sensors, personnel certification and container tracking systems are all critical. These areas are components of the maritime system being analyzed by Sandia as part of an effort under the *Operation Safe Commerce* effort. Sandia has been asked by the Ports of Los Angeles and Long Beach to lead their technical effort to provide port security. Sandia is currently funded directly by the ports and eventually under grants from the *Operation Safe Commerce* program. Sandia is working closely with the Port Authorities, the U.S. Coast Guard, other federal agencies and local organizations ranging from first responders to terminal operators. A recently completed analysis of the port is allowing operators to make smart choices on technologies and in parallel implement a "concept of operations" that integrates this technology into an operational framework.

## **Dependencies, decision analysis and test beds**

In partnership with Los Alamos National Lab, Sandia has established the National Infrastructure Simulation and Analysis Center (NISAC). Now part of the Department of Homeland Security programs, NISAC software is available to model the complex interdependencies between electricity, transportation, natural gas and other embedded infrastructures. These models can be tailored to specific regions and can be utilized to determine the optimum course of action that integrates threats and vulnerabilities into a comprehensive counter-terrorism plan.

To aid decision makers, Sandia has also established the Weapons of Mass Destruction–Decision Analysis Center (WMD–DAC). Focusing on biological and radiological attacks on major population centers, the Center is a user facility that allows key decision makers to “rehearse” their responses to crisis situations. A comprehensive model of the nine county Bay Area is in place and is being used for anthrax attack preparation. Infectious disease models and dynamic population modules are now being added. Sandia is working with county, regional and state agencies in California to extend this capability and to broaden the types of response parameters and training.

Finally, a consortium of national laboratories has established a prototype test bed in Albuquerque, New Mexico under the Bio Defense Initiative (BDI). The test bed integrates airport, hospital, public officials and emergency operations responses to simulated biological attacks. The most important outcome of the initial testing is an integrated communication plan and chain of command that is now being implemented in a multi-agency effort. Lessons learned from the BDI test bed are available to other regions and localities.

These examples highlight the ongoing technologies and programs available to first responders, facility operators, public officials, and the commercial sector in dealing with the potential of domestic terrorism. With the guidance and support of the Department of Homeland Security, the national laboratories are integrating their efforts and are helping to reduce the vulnerability of the nation to terrorist attacks.

## Cargo and Seaport Security

*by Joseph N. Miniace, President and CEO,  
Pacific Maritime Association*

*Challenges and Opportunity for the Marine Transportation System*, a white paper sponsored by the Marine Transportation System National Advisory Council dated July 16, 2001, stated that,

“Seaport security and crime must be addressed before a momentous event thrusts it onto the national agenda. Seaport security designed to combat terrorism will require a joint public and private approach in which multiple jurisdictions share resources and expertise to reduce exposure to attack.”

A few months later, a momentous event did thrust security onto the national agenda, but the terrorist attack came by air, rather than by sea.

Terrorism is generally facilitated through the misappropriation of transportation system assets. Cars and trucks laden with explosives were used to attack overseas embassies and military barracks. Commercial airliners were hijacked to strike the World Trade Center. A small craft was used to attack the USS *Cole*. Anthrax was delivered to its intended victims through the U.S. Postal Service. Each transportation mode was compromised through a breakdown in the chain of asset custody or through an unintended or unlawful use of transportation system assets.

The security of our ports is a critical issue for the Bay Area. With nine seaports—including the Port of Oakland, the nation’s fourth largest container port—this region is a potential target for terrorism.

The focus of this paper is to review the security of the water transportation system as it relates to cargo containers entering our seaports. Marine cargo, cargo that moves primarily on water, may change modes of transportation several times throughout its journey. These changes occur at intermodal connectors at seaports and involve the shift between water transportation and highway or rail transportation on land, and on rare occasions, air transportation.



The advent of containerization made cargo transportation more affordable. When Malcolm McLean loaded 20 modified truck trailers onto the deck of the *Ideal X* for shipment from New Jersey to Texas in 1956, containerization was born. The container “box” facilitated the movement of cargo and revolutionized an entire industry. No longer would cargo have to be palletized, bagged and baled and moved manually into a ship; cargo can now be stored in “boxes” and stacked neatly in a containership for easy loading and discharging. Thus, containerization opened the door to shippers who had previously been unable to afford to participate in the global marketplace. The container became the driving force behind world economic globalization.

Today, over twenty million container TEUs (twenty-foot equivalent units) pass through U.S. ports in international trade. The San Francisco Bay Area accounts for over one million of those TEUs. The TEUs total is projected to quadruple by 2025.

### **Port Security Issues**

The importance of international waterborne cargo has taken on heightened visibility since the events of 9/11. Enhanced security measures have been implemented, some resulting from accelerated normal business improvements and others through legislatively mandated security changes. Port security issues cover a range of cargo- and terminal-related activities including verification and tracking of arriving cargo; identification and authentication of arriving vessels and crew members; harbor, channel, and berth security; terminal land and waterside perimeter security; and truck driver, terminal employee and visitor identification and verification.

Other port security concerns include activities involved with passenger cruise ships, ferry transportation systems, and recreational boating. There is also concern about criminal activity and smuggling of people, drugs, and weapons.

Varying degrees of attention has been focused on various types of cargo vessels arriving from overseas; primarily on container vessels, but also on bulk and tanker vessels as well as auto carriers, general cargo vessels and other types of large and small vessels entering our ports.

Vessels loaded with bulk fertilizers, chemicals and petroleum products are seen as potential weapons *and* targets for terrorists. Various scenarios for terrorist attacks against bulk carriers and tankers have been under review for many years and methods for reducing the risk of a terrorist incident are continually being evaluated.

There have been discussions at many levels that cargo containers arriving from overseas are particularly susceptible to use by terrorists to move weapons. Terrorists seeking to avoid detection could quietly bring in relatively small pieces of larger weapons systems for later assembly. There is also speculation that an entire container could be co-opted and retrofitted as a weapon of mass destruction.

Most U.S. companies engaged in importing and exporting cargo in containers are well known entities with established and trusted overseas partners. Where the shipper, consignee, and cargo are known and where there is a history of transactions, the cargo moved by these companies may be considered low risk shipments and require less scrutiny. At the other end of the spectrum are cargo shippers and consignees that have little or questionable history. These shipments demand greater diligence.

### **Container Security**

A uniform international standard for ensuring the integrity and custody of international container shipments must be established to ensure homeland security. For world trade to continue to expand unimpeded, containerization must not be exploited by terrorists.

Since 9/11, many changes to security regulations and procedures were implemented to significantly reduce the chances for the misappropriation of waterborne containers for clandestine purposes.

While U.S. Customs has always required that cargo be reported upon arrival in a U.S. port, it was not unusual for cargo documentation to arrive separately from the cargo or for Non-Vessel Operating (NVO) carrier cargo to be labeled "Freight All Kinds" (FAK) without further explanation. Although government regulations specified that all import and export cargo manifested be accurately identified, the regulations were not precisely defined nor vigorously enforced. This is no longer the case.

On December 3, 2002, U.S. Customs instituted a new rule that requires advanced manifest filing for all waterborne cargo. Cargo intended for transport to the U.S. must be declared at least 24 hours before the cargo is loaded aboard a vessel at a foreign port. The 24-hour reporting rule and the accompanying regulations mark the beginning of a significant tightening of accountability for cargo custody.

Further changes are needed to ensure container integrity and real-time container tracking. With the right technology and careful planning, this can be accomplished without significantly expanding existing terminal footprints in our ports.

## **Need For Advanced Technologies**

There has been increased emphasis on inspecting inbound containers. This includes the use of gamma-ray penetrating radiation equipment to examine container contents. The U.S. Customs Service uses a gamma-ray system called the Mobile Vehicle & Cargo Inspection System (Mobile VACIS™) to inspect the contents of containers.

The Bay Area is one of the leaders in the development of new technologies for the protection of our ports.

It has been suggested that a parallel could be drawn between x-raying airline passenger checked baggage and “x-raying” containers. Comparing a 40-foot container to a piece of personal baggage is not a valid comparison because the custody and environmental security for each is very different. Airline baggage remains in a very secure environment after it passes through the x-ray machine and remains in that environment until it is picked up by its owner at the baggage claim area after completion of the flight.

A 40-foot cargo container, on the other hand, does not exist in a secure environment. Even when a container is “x-rayed” at a cargo terminal, the integrity of the contents is only ensured to be unaltered at that geographic point and time. Once the container moves out of the inspection area, it again enters a relatively insecure environment. This environment is in no way comparable to the high security environment in which airline luggage moves. Cargo Container security is different and requires different solutions. It is not economically feasible or reasonable to “x-ray” every container.

Maintaining the integrity of a container’s contents throughout the shipping cycle is imperative. Container integrity can only be assured if a reliable chain of custody is maintained and recorded.

A key component for enhanced container security will be the capacity to assign a unique identifier that can be associated to each container shipping cycle. This, in combination with a GPS/active transponder device will enable container cargo to be electronically tracked, in real time, from loading to discharge.

With a better understanding of security needs for container transportation and a better understanding of the environment in which container cargo exists, a picture of the requirements become clearer. A container “black box” that has the following attributes would greatly improve security:

1. Small, rugged and easily portable
2. Capable of assigning a unique identifier with each shipment
3. Self-contained power source
4. Able to transmit its position when interrogated (GPS) or to alert owner when certain parameters are exceeded (sensors)
5. Sensors to detect vibration or motion within certain defined parameters
6. Sensors to detect changes in heat and light
7. Automatic activation when container door is closed and immediate owner notification when door is opened

A new device, tripLOCK (developed by Aeromark, a U.K. company), comes close to meeting the above criteria. There undoubtedly will be others, but a device that can be widely utilized cannot come soon enough. This type of device will soon be commercially available, and should increase cargo transportation efficiency, and significantly enhance homeland security. Moreover, as happened with the 20- and 40- foot container, the uniform adoption by the U.S. would likely establish a world standard.

Terrorism is premised on the unexpected. It thrives on complacency. Its reach can be blunted through just a little common sense and more technology, resulting in a lot more security.

The Bay Area, as a world center of high technology, can play a major role in ensuring the security of our region’s and the nation’s ports.



# **The Private Sector and the Public Sector: Homeland Security Calls for Unprecedented Collaboration**

*by Sunne Wright McPeak, President and CEO,  
Bay Area Council*

Following September 11, Americans learned that new attacks on American soil may not necessarily be military attacks, nor on military structures; they may be against the private sector. Business assets, workers and critical infrastructure have suddenly become the frontlines of a battlefield. As it must, the private sector is rapidly responding to the new threat.

Much of the public focus regarding homeland security has been on state and local governments. The fact is that much of the Bay Area's critical infrastructure (e.g. telecommunications, banking and finance, electric power, office buildings, transportation and energy resources) is owned and operated by the private sector. As witnessed immediately following the 9/11 attacks—when the U.S. closed its airspace, borders and ports (not to mention the stock exchanges)—the economy can be devastated by a terrorist attack.

Given the new threats and ramifications of incomplete preparation, the private sector serves a critical national security role by keeping the economy moving in ways not thought of before. The Bay Area and the United States cannot have a strong economy without security.

## **The Bay Area Has Many Private Sector Vulnerabilities**

In the Bay Area and in Northern California, a coordinated attack on the PG&E electrical power infrastructure leading to a prolonged region-wide electricity outage would have devastating economic effects. When the electricity doesn't work everything else seems to fail. Information and communications, transportation, water and sewer networks all depend on electricity to function. Virtually every cash register in the Bay Area requires electricity to complete a sale. Once the emergency generators run out of diesel fuel, office buildings and factories will go dark and desktop computers will blink off.

Multiple strikes on our transportation infrastructure would also seriously disrupt the Bay Area economy. Not only would prescriptions at Long's be harder to fill, but food shelves in Safeway would soon stand empty.

Banks, like Wells Fargo and Washington Mutual, need to stay up and running to allow the flow of almost \$3 trillion in daily transactions. The entire financial services industry is based on the collective trust that consumers have in the security, confidentiality, integrity and availability of their assets. That trust must be protected.

The Internet, which has several “mission-critical” hubs in the Bay Area, is now central to America’s economic viability. Key industries, such as electricity, communications, transportation and financial networks, have all shifted control of essential processes to computers networked over the Internet. These efforts have saved cost, and made industries more efficient, but their vulnerabilities pose yet another risk to the private sector and the economy.

Clearly the private sector has much to secure. The challenge is to strike the balance between the costs of security and the impacts on economic competitiveness.

### **Security Is a Must: But Tread Carefully With Productivity**

As the newly formed Homeland Security Department takes shape, it and other governmental bodies should recognize that successful security calls for both unprecedented coordination and engagement with the private sector, and caution regarding regulation. The private sector must step up and do its part to defend against terrorism; at the same time the economy could be hurt by excessive security measures that stifle productivity.

For example, according to the December 2002 results of the Bay Area Council’s *Bay Area Poll* (an annual survey of the sentiments of Bay Area residents), over the past 12 months 22% of respondents said that they had taken fewer trips by airplane. A 22% drop in air travel business has significant economic consequences for the region and its employment outlook.

Interestingly, the *Poll* found that people’s impatience with new security at airports, long check-in lines and repeated delays in service—not fear of terrorism—was the primary reason they cited for reduced travel. Indeed, 29% of the respondents said that fears about terrorism have a “great deal” or “some” effect on their desire to travel, while 42% said longer check-in lines and 47% said take-off and arrival delays, impacted their desire to travel. As these results show, the efficient movement of people and goods is critical to economic recovery, and some security measures can be made more efficient. The private sector can help.

## **Bay Area Companies and Organizations Have Solutions Available Now**

The Bay Area, and Silicon Valley in particular, is a hotbed of innovation and entrepreneurial activity, with a proven record of turning ideas into products and applications quickly. It also is the heart of the nation's IT and biotechnology industries. This places our region in a unique position to address the security issues in our own backyard, and to contribute to technology solutions at the national level.

Many of these non-intrusive, efficient technologies are available for deployment immediately. For example, EDS, which has a large Bay Area presence, recently installed a biometric system at Ben Gurion International Airport in Tel Aviv. The system allows Israeli citizens to authenticate their identities with a magnetic card and a hand scan, cutting up to two hours off the wait at passport control. Following September 11, a wealth of Bay Area technologies migrated in awareness from the fringe to the mainstream. InVision Technologies, based in Newark, California, produces an explosives detection system used in airport lobbies in the first phase of security. Its technology, with multiple applications, is reducing reliance on the less efficient and often more costly "guards, gates and guns" approach.

The Bay Area is also home to many members of The Business Recovery Managers Association (BRMA). BRMA has advanced the theory and practice of business recovery, disaster recovery, contingency and continuity planning, and emergency response management since 1993. Members of BRMA are responsible for data center recovery planning, the recovery of business units; and some are the focal point for all contingency planning in their company. The private sector can help the public sector by sharing the accumulated knowledge of such groups.

Security has long been one of their biggest costs in the banking and financial services industry. The industry has accumulated security-related knowledge that it can share. The private sector and the public sector need to foster a regional partnership to share this learning.

Many other Bay Area companies have homeland security-related products and services with potential applications by government at the federal, state and local levels. Embracing the best of these technologies can provide an important economic stimulus to Silicon Valley while making public security more efficient, more effective and less costly.



## **Current Bay Area Security Spending Levels and Procedural Changes**

Along with New York, Washington, D.C. and Chicago, insurance companies deem the Bay Area one of the top four most likely terrorist targets in the United States. The private sector is responding to the threat. The Bay Area Council confidentially surveyed the region's business community between April 16–28, 2003 about homeland security as part of the Council's quarterly *Bay Area Business Confidence Survey*. Of the 503 respondents, more than one in eight companies, or 13 percent, confirmed that they have purchased new equipment to increase security at their company *specifically* due to the threat of terrorist attacks. Not surprisingly, spending levels correlated with company size. Approximately 30 percent of respondents from companies with more than 1,000 Bay Area employees have bought new security equipment. Only 5 percent of companies with 49 or fewer Bay Area employees reported buying new equipment.

Nearly a third (31 percent) of the CEOs and top business executives said that they have made changes to operations or procedures to increase security *specifically* due to the threat of terrorist attacks. As expected, perceived risk precipitated stronger preparation. For companies with more than 500 Bay Area employees the numbers that have made such changes doubles to about 62 percent. In the City and County of San Francisco, 50 percent of top executives report having changed operations or procedures.

How much does this new security cost? Fourteen percent of respondents said they had increased spending on security since September 11. Of those that have increased their spending, 58 percent increased it 1-10 percent, a quarter of them increased it 11-25 percent, 12 percent of them have increased spending 26-50 percent, four percent increased spending more than 51 percent.

## **Harness Market Forces To Improve Security**

While none question the importance, many companies, especially in the current economic climate, have said that they are not able to spend the money required to upgrade their systems to protect their buildings and employees. Businesses can and are acting as a defensive bulwark against terror, but government should be sensitive to two other important responsibilities of the private sector: namely, keeping the economy strong and keeping citizens employed.

Rather than mandate exactly what needs to be put in place, government can harness the dynamism of the private sector by creating standards that companies can meet by any means they devise. This process will put economic pressure on the private sector to create innovative, cost-effective solutions to getting the job done. What the private sector invents can in turn be shared with the public sector. Policy makers may also want to consider incentives to ease the financial load on businesses, such as making some security expenditures tax deductible.

Another important way the Department of Homeland Security can spur a reduction in the cost of security, plus provide an economic stimulus, is to expand its research and development (R&D) budget. President Bush has made this point repeatedly. Federal R&D funding has declined since 1992. Industry now pays for 68% of all R&D, versus the government's 27%. Research funding through the new Homeland Security Advanced Research Projects Agency and through the Department of Homeland Security's support for work at national laboratories will stimulate innovative solutions to the technological challenges posed by homeland security. The federal government should fund a strong homeland security R&D budget to complement more product-focused corporate research.

**Security and Preparedness Are Not New:  
Collaboration Will Produce Results**

While September 11 seared terrorism into the forefront of American life, terrorism is not new. Building security is not new. Disasters at industrial facilities are not new. Preparations for catastrophes are not new. The private sector, and local and state governments have jointly prepared for and responded to challenges in the past.

Given time, and if the public and private sectors work together, we can surmount the challenges of the future.

To echo Governor Tom Ridge, Secretary of Homeland Security, successful security in the Bay Area calls for:

- Innovation in security related technology and techniques
- Partnership among government, the private sector and academia in developing new public policy
- Active participation by the private sector in developing new approaches and strategies



## **Pursuing Counterterrorist Technology: Private Sector Interests and Public Policy**

*by Nicholas Imparato, PhD, Professor of Management,  
University of San Francisco, and Research Fellow, Hoover Institution,  
Stanford University*

The private sector is expected to play a major role in the country's homeland security efforts. Currently, the federal government accounts for about \$35 billion of the \$100 billion\* that constitute the national effort to protect the American homeland. Although a large share of non-federal expenditures are carried by state and local governments, the private sector, which accounts for 85% of the country's critical infrastructure, is expected to meet important challenges and responsibilities as well.

The complexity of the task is enormous. Corporations need, among other items, to protect physical assets, engage in information sharing and analysis, contribute to emergency preparedness and response, and cooperate in border and transportation security.

Additionally, the national strategy depends on products and services that are developed and sustained by profit making enterprises. These include detection equipment for explosive material, biometrics and identification devices, document authentication tools, smart camera technology, robotics, biochemical sensors and pathogen detection and filter devices, antibiotics, vaccines, and other pharmaceutical and biotechnology products, data mining and case management software, resilient communication systems and other information technology products and services, to name a few.

The ability to develop and produce innovative products that will be used in homeland defense security, in turn, depends on many factors, not least of which is the ability of businesses to understand and negotiate the public environment. A host of policy issues affect a company's assessment of how, or even whether, it should engage the federal government as a customer or partner. The first concern centers on resources and the budgets that flow from fiscal policy.

---

\* Dollar amounts cited throughout this essay reflect data reported in early 2003.

## **The Big Picture: Budgets and Counterterrorism R&D**

The federal component of overall R&D expenditures has been declining since 1992. As previously stated, the government now accounts for approximately 27% of the funding for R&D versus approximately 68% by industry.

It is hard to overestimate the importance of federally supported R&D. Most observers agree that the deterioration in government funding has not been in the national interest. Federal expenditures, for example, are the primary support for university research, which normally has a long term, basic research orientation as compared to corporate R&D which normally has a more narrow and near term, product development orientation.

The pressures working against an increase in overall federal R&D expenditures include a difficult economic environment and the political incentive to hold the line on discretionary spending. These influences are not likely to decline in the near term.

It is significant in this context, that the counterterrorism R&D budget has grown in FY 2003 to \$3 billion. The funding, an obvious consequence of 9/11, represents a threefold increase in expenditures over those in FY 2002. Programs in health and human services account for nearly 50% of the budget. National security programs (Department of Defense, DARPA) account for about 25%.

The Department of Homeland Security (DHS) has an estimated funding of \$800 million for R&D. Nearly \$300 million represents transfers from other departments (for example, aviation security, formerly of the Department of Transportation). The budget maintains that “there is \$350 million new funding for vigorous research development, test and evaluation capabilities” for “specific projects, such as nuclear and bioterrorism detection technologies.” The Homeland Security Advanced Research Projects Agency (HSARPA), the Homeland Institute, the University Center for Homeland Security and other components of the newly created department will require supplemental funding. Multiple centers within the department are designated for research, testing and evaluation and a leadership position has been created to work with the private sector to spur innovation in homeland security technologies.

Appropriations and authorization for homeland defense and counterterrorism R&D are a responsibility that is scattered across multiple congressional committees and subcommittees (about 80% of the DHS budget is currently the purview of 19 committees in the House and Senate). The House of Representatives has, however, recently established a Select Committee for Homeland Security. Although no corresponding committee has been established in the Senate, the oversight function has been assigned to its Governmental Affairs committee.

Because there is no one committee in charge, the budget process for homeland security R&D is awkward and complicated. There have been frequent recommendations to alter the arrangement but a combination of institutional and personal motivations delays change. No agreement has been reached yet regarding how to conduct the oversight of DHS' research and development activities.

In any case, it is generally agreed that the procurement process needs to be streamlined. Individual agencies, including DARPA, already have reported that the timeline for attractive proposals to move to funding has been compressed substantially. Several congressmen have used debates on tax legislation to simplify the procurement process and intend to continue that effort.

### **Broader Private Sector Concerns**

The complexity, ambiguity and amorphous nature of the organizational structure within the federal government, as well as the process of working out the post-merger hurdles that face the DHS, will make the task of securing and conducting federally supported R&D projects a challenging one.

As indicated in the Administration's national strategy, the agencies involved with funding and authorization "have little frontline knowledge of homeland security and little or no experience in technology acquisition and supporting research." The fragmentation of research across multiple agencies and departments means that potential competition for funding can delay progress. Moreover, as the science and counterterrorism committee of the National Academy of Sciences observed, the nature of certain initiatives, notably the development of sensor systems, requires the integration of expertise from multiple disciplines and involves any number of agencies with relationships with numerous universities and research centers. How the government sets priorities and provides coordination of the research effort in this setting is still not clear, particularly as it attempts to avoid the problems of "artificial research boundaries," redundant research efforts and overlapping or disjointed data regarding the funding of specific technologies.

The development of codes and standards, driven in part by the acknowledged need for interoperability and related matters, requires the exchange of information among industry participants. Although some legislation has materialized to provide anti-trust exemptions, the issue is still a concern and will continue to get attention.

Intellectual property issues are also significant when firms might be required to share data with competitors and others as part of participation in funded projects. To the degree that the national effort can benefit from a cooperative and open exchange among firms and research organizations, the desire is to strike a balance between the private need to protect proprietary information and the public need to create an environment safe for sharing information.

Indemnification against risks associated with product development, testing and evaluation is an important consideration. Liability protection (including suits from shareholders) for a product's ineffective performance or faulty installation is also being promoted. A separate but related set of issues relates to the standards for a firm's access to critical information, its ability to get security clearances and other elements surrounding risk mitigation.

One point of clarity is that the emphasis on dual use technologies is likely to rise. At the minimum, the likelihood that a product or service can be sustained without government support is attractive in times of economic uncertainty. Examples include the use of video technology, such as advanced video processors, as components of both access control and surveillance systems and broadband entertainment products. The use of data mining and relationship search software has utility in identifying critical associations (for warnings and threat analysis) as well as in a host of business situations (customer relationship management, market research). The tools used for cybersecurity have applicability for both counterterrorist and commercial purposes, as witnessed by the rising concern for online authentication and authorization procedures.

The most dramatic policy area, dealing with the impact of counterterrorist technology on privacy and other civil liberties, will be a continuing source of controversy and debate. Obviously, it is necessary for corporate strategy to reflect society's interest in pursuing security without sacrificing traditional rights and privileges.

## **Private-Public Partnerships**

A number of private-public collaborations have been credited with giving rise to valuable pre-competitive innovations. These include, for example, SEMATECH and the Small Business Research Program. Similarly, special projects and initiatives that have involved government and corporate cooperation have proven successful in the past (for example, the Y2K project). The Smart Security and Tradelanes Initiative, which is currently testing a range of technologies aimed at cargo container security, now involves more than 30 companies, as well as port authorities and other public organizations.

Yet, the challenge still remains as to what kind of private-public partnerships can best be mobilized. There are different philosophies about how to deal with the tension between making a profit and serving the public good. In addition, common perspectives need to develop about how to ensure accountability and set priorities. Different models for financial management (for example, disclosure rules) need to develop as well.

Certain suggestions are gathering consensus. These include recommendations about funding schedules that not only tie to project milestones but that can also be insulated from the normal uncertainties that mark the annual budget cycle. Methods of bolstering public support for a project are recognized as a more serious endeavor now than before. Effective feedback systems for all parties, derived from agreed upon business plans, are compelled by the necessity to build trust and diminish the often contentious relationship that exists between the private sector and government officials.

Summing up, business must consider a host of non-market issues and circumstances in order to contribute to developing and distributing efficacious counterterrorism technology. Coming to grips with the pertinent public policy concerns and various forms of working arrangements is now an integral part of business strategy. The security of the American homeland depends on meeting the challenge successfully.





# Positioning Security Technologies for the Future

*by Robert J. T. Morris, PhD, Chairman, BASIC, and Director of the IBM Almaden Research Center*

The Bay Area is a focal point for creativity in technologies and business models, and boasts a long history of innovation. Today we are faced with the urgent challenge of protecting our region and the industry that we helped create. We also have the opportunity to develop and deliver technologies to the world that will enhance national and international security.

Capitalizing on the Bay Area's deep pool of innovation, we are well-positioned to accomplish this. However, in today's economy, new models and technologies must not only improve security and make it more effective, but also must provide a return on investment. Enterprises must be given new solutions which leverage limited resources, such as funding, IT capacity and IT skills.

One of the best ways to do this is to push system complexity into the background, so that security becomes a more natural, reliable part of the system, like robustness and performance.

There are two major trends that are emerging in IT that are aligned with these needs: they are *autonomic computing* and *on demand computing*.

Autonomic computing systems are self-configuring, self-protecting and self-healing. Such systems deal automatically with problems—before and after they arise—while dramatically improving the performance and security posture at the same time.

On demand systems are responsive, flexible and virtual. Their costs shift from fixed toward variable. They use technologies from grid computing and autonomic computing to create a more efficient operating environment, which also leads to greater responsiveness and resilience of the enterprise. On demand systems also lead to increased organizational productivity through process transformation. They directly enable security because they allow inter-enterprise collaboration and sharing, and create a broad and stable resource base that can be directly engineered to meet security concerns.

Finally, there is an opportunity where the Bay Area can take a leadership position and distinguish our solutions: this is through *privacy technology*.

## **Autonomic computing**

Autonomic computing is a fundamental change which seeks to make systems more self-managing from configuration, security and capacity standpoints. This is necessary, in part, because the increasing complexity of systems is outpacing the human resources available to manage them. There is already a drastic shortage of IT-skilled personnel and IT security personnel, and this deficit will only accelerate. In addition to the very obvious ways the Bay Area universities are expanding the numbers and skills of IT people, we also need to find ways to make the security of our systems more effective by better leveraging those scarce human resources. Autonomic computing is also part of a broader system management effort to shift from component and system security to holistic security.

Security, in the autonomic sense, is more than perimeter security, because with cross-entity transactions and collaboration, perimeters can exist on many levels. Instead, security must be multi-layered with protection at many points. Access and authentication controls are also key elements.

Security must exist on an end-to-end basis. This is important whether one is talking about internal collaboration or process transformation; transactions that cross organizational boundaries (companies, suppliers, customers, business partners); or interactions with individuals in many capacities (consumers, citizens, employees). End-to-end transactions require interoperable standards. Often such solutions are built on web-enabled platforms for this reason. By definition then, end-to-end *security* also demands interoperability. Such security needs to support integration, virtualization, flexibility, and scalability (high transaction rates) on multiple vendor platforms. Many Bay Area companies and universities are involved in the underlying elements needed to support such interoperability, such as XML (extensible markup language) and SAML (secure access markup language).

Security at this level also encompasses more than vulnerability remediation and “patch management.” Experience has also taught us that we need to move in the direction of autonomic computing because we cannot assume that patches, which address known vulnerabilities, will necessarily be applied. Vulnerabilities not known to the vendors may also exist.

While vulnerability remediation, patch management, and traditional perimeter approaches to security still have value and are in wide use, security is quickly evolving beyond those approaches. Today, Bay Area vendors of security products are offering real-time analysis of comprehensive security incident data from hundreds of thousands of sources worldwide to give early warnings of trouble.

Real time analysis is a vital step, but the greater challenge is to move rapidly to realtime-responsive computing that is self-immunizing and self-healing. We don't have the time to take a threat, analyze it and eventually respond several days, or even weeks, later. We must be able to guard against the bad actions that a program seeks to take, not because we have already identified it as a virus or a worm, but because the action it seeks to implement could potentially do harm. In this case, such a proposed action would be further examined before it was permitted to occur.

Such approaches can also be extended beyond systems to networks. Through the Cybershield project organized by SRI International and others, we can seek to become aware, on a realtime basis, of harmful actions or the potential for harmful actions in these networks, and take appropriate countermeasures.

Many vendors with presence in the Bay Area such as Cenus Technologies, IBM, Symantec, Network Associates, Hewlett Packard, Intel, Sun, Computer Associates, and many others are already implementing these emerging autonomic, self-managing computing functions into their offerings.

The secure, cross-organizational, transactional, end-to-end, self-managing, scalable, interoperable, and multi-vendor platform aspects of autonomic computing solutions present many technical challenges that are beyond the scope of any one vendor or university to address. Recognizing this, in 2002, the IBM Almaden Institute hosted the first large-scale conference on autonomic computing. This conference brought together nearly 150 scientists from entities such as HP, IBM, Microsoft, Sun, DARPA, NASA Ames, UC Berkeley, Columbia, and Cornell to discuss this subject and further their collaborative efforts.

As one example of an on-going research effort in the Bay Area, UC Berkeley and Stanford have a joint project focused on Recovery-Oriented Computing (ROC). This project is complementary to autonomic computing, whose ultimate objective is fault (or incident) avoidance. Taking a different approach, the ROC project assumes that it will not always be possible to avoid all incidents, and so seeks to identify those elements of computing that can improve recovery from failures.

## **On demand computing**

On demand computing can help entities become more secure, more compliant, and, simultaneously, better able to manage privacy.

We have the ability to position entities to share computing resources, such as processing power or storage, through such concepts as grid computing and on demand computing. Today, a good deal of computing power or storage that exists in an entity's information technology systems may be underutilized. Grid computing enables such capacity to be shared. Grid computing also supports computationally-intense projects, such as ligand matching for potential vaccines.

Putting in place shared resources, such as secure storage area networks, is of interest to the Bay Area's many storage vendors, such as Hitachi, Hewlett Packard, IBM, Veritas, and others. In fact, the Storage Network Industry Association is one of many entities focused on this cooperative effort.

Universities have been leaders in sharing computing capacity, and are continuing to expand that presence. NASA's Ames Research facility is participating in a national grid project called the Information Power Grid (IPG). This project enables major NASA facilities to share computational and storage capabilities among real users on a seamless basis. NASA IPG and many well-recognized Bay Area companies are members of the Global Grid Forum which seeks to expand development and implementation of grid technologies.

On demand computing goes the next step, and enables an entity to call up computational resources or applications as needed. This is both more economical as well as more flexible. Furthermore, it enables an entity to more rapidly integrate and collaborate across its own units as well as across other entities. It also speeds the transformation process. Both centralized and distributed systems can be used to provide on demand computing, elements of which are offered today by many Northern California vendors.

## **The Importance of Privacy**

The creation of unprecedented amounts of digital content is being enabled by the technological innovations in computing capacity, storage and connectivity. Experts estimate that the amount of global data is doubling every twenty months. This creates an opportunity for increased factual data analysis as well as data protection technologies. Nowhere do these two issues intersect more than in the area of security.

The current heightened interest in security provides an attractive opportunity to enhance privacy while strengthening security at the same time. Unfortunately, the perception is that there must be a significant tradeoff between privacy and security. But this perception is fallacious. Current technology allows us to dramatically improve both the privacy and security of information. While neither comes without financial cost, both can also create competitive advantage, and position an organization for transformation, productivity gains, and risk mitigation.

The 2003 Almaden Institute focused on privacy in data systems. The conference challenged over 100 attendees from government, academia and industry to address the questions: Which data should we collect? Who can access the information? What can be done with it? And what technology can we use to enforce these rules?

Many industry leaders in privacy-enhancing technologies are active in the Bay Area. For example, one company is enabling raw data to be rendered anonymous through randomization, yet still be factually analyzed to discern patterns. Other technologies in the Bay Area enable operations to be performed on sensitive data in secure processors, and only non-sensitive outcomes or feedback are then made available to the authorized parties.

In addition, we are doing research in compelling areas such as privacy architectures, handling privacy across domains and entities, and creation and enforcement of organizational privacy policies and individual privacy choices. All of this work will support the privacy and security needs of the future.

The Bay Area has been a driving force for much of the public debate on privacy and information protection. California breach disclosure legislation, which became effective on July 1, 2003, not only highlights the issue of protecting sensitive personal information, but it is also spurring further development and offerings of privacy-enhancing technologies by Bay Area vendors. For example, improved authentication, authorization and access controls are emerging as cost-effective ways to determine who can access the data and to limit what can be done with it. Better audit safeguards can also help demonstrate compliance with corporate privacy policies.

## **Conclusion**

Vendors, universities and customers in the Bay Area are already embracing and implementing self-managing, on demand and privacy-enhancing solutions. However, significant technological challenges remain, which the Northern California research and vendor community is well positioned to address. The Bay Area has a wide spectrum of skills and resources to overcome these challenges. Our broad collaboration and individual competition can enable the deployment of secure, flexible, self-managing, and on demand computing with advanced privacy capabilities. The availability of such capabilities will enable companies across the U.S. to enhance their security, ensure the confidentiality of their customers' data, and continue to be at the forefront of international competition.

# **The Political Economy of Protection: Appreciating the Political and Economic Aspects of Investments in Homeland Security**

*by Jay Stowsky, PhD, Executive Director, UC Berkeley Project on  
Information Technology and Homeland Security  
(based at the Goldman School of Public Policy)*

In these first years of the 21st century, Americans are both privileged and cursed to be living through two epic transformations. The first transformation is the much discussed shift to a “new economy,” digital, flexible, and networked, a seemingly inexhaustible engine of increased productivity. The second is the transformation of the security challenge facing the United States and the world: the shocking emergence of so-called “asymmetric” threats, characterized by weak adversaries able to sucker-punch the strongest nation in the history of the world by identifying otherwise unguarded points of vulnerability and striking whenever opportunity allows.

In the technological arena, the key source of these transformations and, ultimately, the essential link between them, is *the revolution in information technology*. The same spectacular array of new digital communications and information processing tools that powered the United States’ economic and military resurgence at the end of the 20th century paradoxically makes Americans more vulnerable, whether abroad or at home, at the start of the 21st.

America’s economy and domestic security operations are both newly strengthened and newly imperiled by the global digital networks that run them both:

- Commercially available information technologies useful for securing the homeland are also accessible tools for terrorists.
- Technologies that might create significant side benefits in terms of economic growth, government services, public safety and public health may be newly subject to strict export and publication controls or outright classification.
- Digital surveillance technologies that may enable quicker detection of terrorist plots may also enable unprecedented invasions of individual privacy and other serious encroachments on the civil liberties of innocent citizens.



Public officials and industry leaders need to grapple with the complex issue of such risks and their implications for the use of digital technologies to protect and defend the country's critical infrastructures. These infrastructures include everything from the air traffic and flood control systems to ports to power plants, from the digital networks that operate and regulate the nation's financial markets to the physical transportation and telecommunications networks themselves. To some degree these infrastructures are all at risk of malicious physical and cyber attack; but they are not equally at risk nor would their disruption cause equal damage to public health or safety or the economy.

The terrorist threat to such infrastructures via a combined physical and cyber attack has been likened by some to an electronic Pearl Harbor, but it is likely more subtle and insidious than that. This threat cannot be overcome solely by a massive technology fix, though IT will be a major part of the solution in the form of improved capacities for data sharing, "smart" ID cards and visas with biometric identifiers, new types of sensors and nanotechnology for detecting the presence of chemical, biological, or radiological agents, and various forms of digital surveillance as mentioned earlier.

Economic incentives, psychological motives and political interests must be taken into consideration also as both public and private sector officials decide what needs protection, what type of protection, and how much.

A number of difficult questions must be confronted and addressed:

- **Risk Assessment and Mitigation**  
What is the nature of the terrorist threat to digital network security? How do we assess the risks and consequences for different types of critical infrastructures? When is government protection warranted (and what kind?) and when can market mechanisms be employed (e.g., discounted rates on terrorism insurance for owners of such infrastructures) to encourage the private sector to mitigate the risks? These questions must be addressed from the standpoint of economics, computer science, social psychology, and political science.
- **Economic Incentives and Cyber Security in the Private Sector**  
Even when there are technical solutions available, are privately owned networks remaining unprotected due to the presence of perverse economic incentives? For instance, the person in charge of cyber-security for a corporation may be insufficiently vigilant, merely because the actual costs of system failure fall on someone else. In addition, information security mechanisms are now being used for competitive advantage, to segment markets, to differentiate products, to protect monopolies. The economic nature of the cyber-security problem, including such concepts as externalities, adverse selection, asymmetric information and moral hazard, must be appreciated and addressed if technical solutions are to be implemented.

- Digital Supply Chain Management, Network Centric Warfare and Emergency Response**

The notion of “network centric warfare,” an element of the so-called “revolution in military affairs” in the battle strategies of the armed forces of the United States, is a conscious attempt by U.S. military planners to learn from successful retailers such as Wal-Mart and Dell Computer that have applied information technology to create flexible, non-hierarchical organizations and just-in-time supplier networks. How do these retail supply chain networks actually work? What are their strengths and weaknesses? How has the introduction of network-centric battle strategies worked, for example, in the recent conflicts in Afghanistan and Iraq? How do the military and commercial sectors differ as users of IT technology? What are the implications of such differences for user-driven technological innovation? What are the opportunities and the impediments to applying these techno-organizational models to the task of homeland defense, particularly for federal, state and local agencies charged with detection, prevention and emergency response?
- Dual-Use Technology Development, Diffusion and Innovation**

The military’s sponsorship of new technology that has both military and civilian applications has always carried with it the risk that military sponsors will steer the technology’s development trajectory in a direction that will undermine or destroy the technology’s commercial appeal. Are new homeland security technology policies building on lessons from recent Pentagon-sponsored dual-use development programs? Now that many of the most useful technologies for fighting terrorism are also useful for helping groups to wage it, can the U.S. military continue to involve research universities and commercial producers (some of them foreign-based) in the development of critical dual-use technologies for military use? Will efforts to deny terrorist adversaries ready access to those technologies impede the free flow of scientific and technical information that is so essential to innovation and successful commercialization? What are the implications of new security-based restrictions on research, exports and the flow of information for the academic-industry-government research partnerships that have become a major vehicle for technological and economic development in the United States since the 1980s?

- **Surveillance, Privacy, Civil Liberties and Security**  
Digital information technologies make possible pervasive and barely visible forms of surveillance that violate standard notions of individual privacy. Different countries have different rules about balancing privacy and security. What are the implications of these different privacy rules for the structure and operation of global digital networks and their use by military and law enforcement agencies? What are the relationships between current regimes of intellectual property protection (e.g., of databases) and the needs of the national security apparatuses? What about other legal regimes that regulate the use of information? In the U.S., for example, in order to ensure the accused a fair trial, local police cannot share with national security agencies some of the information generated in the course of a criminal investigation. Are there lessons to be drawn by U.S. law enforcement agencies from the ways that authoritarian regimes (e.g., China, Cuba) have attempted to regulate the Internet and other digital information infrastructures as part of their efforts to manage what those regimes define as internal security threats? What are the potential implications for civil liberties in the U.S.?

Terrorist attacks, as spectacularly devastating as they can be, are each likely to affect directly only one or a few population centers at a time. The psychological and economic impact on the rest of the population, however, will be great. Unlike Cold War-era nuclear deterrence—mutual assured destruction—it is not possible to protect everyone at once, nor is everyone equally at risk. Terrorists might never hit those facilities and population centers judged to be most at risk.

Thus the high costs of investment in technological systems for domestic security can become politically precarious, as local taxpayers and their representatives begin to ask who and what is being protected, who and what is not, and why. Policy makers need to understand that the most straightforward way to justify the costs of such technology investments politically is to sponsor the development of military/security technologies that can also produce demonstrable social or economic benefits.

Those benefits must be weighed, however, against the new risks the technologies may introduce, risks to individual privacy and civil liberties, the very features that make our system so maddening to our adversaries and so precious to us.

## **SECTION II**

# **BAY AREA TECHNOLOGICAL CAPABILITIES TO ADDRESS THE CHALLENGES OF HOMELAND SECURITY**



## INTRODUCTION

The research and development of effective technologies for homeland security is a national priority of major importance. As stated in the executive summary of the Administration's *National Strategy for Homeland Security*, "The Nation's advantage in science and technology is a key to securing the homeland...Just as science has helped us defeat past enemies overseas, so too will it help us defeat the efforts of terrorists to attack our homeland and disrupt our way of life."

The Bay Area is a national leader in homeland security. This leadership position is based on a research and development capacity and infrastructure that may be unparalleled in its strength and diversity:

- Five leading research universities
- Five national research laboratories
- Four international independent research centers
- National leadership in information technology, bioscience, electronics, communications, nanotechnology and homeland security technologies

Completing the circle of key elements in the Bay Area's technological strength is the nation's largest concentration of venture capital and the nation's largest entrepreneurial community. The close proximity of venture capital to industry enables the Bay Area to rapidly move new technologies from the laboratory to production. With homeland security a high priority and fast deployment critical, the Bay Area's proven ability to deploy new technologies quickly is another major factor in its leadership position.

Therefore, the strength of the Bay Area as a center for research and innovation comes not from any single piece of its research and development infrastructure, but from the combination and interaction of these diverse elements in a uniquely creative and entrepreneurial environment.

Prior to September 11, public and private Bay Area laboratories were already focused on many of the challenges now identified under the umbrella of homeland security. Since September 11 these efforts have accelerated, with many technologies developed by national and industry laboratories already deployed or in advanced stages of development.

This section of the report presents important technologies from thirty-eight of the region's numerous large and small research companies and laboratories—technologies that are directly related to the six specific mission areas identified by President Bush in his proposal to establish the national homeland security research program:

- Intelligence and Warning
- Border and Transportation Security
- Domestic Counterterrorism
- Protecting Critical Infrastructure
- Defending Against Catastrophic Terrorism
- Emergency Preparedness and Response

It is well recognized that research laboratories in the Bay Area, the State of California and across the country are only at the beginning of what must be a greatly expanded, long-term commitment to protecting the nation.

The Bay Area, with its scientific capabilities and technological expertise, is committed to assisting the nation to achieve its critical objective of providing a secure homeland for its people and to fighting terrorism worldwide.

# Examples of Bay Area Technological Capabilities Related to the Critical Mission Areas of Homeland Security

## INTELLIGENCE AND WARNING

*“We must have an intelligence and warning system that can detect terrorist activity before it manifests itself in an attack so that proper preemptive, preventive, and protective action can be taken.”*

*—National Strategy for Homeland Security*

- **Biometrics:** IBM has nearly 50 scientists dedicated to biometrics research, including speech technologies and voice and fingerprint recognition. **(IBM)**
- **Computer Vision:** piXlogic software automatically scans the contents of a digital image and “sees” the visual objects it contains. This technology can be used to visually search repository of pictures and videos. It can also be used to monitor live video feeds to trigger an event when an object of interest comes into the field of view. The software can also recognize text in a picture/video. **(piXlogic)**
- **Corporate Immune Systems:** HP Labs is applying biologically inspired models to the development of cyber attack detection and response mechanisms. Scanning techniques developed as part of Corporate Immune System research project provide early detection and warning for a variety of cyber attacks. **(Hewlett-Packard)**
- **Data Collaboration and Analysis:** Melior Technologies Extreme Networking (XN) platform allows intelligence agencies to work together by providing a framework that allows the integration of any application, data or device across or beyond their networks, while also providing a distributed computational engine for data analysis, all within a self-managing, self-healing environment that ensures data security while significantly reducing development costs and administrative overhead. **(Melior Technologies)**
- **Data Protection/Collaboration:** Oracle’s solutions for connected and disconnected wireless access, decision support and multi-channel interaction centers help the public sector coordinate, collaborate and communicate across government agencies and with its constituents. **(Oracle)**



## Intelligence and Warning (continued)

- ***Data Representation for Rapid Insight:*** SGI's Visual Simulation Lab develops visualization and human-machine interface technologies to rapidly overcome information overload concepts. **(Silicon Graphics Inc.)**
- ***Information Search and Discovery:*** Inxight's search and information discovery solutions quickly combs through huge amounts of information, analyzes and organizes it to help narrow the search, and delivers specific information supporting government/intelligence processes. Using Inxight solutions, analysts and law enforcement officers could quickly spot early warnings of terrorist or criminal activity, such as previously unknown people associating with known terrorists or known terrorist organizations. **(Inxight)**
- ***Information Technology:*** Computer scientists at Berkeley Lab are developing: (1) Information processing and retrieval technology for detecting and identifying terrorists from text-based and network-based databases; (2) Computational and informatics techniques for model recovery from observed images and video streams. **(E. O. Lawrence Berkeley National Laboratory)**
- ***Intelligence Analysis:*** Lawrence Livermore's International Assessments Program is among the strongest in the nation for analysis and research related to foreign weapons of mass destruction, including early stage foreign technology development and acquisition, patterns of cooperation and foreign cyber threats. **(Lawrence Livermore National Laboratory)**
- ***Intelligence and Warning:*** The Zero Latency Enterprise (ZLE) architecture, based on the Hewlett-Packard NonStop computing platform integrates data from disparate databases, analyzes it in real time, and applies predetermined rules to enable an immediate and appropriate response. ZLE has the ability to recognize patterns in data residing in existing legacy systems in real time, so that threats can be responded to as they are evolving. **(Hewlett-Packard)**
- ***Intelligence and Warning:*** Integration of multiple real-time data and analysis channels (e.g. from hyperspectral imaging, remote sensing, biomolecular sensors, medical facilities, etc.) using an interactive web-based platform (Bio-Act) with advanced data mining, pattern recognition, and contextual search and retrieval software to detect threats and provide customized meaningful visualizations and early warnings across agency jurisdictions. **(NASA Ames Research Center in partnership with California Menay Institute)**

## Intelligence and Warning (continued)

- ***Intelligence and Warning:*** SRI has developed technologies for computer network intrusion detection; threat assessment and information sharing; collaborative intelligence analysis; and image and text analysis for intelligence extraction. SRI's discoveries in sensors and sensor systems for detection of chemical and biological agents have been applied to micro-detectors, laboratory-quality instrumentation systems, remote optical and chemical identification systems, and portable and mobile devices. **(SRI International)**
- ***Internet Resource/User Access:*** Cenus Technologies' globally scalable Layer 7 networking technology enables the compilation, for analysis, of usage and access data of Internet, World Wide Web, and WAN/LAN based resources and traffic, by individual users, user populations, and by files accessed. This enables the mining of such data to discern patterns of resource usage and communications, and enables identification of users to exacting and discreet levels of locality, and paths of access. **(Cenus Technologies)**
- ***Mission Critical Communication Platform:*** Aspect's technology provides ability to link government and private sector data; monitor and track information and people to identify potential threats; and proactively sends alerts and notifications to appropriate individuals via any communication channel. **(Aspect)**
- ***Night Vision:*** Intevac's intensified digital video sensors for high performance camera applications offer high sensitivity and high resolution in both the visible and near infrared range of the electromagnetic spectrum. These sensors and cameras provide important military and commercial applications for detecting or imaging objects using infrared radiation, including low light level surveillance to nighttime long-range target detection and identification. **(Intevac)**
- ***Nuclear Threat Assessment:*** Lawrence Livermore's Nuclear Assessment Program is the DOE/NNSA lead for technical, operational, and behavioral assessments of nuclear and radiological threats. This program also provides technical support to the law enforcement and intelligence communities, including real-time assessments of nuclear black market transactions, field support for seizures of illicit nuclear materials, participation in FBI-designated special events, and instruction related to nuclear crime at various national and international law enforcement training venues. **(Lawrence Livermore National Laboratory)**

## Intelligence and Warning (continued)

- ***Pattern and Trend Discovery:*** IBM has several projects among its eight worldwide research labs for the comprehensive intelligent mining of unstructured, semi-structured and structured digital data. **(IBM)**
- ***Privacy Preserving Identity Management and Computation:*** The Trusted Systems Lab of HP Labs develops technologies that balance the need for strong identification and authentication with the privacy concerns of individuals. Research is ongoing in the areas of Identity Based Encryption, Personal Trust Assistants and cryptographic techniques for privacy preserving computation. **(Hewlett-Packard)**
- ***Rich Media Content Extraction:*** HP Labs is conducting research that will allow easy access, navigation, and organization of vast repositories of multimedia (audio, images, video) content. Ongoing projects address the following key research problems: multimedia annotation using automatic content analysis techniques (automatic metadata generation); semantic metadata representation, storage, and indexing for efficient information retrieval and browsing; system design for processing, indexing, and retrieval of vast repositories of rich media content. **(Hewlett-Packard)**
- ***Specialized Sensors:*** Eoplex's technology, High Volume Print Forming (HVPF™) used in producing complex 3-D components and circuits contributes to homeland security in the form of specialized sensors and unique hybrid circuits for detection applications. **(Eoplex)**
- ***Systems Security:*** IBM Research's Global Security Analysis Lab creates tools and services for system security needs, including intrusion detection, vulnerability testing, intrusion avoidance, wireless security, and advanced cryptography. **(IBM)**
- ***Systems Security:*** Visuale's Process Fusion Software platform allows for comprehensive threat modeling, data integration and analysis, without the expensive and time-consuming aspects of application development and deployment. Visuale also offers a comprehensive security model for access control, escalation and an event notification processes. **(Visuale)**

## Intelligence and Warning (continued)

- ***Threat Assessment:*** ArcSight's enterprise software utilizes sophisticated real time correlation technology enabling large, geographically-dispersed organizations to better manage their security function by consolidating and analyzing diverse sources of security-relevant information to identify and react to true threats and attacks. **(ArcSight, Inc.)**
- ***Threat Assessment:*** NASA Ames Research Center has extensive experience and a diverse range of world-class researchers in critical information technologies for the detection of threats. Expertise includes data mining and analysis, information sharing, collaborative systems, human factors, high-performance computing and information fusion. Ames has expertise in the development of integrated systems to deploy advanced technologies, including work with the FAA and NASA space missions. Ames is working with the Transportation Security Agency to apply these technologies to the problem of passenger threat assessment. **(NASA Ames Research Center)**
- ***Threat Assessment:*** Enterprise software utilizes the latest hacking techniques and signatures to assess the susceptibility of an organization's Web site to attack and report out to management and security teams on recommended fixes. **(Sanctum)**
- ***Verified Information Sharing:*** VeriSign offers a range of solutions to authenticated users—intelligence community, law enforcement and first responders—establishing trust and verifying the level of access users have to certain information. **(VeriSign)**
- ***Video Intelligence and Automated Monitoring:*** IntelliVision's technology analyzes video in real-time and automatically identifies inconsistencies and abnormalities in environment, human behavior and movements of people, vehicles and objects. Automatically detects security threats and breaches and alerts security professionals in timely manner. Vastly enhances reliability of CCTV, access control, intrusion detection, perimeter monitoring, asset protection, and other security systems. **(IntelliVision)**
- ***Video Surveillance:*** NEC's system, SmartCatch, is real time video intelligence software that detects, tracks and identifies active and static objects within video streams. It offers real time behavior recognition and analysis, anomaly detection, and automatic alarm verification—all deployable within existing CCTV systems. **(NEC)**

## Intelligence and Warning (continued)

- ***Visual Data Collection and Analysis:*** iPIX's Rimfire® imaging platform enables collecting, processing, and analyzing photos captured by field personnel and surveillance cameras. Millions of images are handled daily by this robust distributed infrastructure. **(iPIX)**
- ***Visual Surveillance:*** iPIX's 360-degree-by-360-degree video camera solutions provide complete, live and archived visual coverage in real time, using only one camera head with no moving parts and in a package that can be configured to provide situational awareness and tele-operation on unmanned vehicles, robots, and ground sensors in any environment. **(iPIX)**
- ***Wireless Sensor Networks:*** Research at the Palo Alto Research Center (PARC) is aimed at developing scalable, generic algorithms and software systems for analyzing data from distributed sensor networks. In a current project, co-funded by Defense Advanced Research Projects Agency (DARPA), PARC scientists are developing an experimental Smart Sensor system for tracking targets on a battlefield. **(Palo Alto Research Center)**

## **BORDER AND TRANSPORTATION SECURITY**

*“We must...promote the efficient and reliable flow of people, goods, and services across borders, while preventing terrorists from using transportation conveyances or systems to deliver implements of destruction.”*

*—National Strategy for Homeland Security)*

- ***Border and Seaport Security:*** ARACOR’s Eagle system, a powerful, mobile, relocatable cargo inspection system provides a combination of cargo x-ray inspection capabilities for seaports, border crossings, and facility entry points to detect explosives, weapons, drugs, and, potentially, special nuclear materials. U.S. Customs Service gave the Eagle its highest rating based on x-ray inspection capabilities and selected it as the primary security system for U.S. seaports. **(ARACOR)**
- ***Border, Container and Seaport Security:*** RAE Systems has developed hazardous gas and radiation sensors to be deployed in intermodal shipping containers, giving customs and port officials pervasive sensing abilities to identify and interdict suspect shipments. Its handheld radiation sensors provide on-the-spot detection of illicit radiation in shipping containers, automobiles, on persons or in luggage, enabling customs and border patrols to assess and deter entry of radiological contraband. **(RAE Systems)**
- ***Border and Transportation Security:*** Ancore has major R&D and D&E programs to develop and test non-intrusive neutron based techniques for the detection of a wide range of threats (explosives, chemical agents, nuclear materials and devices, radiological weapons, drugs, etc.) in all modes of transportation: fully loaded trucks crossing borders, marine cargo containers at seaports of entry, other vehicles, air cargo, air passenger luggage, etc. **(Ancore Corp.)**
- ***Border and Transportation Security:*** Quantum Magnetics, a wholly-owned subsidiary of InVision Technologies, specializes in developing aviation security products such as the i-Portal (imaging weapons detector) and LiquiScan (sealed bottles) in addition to quadrupole resonance (QR) technology-based Qscan (luggage and smaller parcels), wand (persons) and portal (persons). **(InVision Technologies and Quantum Magnetics)**
- ***Border and Transportation Security:*** Research on system for container tracking for port security. **(NASA Ames Research Center in partnership with California Menay Institute)**

## Border and Transportation Security (continued)

- ***Border and Transportation Security:*** Recognition Systems' biometric verifications systems use the size and shape of a person's hand to help speed them through border crossings. This technology is already at work at Israel's Ben Gurion International Airport with millions of inspections already completed. **(Recognition Systems, Inc.)**
- ***Border and Transportation Security:*** SRI, a leader in natural language speech recognition, has licensed its spoken language recognition system to a commercial firm that has deployed it into a translation device in use in Afghanistan. **(SRI International)**
- ***Border and Transportation Security/Nuclear Detection:*** Advanced radiation detection technology and analysis techniques for application to transportation and border security. **(E. O. Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, Sandia National Laboratories)**
- ***Border Security/Visual Surveillance and Documentation:*** iPIX's highly compatible fixed spherical platforms allow live and/or archived capture of 360-degree-by-360-degree as well as 360-degree-by-180-degree views of any area, allowing for single camera surveillance at border crossings, cockpits, and security checkpoints. **(iPIX)**
- ***Border Surveillance:*** Research on the use of high-definition video technology developed for the entertainment industry has broad application for border surveillance. **(Silicon Graphics Inc. and AliasWavefront)**
- ***Border Surveillance and Aviation Security:*** InVision Technologies has developed one of only two FAA-certified explosives detection systems (EDS) deployed by the federal government in 90% of the airports nationwide. Its detection system is based on computed tomography technology, which has proven effective in detecting explosives determined by the Federal Aviation Administration (FAA) to be a significant threat to commercial aviation. **(InVision Technologies)**
- ***Border Surveillance and Aviation Security:*** SRI is working in several areas, including identity verification; person and asset identification and tracking; aircraft protection, including fuselage ballistic armor and explosion-containing luggage containers; silent micro-air vehicles; and electronic no-fly zones. SRI's expertise in electromagnetics has resulted in penetrating radar systems; reliable wireless systems; precision navigation; and autonomous command and control systems. **(SRI International)**

## Border and Transportation Security (continued)

- ***Cargo Container Evaluation and Experimental Facility:*** Lawrence Livermore provides unbiased testing of commercially available and prototype technologies for detecting nuclear materials inside cargo containers. Active and passive detection technologies are being tested against real nuclear materials inside real cargo containers filled with goods typical of air, sea, and truck cargo. **(Lawrence Livermore National Laboratory)**
- ***Cargo Container Tracking System:*** ContainerTrac has developed a Port Automated Tracking Service (PATs), a container tracking service which enables marine terminal operators to track in real-time, with 100% accuracy, the exact location of every container in port. This automated system replaces the manual process of identifying and retrieving containers, and enables U.S. Customs to immediately retrieve containers for inspection. **(ContainerTrac)**
- ***Commercial Airport Facilities Security:*** Research and development of biometric verification systems that protect the nation's airports by positively identifying each worker as they enter the airfield. This work leverages the unique installation at San Francisco International Airport which is the only airport in the world using biometrics throughout the entire airport for access privileges. **(Recognition Systems, Inc.)**
- ***Commercial Aviation, Cargo and Seaport Security:*** Berkeley Lab is developing reliable, long-lived neutron sources and detectors specially designed for rapidly screening cargo ranging from passenger luggage to containerized cargo. It also is exploring a new technology, ex-situ MRI, which could search for specific chemical compounds (such as drugs or explosives) in luggage without the use of ionizing radiation. **(E. O. Lawrence Berkeley National Laboratory)**
- ***Commercial Aviation, Cargo and Seaport Security:*** LLNL has developed search and inspection technologies for screening airport passengers, baggage and cargo, including computed tomography, x-ray scanning, gamma-ray imaging, neutron interrogation and thermal imaging. **(Lawrence Livermore National Laboratory)**
- ***Commercial Aviation Security:*** InVision Technologies' explosives detection system (EDS) machines currently exclusively screen checked baggage in airports across the nation and airports worldwide. **(InVision Technologies)**
- ***Commercial Aviation Security:*** Research on methods for preventing terrorists from boarding public transportation, particularly commercial aircraft. **(NASA Ames Research Center)**



## Border and Transportation Security (continued)

- ***Commercial Aviation Security:*** Ames Research Center, with other NASA facilities, is developing a comprehensive program addressing the challenges of Commercial Aviation Security, including: passenger threat assessment and monitoring of the airport grounds; protection of the overall Air Transportation Management system; and hardening of the airplane in-flight to ensure its safe operation. Ames monitors and maintains a record of safety violations within the national airspace to track security infractions and detect patterns that reflect a weakness in the overall system. **(NASA Ames Research Center)**
- ***Commercial Aviation Security:*** NEC's SmartCatch Vision surveillance technology has been used to detect unattended baggage; unattended vehicles or persons in a restricted area; persons attempting to bypass a security gate; people moving against normal traffic flows; release of chem/bio hazards, etc., all in multiple lighting and weather conditions. Currently it is being deployed at a major California airport for detecting unauthorized piggybacking and tailgating in violation of established access control policies and procedures. **(NEC)**
- ***Interconnection of Border and Transportation Security Systems:*** Cenus Technologies' service-agnostic routing enables the networking of existing distributed agency networks and autonomous systems; allowing for real time distribution and information sharing between heterogeneous networks involved in border and transportation security. This provides disparate agencies global coordination and global access to knowledge which is crucial to secure public and private transportation systems and facilities and the nation's borders. **(Cenus Technologies)**
- ***Long Range and Remote Surveillance:*** Intevac's Laser Illuminated Viewing and Ranging (LIVAR<sup>®</sup>) imaging system enables the visual detection of targets at ranges extending beyond 20 kilometers. LIVAR<sup>®</sup> enables remote areas, which cannot be monitored by standard surveillance equipment at night, to be effectively searched for potential threat targets. **(Intevac)**
- ***Smart Visas:*** To ensure positive ID and control of foreign visitors, VeriSign's two-factor smart visas, with digital certificates and biometrics, will verify the identity of the person with the visa. **(VeriSign)**
- ***Transportation Security:*** RAE Systems' Photo-Ionization Detectof-based gas detection instruments provide commercial and military staffs the ability to detect toxic gases in minute concentrations prior to their entering truck trailers for maintenance or inspection. **(RAE Systems)**

## DOMESTIC COUNTERTERRORISM

*“Our Nation will use all legal means—both traditional and nontraditional—to identify, halt...terrorists in the United States.”*  
—*National Strategy for Homeland Security*

- ***Bomb Detection:*** Technology to disable suspected explosive devices while preserving forensic information (used to disable the shoe bomb of accused terrorist Richard Reid) has been licensed to industry and is now a primary tool of bomb squads nationwide. (**Sandia National Laboratories**)
- ***Concealed Weapons Detection:*** Naval Postgraduate School is researching a concealed weapons detection system using ultra-wideband impulse electromagnetic wave illumination of persons armed with concealed weapons. (**Naval Postgraduate School**)
- ***Covert Surveillance:*** Intevac’s EBAPS™ cameras, built upon state-of-the-art night vision technology, provides low light level surveillance capability without the need for artificial illumination. (**Intevac**)
- ***Explosives and Weapons Detection:*** ARACOR is currently developing enhanced Eagle cargo inspection system neutron-based capabilities for detecting explosives. ARACOR also is working with the Department of Energy’s National Nuclear Security Administration to jointly develop an inspection method to detect weapons of mass destruction and special nuclear materials. (**ARACOR**)
- ***Explosives and Weapons Detection:*** InVision Technologies provides 90% of the explosive detection systems (EDS) to the Transportation Security Administration (TSA) for checked baggage screening at the nation’s airports. Its subsidiary, Quantum Magnetics, concentrates on developing screening devices using quadrupole resonance, which targets explosives’ molecules and low-frequency magnetic sensing for detecting weapons and currency. (**InVision Technologies and Quantum Magnetics**)
- ***Forensic Analysis:*** Lawrence Livermore National Laboratory’s Forensic Science Center has developed unique capabilities to detect and characterize ultratrace levels of virtually any compound in any sample matrix. It has been designated by the international Organization for the Prohibition of Chemical Weapons as the second U.S. chemical weapons (CW) challenge inspection analytical laboratory. (**Lawrence Livermore National Laboratory**)
- ***Forensics and Materials Characterization:*** The Advanced Light Source (ALS) at Berkeley Lab provides a variety of synchrotron based spectral tools useful for analytical and surface chemistry work including forensics and biological research using Fourier-transform infra-red spectroscopy. The National Center for Electron Microscopy has forefront capabilities with potential for forensics, surface science. (**E. O. Lawrence Berkeley National Laboratory**)

## Domestic Counterterrorism (continued)

- **Human Identification Technology:** Applied Biosystems' human identification technology is used for criminal investigations, identification of missing persons, military personnel and victims of mass disasters. Applied Biosystems' identification kits and genetic analysis instrumentation were used in the World Trade Center victim identification process. (**Applied Biosystems**)
- **Information Dissemination Control:** VeriSign's secure communications for public health, disease control and emergency responders enables experts to effectively address threats and prevent unwarranted public alarm. (**VeriSign**)
- **Information Security:** The computer scientists and applied mathematicians in Berkeley Lab's Computational Sciences Division are contributing to information security via study of: (1) Data protection technology—essential for the preservation of the national infrastructure; (2) Secure and reliable multicast development and deployment for monitoring and information sharing. (**E. O. Lawrence Berkeley National Laboratory**)
- **Physical Detection:** SRI's research and development of electromagnetic through-the-wall radar, clandestine detection and surveillance and systems to shield and disarm chemical and biological agent dispensers. (**SRI International**)
- **Privacy protection and inference control:** PARC's security researchers have been selected to develop the privacy protection for the Genisys program, funded by the Defense Advanced Research Projects Agency (DARPA). The program's goal is to produce technology enabling information repositories that can be used to predict, track, and preempt terrorist attacks. (**Palo Alto Research Center**)
- **Security with Privacy:** IBM is pioneering IT systems that enhance personal privacy while also providing the security features necessary to combat domestic terrorism. One technique protects individual privacy by randomizing data values in a way that still permits patterns within an ensemble of data to be discerned. Improved authentication, authorization and audit safeguards are also underway. (**IBM**)
- **Truck and Car Bomb Detection:** Development of technologies and production of mobile or stationary material specific non-intrusive inspection system to detect presence of bulk explosive concealed in trucks and cars. (**Ancore Corp.**)

## PROTECTING CRITICAL INFRASTRUCTURE

*“We must...improve protection of the individual pieces and interconnecting systems that make up our critical infrastructure.”*  
—National Strategy for Homeland Security.

- ***Blast and Structural Analysis:*** Computer scientists and applied mathematicians at Berkeley Lab have developed powerful new techniques for simulating explosions and deflagrations in underground chambers. **(E. O. Lawrence Berkeley National Laboratory)**
- ***Blast and Structural Analysis:*** SGI’s research on the use of computer modeling applications developed for crash analysis in automotive industry is being applied for buildings and construction. **(Silicon Graphics Inc.)**
- ***Controlled Viewing of Secured Locations:*** iPIX’s networked video security cameras (NetCams) provide 360 degree-by-180 degree coverage, reducing the number of cameras necessary, yet allowing for a higher level of visual awareness and analysis from multiple locations. iPIX NetCams have no moving parts and provide digital pan tilt and zoom for comprehensive visual capture with targeted information, capturing and recording the entire environment, while panning and zooming to view just a portion of the scene. **(iPIX)**
- ***Cyber Counterintelligence and Security Countermeasures:*** Naval Postgraduate School is researching the use of deception, psychological operations, and other aspects of information operations as a means to conduct cyber counterintelligence and security countermeasures against technically savvy information warriors, with particular emphasis on attackers sponsored by nation-states, terrorist organizations and criminal syndicates. **(Naval Postgraduate School)**
- ***Cybersecurity:*** ArcSight provides the software for building the Information Sharing and Analysis Centers recommended by the National Strategy to Secure Cyberspace by allowing independent organizations to share in a controlled manner relevant real time security information with trusted partners. **(ArcSight)**
- ***Cybersecurity:*** Array Networks’ Array SR technology is the first wire-speed network traffic analyzer designed to scan, analyze and record incoming and outgoing network traffic in real-time. Unlike traditional monitoring, detection and network sniffing technologies, the Array graphically reconstructs a snap-shot of data as it was viewed or created by the user, and records a copy of what traveled over the network at a specific time, traceable to any network-connected device, and enables administrators to monitor and flag suspicious activity in real-time. **(Array)**

## Protecting Critical Infrastructure (continued)

- **Cybersecurity:** Cylink is the developer and provider of real-time security solutions which ensure confidentiality, integrity and authentication during the critical information-sharing process between federal, state, and local law enforcement agencies. **(Cylink)**
- **Cybersecurity:** HP Labs maintains a robust global research program developing IT Security technologies for adaptive and critical infrastructures. Areas of focus include improved and simplified manageability of large scaled systems through the application of our corporate immune system model, hardware security appliances and policy driven control. Platform protection research is developing automated information flow controls and the integration of trusted computing modules with general purpose IT machines. **(Hewlett-Packard)**
- **Cybersecurity:** IBM has a substantial research and development effort for cryptographic coprocessors, secure storage devices, and data recovery for applications and devices. **(IBM)**
- **Cybersecurity:** Lawrence Livermore National Laboratory is home to the Computer Incident Advisory Capability (CIAC), the Department of Energy's cyber watch and warning center. CIAC assists any DOE facility experiencing a computer security incident with analysis, response and restoration support. CIAC also develops cyber security and intrusion detection tools and cyber defense solutions to attacks. **(Lawrence Livermore National Laboratory)**
- **Cybersecurity:** Network Associates' suite of McAfee security solutions provides consumers, industry and government manageable virus protection and security against malicious code and content. In addition, Network Associates Laboratories, the technology research division of Network Associates, Inc., is widely recognized as the world leader in information security research and development. **(Network Associates, Inc.)**
- **Cybersecurity:** Sanctum's industry leadership in Web Application Security solutions aids industry and government in stopping Web application attacks. AppShield, an automated Web application firewall, provides 24/7 automatic defense to Web applications from threats such as internet worms (e.g. Nimda), identity theft, e-shoifting, web site defacement and many more. **(Sanctum Inc.)**

## Protecting Critical Infrastructure (continued)

- ***Cybersecurity:*** Development of intrusion detection and response systems that prevent or delay intruder access to critical computer networks. These systems include countermeasures that confuse cyber attackers and reduce their effectiveness.  
**(Sandia National Laboratories)**
- ***Cybersecurity:*** As the operator of a critical infrastructure, the DNS and SS7 networks, VeriSign has developed leading edge cybersecurity practices to address cyber attacks. It engages in R&D for security software for authentication and encryption of networks and provides a system testbed for state-of-the art security hygiene applied to critical infrastructure data centers. **(VeriSign)**
- ***Cybersecurity and Critical Infrastructure Protection Applications:*** Oracle's solutions prevent destruction, corruption or degradation of information while protecting against a disruption of service. Solutions also provide connected and disconnected wireless access, decision support and interaction centers to help coordinate, collaborate and communicate across government agencies and with constituents.  
**(Oracle)**
- ***Electrical Infrastructure Security:*** The Consortium for Electric Reliability Technology Solutions (CERTS) program office located at Berkeley Lab, develops and disseminates new tools and technologies to model, protect and enhance the reliability and security of the nation's electrical power grid.  
**(E. O. Lawrence Berkeley National Laboratory)**
- ***Electrical Power Grid Security:*** Naval Postgraduate School is researching techniques for improving the security of electrical power grids in the country subject to terrorist attacks and natural disasters.  
**(Naval Postgraduate School)**
- ***Entry Point Screening:*** ARACOR's Eagle can be used to rapidly inspect cargo at entrances to military bases, government offices, and critical facilities, such as nuclear power plants. The Eagle is the only system capable of inspecting fluid-filled trucks, such as those used to destroy US embassies and barracks overseas. **(ARACOR)**
- ***Facility Entry Security:*** Ancore's technology is used for detection of bombs and other threats at entrances to sensitive facilities. Non-Intrusive systems, based on neutron interrogation, are being developed; some already installed, **(Ancore Corp.)**

Protecting Critical Infrastructure (continued)

- ***Food and Agricultural Crop Security:*** The USDA's Research Laboratory is a key national facility for research in developing diagnostics for food and agricultural crop contamination. **(USDA Agricultural Research Service's Western Regional Research Center and Plant Gene Expression Center, East Bay)**
- ***Fully Re-configurable Mobile Computer Network Attack/Defense and Exploitation Lab and Research Platform:*** Naval Postgraduate School is in the process of outfitting a mobile laboratory which will be used to access vulnerabilities of wireless devices/systems. Current efforts are being directed at wireless vulnerabilities and at network management for the ubiquitous surveillance environment. **(Naval Postgraduate School)**
- ***IT Security, High-End Computing and Dependable Software Systems:*** NASA Ames is developing a diverse range of IT Security and High-end Computing technologies necessary to protect the nation's critical IT infrastructure. Ames has led the recent trend toward grid computing which enables a decentralized approach to managing computing resources. NASA, a leader in high-dependability computing, has formed a partnership with Carnegie Mellon in this area. **(NASA Ames Research Center)**
- ***Physical Infrastructure Protection and Cybersecurity:*** Research and development on explosives detection and explosion containment such as permeable blast barriers. To protect critical information systems such as power grids, air traffic control, and financial systems, SRI has developed software for threat analysis, including intrusion detection software, multilevel security software systems, and authentication systems. SRI's Cyber Defense Research Center conducts vulnerability assessments. **(SRI International)**
- ***Protecting Information Systems:*** Oracle's database technology to protect information systems helps maintain organizational information availability, integrity, authentication, confidentiality and non-repudiation, and enables the public sector to prevent unauthorized disclosure of information. **(Oracle)**

## Protecting Critical Infrastructure (continued)

- ***Survivable Application Infrastructure:*** Melior Technologies Extreme Networking platform (XN) provides a framework for restoring critical enterprise systems, clients and devices after a catastrophic event. XN provides dynamic clustering and failover-protection of these resources, and allows them to dynamically reconnect with one another once the underlying networking infrastructure has been restored. **(Melior Technologies)**
- ***Survivable and Secure Infrastructure:*** Cenus Technologies' fully distributed application level routers interconnect servers and server networks in a fully distributed manner allowing for a geographically diverse architecture without any central points to congest or fail. These networks are fully self-healing and self-configuring, able to reconfigure themselves and continue to provide uninterrupted service from attacks and failures. These systems also add security, preventing the unauthorized access to server system resources, and the introduction of illegitimate information into interconnected server systems. **(Cenus Technologies)**
- ***Sustainability:*** HP Labs has a major research initiative to further HP's Adaptive Infrastructure product offering. The Utility Data Center already offers the ability to develop data centers with the flexibility to repurpose resources for priority tasks and to federate and manage large IT infrastructures from remote locations. HP Labs is extending these capabilities by conducting research on how to automate fully deployment and dynamic redeployment of resources (servers and storage) and applications to accommodate both foreseen and unforeseen workloads. This approach also allows for maximum prioritization should portions of the infrastructure be disabled. **(Hewlett-Packard)**
- ***System Security:*** IBM is developing new classes of "autonomic" IT systems that are self-configuring, self-protecting and self-healing. In addition to being simpler to operate, autonomic systems would enable security features to be implemented in the core of IT systems—not their periphery—thus enhancing their ability to protect data and rapidly recover from incidents. **(IBM)**
- ***System Security:*** IBM is pioneering on-demand computing, an advanced IT concept that builds on the features of autonomic and grid computing to provide computational resources and applications as needed in ways that are more economical and flexible than is possible today. On-demand computing will enable critical IT systems to respond robustly to accommodate spikes in demand, enhancing its effectiveness in any crisis situation. **(IBM)**



## Protecting Critical Infrastructure (continued)

- ***Vulnerability Reduction:*** Aanko Technologies' Supervisory Control and Data Acquisition (SCADA) Vulnerability Profiler (SVP)<sup>®</sup> bridges the gap between cyber and physical security by providing decision-makers with strategies for vulnerability reduction. SVP<sup>®</sup> offers prioritized steps to cost-effective mitigation, providing additional information on potential vulnerabilities beyond the scope of a facility's existing assessment, particularly on infrastructure interdependencies (power grid, manufacturing, transportation, communication, etc.). **(Aanko)**
- ***Water, Air and Food Security:*** Research on monitoring and preservation of water quality, air quality, and agriculture and food production in the face of chemical or biological attacks. **(NASA Ames Research Center in partnership with California Menay Institute)**

## DEFENDING AGAINST CATASTROPHIC TERRORISM

*“...the threat of terrorist attacks using chemical, biological, radiological, and nuclear weapons requires new approaches...”*

*—National Strategy for Homeland Security*

- ***Atmospheric Release Modelling:*** The National Atmospheric Release Advisory Center (NARAC), located and operated at Lawrence Livermore National Laboratory, is a national resource for real-time assessment of atmospheric releases of radiological, chemical, biological or natural hazardous materials. NARAC models and plume predictions are used by emergency managers across the nation to facilitate response planning and training and to guide decision making during an emergency. **(Lawrence Livermore National Laboratory)**
- ***Bioanalysis:*** Two state of the art synchrotron light sources provide forefront capabilities in protein crystallography, a critical tool in biodefense. **(E. O. Lawrence Berkeley National Laboratory, Stanford Linear Accelerator Center)**
- ***Biocharacterization:*** The Material Sciences Division of Berkeley Lab has developed extremely sensitive techniques in the application of Superconducting Quantum Interference Devices (SQUIDS) to high sensitivity antibody detection. **(E. O. Lawrence Berkeley National Laboratory)**
- ***Biodefense Systems:*** LLNL has made significant breakthroughs in biodetection instrumentation (miniaturization and increased ruggedness of DNA identification devices and flow cytometry) that are at the core of biodefense capabilities deployed since the September 11 terrorist attacks. The Biological Aerosol Sentry and Information System (BASIS), developed jointly by Livermore and Los Alamos, was deployed for the Salt Lake Winter Olympics. The two labs worked closely with many law enforcement, emergency response and public health agencies that would be involved in dealing with bioterrorism to develop appropriate sample handling, communications and response protocols. **(Lawrence Livermore National Laboratory, Los Alamos National Laboratory)**
- ***Biodetection:*** Applied Biosystems is the exclusive licensee of Hoffman-La Roche, owner of the basic PCR process and reagent patents, for research and development, and applied fields such as quality assurance and control, environmental testing, food testing, GMO testing, agricultural testing (including plant disease diagnostics), forensics and identity testing in humans (other than parentage testing), and animal identity testing. The 5' nuclease process using TaqMan<sup>®</sup> probes is the methodology being used by the Center for Disease Control (CDC) for detection of bioterrorism agents. **(Applied Biosystems)**

## Defending Against Catastrophic Terrorism (continued)

- ***Biodefense:*** LLNL developed technological breakthroughs in biodefense instrumentation, enabling DNA amplification and identification in minutes rather than hours and days as previously required, have been licensed to industry. DNA chips have been developed in partnership with Affymetrix. Sensitive polymerase chain reaction (PCR) technologies have been transferred to Cepheid Corp. Research on proteomics and pathogen detection is currently being carried out with CIPHERGEN Corp. (**Lawrence Livermore National Laboratory**)
- ***Biodefense:*** Extensive tools have been developed to model and monitor the transport of toxins and pathogens in open areas and in buildings. (**NASA Ames Research Center**)
- ***Biotechnology:*** The Joint Genome Institute is at the forefront of the nation's capabilities in biotechnology, with specific applicability to defense against bioterrorist attacks. (**E. O. Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, Los Alamos National Laboratory**)
- ***Biotechnology Cluster/Vaccines, Anti-infectives and Diagnostics:*** A major concentration of private sector scientific talent is present in the Bay Area on which to build a viable biodefense effort. The Bay Area, home to more than 600 bioscience companies, is the world's oldest and largest biotech cluster. The region's biotech industry is dominated by health-care firms focused on vaccines, therapeutics, diagnostics research, development and commercialization. Among these companies are nine working on vaccines, 18 developing anti-infectives (anti-viral, anti-bacterial and anti-fungal), and seven are perfecting diagnostics. (**Bay Area's bioscience companies**)
- ***Biotechnology/Vaccines – Anthrax, Smallpox:*** VaxGen has been funded by the National Institute of Allergy and Infectious Diseases (NIAID), a part of the National Institutes of Health (NIH), to develop a modern, recombinant anthrax vaccine (rPA) and to create a feasibility plan to manufacture an emergency stockpile of 25 million doses. In June 2003, the company initiated a Phase I clinical trial in humans to evaluate how rPA compares to the only currently licensed vaccine, in terms of its safety and its ability to induce the immune system to develop antibodies to anthrax. Under an agreement with the Chemo-Sero Therapeutic Research Institute (Kaketsuken) of Japan, VaxGen has begun development of a potentially safer smallpox vaccine. (**VaxGen, Inc.**)

## Defending Against Catastrophic Terrorism (continued)

- ***Chemical Agent Detection:*** Development of active neutron based techniques to detect presence of chemicals in cargo carried in trucks and in land and sea cargo containers. (**Ancore Corp.**)
- ***Chemical and Biological Detection:*** Research on a smart suite of physiological and environmental sensors for early detection of chemical and biological attacks. (**NASA Ames Research Center**)
- ***Chemical and Biological Detection:*** Microsensors for advanced detection of chemical and biological agents, using microchips as miniature chemical analysis laboratories for portable use by first responders, are now under development and testing with commercial partners. (**Sandia National Laboratories**)
- ***Chemical and Biological Detection:*** Remote bioagent detection systems provide advanced warning of a biological weapon threat using ultraviolet laser-induced fluorescence to scan for and discriminate clouds of biological agents over a broad area. (**Sandia National Laboratories**)
- ***Chemical and Biological Detection and Response Systems:*** Technologies are currently deployed in the Washington Metro and in prototype form at San Francisco International Airport. (**Sandia National Laboratories**)
- ***Chemical and Biological Sensors:*** Nanosys' proprietary nanotechnology-enabled sensor platform enables the direct electrical detection of biological and chemical analytes in a label-free, highly-multiplexed format over a broad dynamic range. This revolutionary technology will enable applications ranging from high throughput genetic analysis and proteomics to drug screening to clinical diagnostics and biowarfare detection. (**Nanosys, Inc.**)
- ***Chemical and Biological Warfare Defense:*** SRI's programs to detect, identify, neutralize and protect against chemical and biological agents in a variety of environments have been ongoing since 1978. Work ranges from basic research, applied science and engineering, database and signal processing, algorithm development, modeling, and concept feasibility demonstrations to hardware integration and field testing of systems. (**SRI International**)
- ***Chemical Detection:*** LLNL has developed portable chemical sensors, for both attended and unattended operation, that can variously detect waterborne species, airborne volatiles, and particulates. LLNL also has developed systems of remotely detecting and identifying a wide range of gases from high overhead and characterizing effluent materials by the spectral fingerprints. (**Lawrence Livermore National Laboratory**)

## Defending Against Catastrophic Terrorism (continued)

- ***Contamination of Buildings:*** Berkeley Lab's Environmental Energy Technologies Division investigates indoor and outdoor air fate and transport for the DOE and DTRA. Specifics of their work include modeling of transport of chemical and biological agents in buildings, design of sensor networks for buildings, and self-defending buildings. **(E. O. Lawrence Berkeley National Laboratory)**
- ***Decontamination:*** Non-toxic foam to decontaminate facilities following an anthrax attack, licensed to two industrial firms and used for clean up of the Dirksen, Hart and Ford Buildings in Washington and contaminated U.S. Postal Service sites. **(Sandia National Laboratories)**
- ***DNA Signatures:*** LLNL is developing "gold standard" DNA signatures for top priority threat pathogens, and is working with the Centers for Disease Control to validate these signatures and distribute them to public health agencies nationwide. LLNL also works with the FBI, Department of Defense, and the Intelligence Community to develop detailed biological "fingerprints" and data to support forensic analysis for any act of biological terrorism. **(Lawrence Livermore National laboratory)**
- ***Ensure Business Continuity:*** Oracle's solutions for redundant systems to ensure that organizations are fully prepared to detect, prevent and respond to unforeseen disruptions in system availability, whether the result of natural disasters, internal sabotage or terrorist threats and attacks. These include redundant hardware and software, synchronous and asynchronous off-site back-up, and online systems maintenance. **(Oracle)**
- ***Environmental Characterization:*** Berkeley Lab's Center for Environmental Biotechnology researches all aspects of bacterial survival and use in the natural environment. Its studies of natural biological background can help distinguish man-made attacks from natural outbreaks and studies of the survivability of bacterial and viral agents in the environment under various conditions. A particular research interest is the use of chemotaxis for mapping water-borne biochemical contaminants with bacteria. The Isotopic Geochemistry group can geo-locate materials from variations in isotopic abundances around the world. Berkeley Lab's geophysics and water resources experts can contribute to locating and characterizing underground facilities and to performing threat analysis on domestic water supplies respectively. **(E. O. Lawrence Berkeley National Laboratory)**

## Defending Against Catastrophic Terrorism (continued)

- ***Genetic Analysis:*** Applied Biosystems provides DNA-based analysis kits for identification of microorganisms through sequencing of ribosomal DNA genes, and manufactures genetic analysis systems—the technology that made it possible for the rapid sequencing of the human genome by both the public and private sectors. **(Applied Biosystems)**
- ***Nuclear Detection:*** Ancore developed active neutron based techniques to detect nuclear materials and device components in fully-loaded trucks and cargo containers. **(Ancore Corp.)**
- ***Nuclear Detection Systems:*** LLNL's rapidly deployable, reconfigurable network of correlated radiation detectors and cameras can detect, characterize and track vehicle-transported radioactive or nuclear material moving at near-freeway speeds. Upon detecting an unknown source, the system warns security authorities, providing information about the detection, vehicle type and location. This system also is being adapted for waterway applications. **(Lawrence Livermore National Laboratory)**
- ***Nuclear Incident Response:*** LLNL is a key participant in regional and national nuclear response teams, including a radiological assistance team (which assists state and local agencies), a nuclear accident response group (which deals with accidents involving U.S. nuclear weapons), and a joint technical operations team (which deals with nuclear terrorism and extortion threats). LLNL maintains a deployable response capability of expert personnel and equipment, including the HotSpot mobile radiological laboratory. **(Lawrence Livermore National Laboratory)**
- ***Protein/Small Molecule Analysis:*** Applied Biosystems manufactures mass spectrometry systems for analysis proteins and small molecule metabolites – important for detecting how a substance is metabolized by the body. These systems can be used toward the identification of microorganisms as well as to measure the level toxins and/or drug quantities present in a sample. **(Applied Biosystems)**
- ***Radiation Detection:*** LLNL has half a century of experience in the detection and analysis of radiological and nuclear materials. The Lab is developing a suite of new radiation detectors suitable for Customs officials and other first responders, including portable, easy-to-use, high-resolution handheld detectors that use electromechanical cooling (instead of liquid nitrogen) and that provide reachback capabilities to technical experts at the Laboratory. **(Lawrence Livermore National Laboratory)**

## Defending Against Catastrophic Terrorism (continued)

- ***Real Time Networking for Emergency Information***  
***Access/Distribution:*** Cenus Technologies' scalable networking enables agencies responsible for the detection, collection, analysis, and distribution of critical information from distributed sources and computational systems to coordinate and deliver instructions and treatment regimens globally with sufficient speed for a successful response to bioterrorism, and nuclear terrorist attacks.  
**(Cenus Technologies)**
- ***Ultraviolet LEDs for Bioagent Detection:*** A joint university and industry team, including Lumileds and Palo Alto Research Center (PARC), is developing a compact bioagent warning and detection system that will be based on high-performance ultraviolet semiconductor optical sources, and draws on their industry-leading expertise in fields such as optical engineering and material sciences in the field of blue and near ultraviolet nitride light emitters.  
**(Lumileds, Palo Alto Research Center)**
- ***Urban Defense:*** The Biological Aerosol Sentry Information System (BASIS), used to monitor major events, combined with the Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism (PROTECT) for high-value installations, serves as the basis for the "Defense of Cities" effort to detect and mitigate the consequences of a major chemical or biological attack. **(Sandia National Laboratories, Lawrence Livermore National Laboratory, Los Alamos National Laboratory)**

## EMERGENCY PREPAREDNESS AND RESPONSE

*“We must prepare to minimize the damage and recover from any future terrorist attacks... We must plan, equip, train, and exercise many different response units to mobilize without warning for any emergency.”*  
—National Strategy for Homeland Security

- ***Biological Threat Response:*** Oracle’s solution enables emergency department physicians to quickly assess and monitor disease outbreaks through a form indicating symptoms. The solution includes software in the database that analyzes data for aberrations that could indicate an unusual event. The database stores all information, which is easily accessible by designated and trained members of the hospital staff using only a browser in a hosted environment. **(Oracle)**
- ***Command and Control Based on Geospatial Information Systems:*** SGI’s advanced command and control systems is designed to get the right information to the right people at the right time—based on geospatial data processing in support of first responders. **(Silicon Graphic Inc.)**
- ***Commercial Transportation Security:*** AQUI Systems provides innovative tracking, routing and navigation software for commercial vehicles. Its technology uses GPS sensors to build road condition databases and next generation routing/navigation software that enables commercial vehicles to navigate safely around trouble spots. Following a terrorist incident, it is critical that commercial vehicles be able to navigate around the region to provide supplies to the communities. **(AQUI)**
- ***Data Automation and Improved Case Management Process:*** Fully integrated Oracle E-Business Suite makes agencies’ front-and-back-office systems work together seamlessly. The suite is the only complete set of business applications that enables agencies to cut costs across supply chain, financials, projects, human resources and business intelligence functions. **(Oracle)**
- ***Demonstration of Linked Unmanned Aerial Vehicle (UAV) Observations and Atmospheric Model Prediction in Chem/Bio Attack Response:*** Naval Postgraduate School has demonstrated the feasibility of linking a coarse grid mesoscale model to a fine scale diagnostic wind model for producing fine resolution forward and backward plume trajectories. The study also demonstrated the utility of using a UAV platform for measurements and a field laptop computer for data display. **(Naval Postgraduate School)**



## Emergency Preparedness and Response (continued)

- ***Emergency and Surveillance Network:*** Naval Postgraduate School has research underway on integrating, deploying and monitoring collaborative networks designed for maintaining emergency site situational awareness and ubiquitous surveillance. The project is also addressing the challenges of civil-military situational awareness and interagency data fusion. **(Naval Postgraduate School)**
- ***Emergency Preparedness:*** Research and development on emergency response training, emergency response tools, command and control systems for first responders, and robust, mobile, ad hoc wireless communication systems. **(SRI International)**
- ***Emergency Preparedness and Response:*** The web-enabled Bio-Act platform provides users with a single, integrated point of access to observe real-time, geographically-based crisis situations, run predictive simulations, communicate instantly across diverse venues and collaborate on decision-making when faced with actual or potential public health and environmental safety disasters, including bio-attacks. **(NASA Ames Research Center in partnership with California Menay Institute)**
- ***Emergency Preparedness and Response:*** RAE Systems' rapidly deployable networks of sensors provide real-time, flexible monitoring of toxic chemical gases and radiation at terrorist event sites. Networks can be easily shifted to accommodate shifting wind patterns or a changing situation. In addition, RAE Systems equips first responders in all 50 states with handheld gas and radiation detectors. **(RAE Systems)**
- ***Emergency Preparedness and Response:*** Ramsesrisk solutions provide a quantitative and comprehensive solution for determining how to cost effectively prepare for and mitigate a terrorist threat against fixed assets, mobile assets and cyber assets. The system incorporates an event notification process in the event of an attack that may be near a given property but not the exact target. Once the risk score is determined, Ramsesrisk works with the organization to insure the exposure through risk transfer methods. **(Ramsesrisk)**
- ***Emergency Response Control Center:*** NASA Ames Research Center expertise in the development and application of information systems technologies for managing and controlling a complex logistics operations during emergency response includes: planning and scheduling of limited resources; human-centered systems techniques to analyze and help develop the threat response system; anomaly detection techniques to monitor process; and advanced human-computer interaction research to ensure the appropriate information is provided to the human operators. **(NASA Ames Research Center)**

## Emergency Preparedness and Response (continued)

- ***Emergency Response Information:*** During an emergency, stress on critical information systems means more servers and resources must be brought into play rapidly. However, these systems must also be able to respond rapidly and be in the appropriate places for optimal response time. Cenus Technologies makes it possible to provision new systems on-the-fly to handle emerging needs for these systems without pre-positioning of hardware. **(Cenus Technologies)**
- ***Emergency Response Planning:*** The Homeland Operational Planning System (HOPS), developed by LLNL in partnership with the California National Guard, provides insight into the vulnerabilities of elements of U.S. infrastructure and the likely consequences of strikes against potential targets. The Joint Conflict and Tactical Simulation (JCATS) developed initially for the Defense Department to model military operations, also can be used to assess tactics and strategies for protecting cities, industries and other critical sites against terrorist attack. **(Lawrence Livermore National Laboratory)**
- ***Emergency Response Transportation:*** NASA Ames is developing advanced-technology for extremely short take-off and landing vehicles, enabling rapid deployment of people and resources to inaccessible or highly dangerous environments. **(NASA Ames Research Center)**
- ***Facilities Documentation:*** iPIX's capture and playback of 360-degree-by-360-degree Immersive Still Image technology, referred to as Virtual Tours, are used at The White House to provide "virtual visits" while protecting secured locations from potential threat. The Winter Olympics in Utah used 3000 iPIX images to provide first response law enforcement and safety personnel with complete views of every venue they were protecting. **(iPIX)**
- ***First Responders Communications Platform:*** Melior Technologies Extreme Networking platform (XN) provides a solution for the issue of connecting divergent systems and resources used by "first responders." XN provides a wireless, cross-platform, protocol-independent framework that allows everything from simple legacy devices to the latest hi-tech platforms to be integrated with one another seamlessly and dynamically at the disaster site, all while ensuring the reliability, scalability and security of this ad hoc network. **(Melior Technologies)**

## Emergency Preparedness and Response (continued)

- ***Homeland Security Analysis:*** The supercomputers at Lawrence Berkeley and Lawrence Livermore National Laboratories are collaborating with private industry in database management, terascale computing, modeling and complex simulation software—technologies critical to homeland security analysis. (**Advanced Micro Devices, Applied Materials, E. O. Lawrence Berkeley National Laboratory, IBM Almaden Research Center, Intel Corporation, Lawrence Livermore National Laboratory, Oracle Corporation, People Soft**)
- ***Homeland Security Analysis:*** Supercomputing/computational biology research directed toward the development and use of bioinformatics tools and databases. (**E. O. Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory**)
- ***Identity Management:*** Aquave suite of SmartCard-based systems provides strong authentication, access control and secure data portability for emergency response personnel. This technology reduces the risk of terrorists impersonating emergency workers at federal, state and local levels. It also allows the first responders to operate and access data in offline mode, in case of attacks which may compromise computer networks. (**Aquave Group**)
- ***IT System Recovery:*** Cenus Technologies' unique ability to provide load-balanced cluster support for high volume systems allows for distributed clusters with virtually local performance characteristics and rapid recovery if critical systems are lost. (**Cenus Technologies**)
- ***IT System Recovery:*** IBM's Business Continuity and Recovery Services leverages the innovative security research from IBM's worldwide research labs to assess and protect data, networks and systems and address intrusion detection, security assessment, incident management, firewall management, data backup and recovery and secure hosting. (**IBM**)
- ***Meta-Data and Advanced Networking:*** Cenus Technologies' advanced next generation networking technologies enables the interconnection of distributed heterogeneous server networks on either an inter-agency and/or inter-autonomous system basis. This seamless routing platform enables these networks to leverage existing IT infrastructure investments and access, distribute, share and coordinate resources and information in real time, ultimately enabling the efficient distribution and coordination of meta-data. (**Cenus Technologies**)

## Emergency Preparedness and Response (continued)

- ***Mission Critical Communication Platform:*** Aspect's technologies enable the deployment, scheduling, and tracking of personnel based on communication, collaboration, and intelligence data. **(Aspect)**
- ***Modular Robotics:*** Palo Alto Research Center, in a program co-funded by the Defense Advanced Research Projects Agency (DARPA), is developing reconfigurable modular robot systems composed of modules less than 5 cm on a side, that can reconfigure themselves into various shapes using onboard actuation, sensing, computation and communication. Such systems have potentially high value in search-and-rescue, making it possible to perform rescue operations without endangering workers. **(Palo Alto Research Center)**
- ***National Surveillance Network and California Center for Preparedness:*** LLNL, the Governor's Office of Emergency Service, and UC Davis are key participants in the California Center for Preparedness (CCP). The CCP coordinates operational and communications infrastructures needed to address large-scale medical and public health events, conducts training, education, and distance-learning programs for first responders, serves as a clearinghouse for basic and applied research into issues concerning biodefense and homeland security, and disseminates research in biodefense and homeland security into mainstream applications in human health, animal health, and agriculture. **(Lawrence Livermore National Laboratory, Governor's Office of Emergency Service, and UC Davis)**
- ***Portable Energy Supply:*** Nanosys is developing nanocomposite photovoltaic technology that combines precisely engineered inorganic semiconductor nanocrystals with a light-weight, flexible host-matrix to generate solar cells. This single photovoltaic technology will provide first responders or dismounted soldiers with a portable power supply following a terrorist incident. **(Nanosys, Inc.)**
- ***Prevention of Vehicle Contamination:*** Nanosys' nanostructured surface technology creates controlled surfaces with unique and extreme surface-characteristics by controlling the orientation, geometry, packing density and composition of various nanostructures applied to the surface. Among other uses, this technology will provide anti-bacterial coatings for vehicles to prevent contamination by biological weapon agents. **(Nanosys, Inc.)**

## Emergency Preparedness and Response (continued)

- ***Public Alert Distribution:*** SocialTech’s TRAK Alert System enables multiple authorities to share image-based alert information with each other and with the public. Bi-directional information flow enhances prevention and response capacity. The solution includes building a deeply populated shared address book of recipients for pinpoint distribution of alerts that is easily scalable to regional, statewide, or national levels. The TRAK Alert System directly impacts Terror Alerts, Amber Alerts, and daily Community Health and Safety Alerts. **(SocialTech, Inc. in partnership with Unisys and Microsoft)**
- ***Public Alert Network:*** Vasona’s Public Alert Software System, PASS, an “intelligent network” manages, distributes and displays event specific emergency instructions via strategically located digital displays managed by computers linked by intelligent software via wired or wireless networks. The public is automatically informed of an emergency and the appropriate response is immediately conveyed. Information about terror incidents can be disseminated on several levels: national, regional, local or individual locations within a facility. As a regional alert system, PASS can be integrated with other systems such as the Amber Alert or Emergency Alert Systems. **(Vasona Technology, Inc.)**
- ***Security Preparedness and Response:*** NEC’s SmartCatch Vision surveillance technology provides a quantifiable increase in security while increasing the confidence of employees and the general public. It offers increased facility efficiencies while reducing total security costs without any delays or inconvenience to employees or customers. It can be deployed both for real time detection of suspicious behaviors as well as forensic search for after the fact analysis and increased preparedness. **(NEC)**
- ***Surveillance and Emergency Preparedness:*** Nanosys’ proprietary technology for nano-enabled high-performance macroelectronics has a variety of defense applications for surveillance and emergency preparedness. Its technology includes both portable and large-area flat panel displays, low-cost RFID and smart cards, distributed RF-sensor security networks and electronically steerable phased-array RF antennas. **(Nanosys, Inc.)**

# **Examples of Bay Area University Research Programs Benefiting the Nation's Security**

## **STANFORD UNIVERSITY**

### **Bio-X Program**

The Stanford University's Bio-X program brings together engineering, physics, chemistry, and the information sciences with biology and medicine to foster new discoveries and inventions. The Stanford Schools of Engineering, Medicine, Humanities and Sciences, and Earth Sciences teamed up to form the new program. Bio-X will create opportunities for fundamental discoveries that emerge from new intellectual connections between traditionally separate disciplines.

Stanford scientists, including a number of Bio-X affiliates, have been heavily involved in homeland security issues. Bio-X holds great opportunities for discovering new ways to sense and control biological agents, for designing new defenses against pathogens and for promoting healing with new techniques and new instruments.

The Bio-X program is headquartered in the new Clark Center which, when fully occupied, will house about 700 people from all of the participating scientific fields and more than twenty-five university departments. This unprecedented gathering of specialists from different areas of science and technology forms a geographic focus for bringing together the much larger Stanford community of scientists and engineers working on interdisciplinary projects involving biology. Bio-X will also engage collaborators and industrial affiliates from outside Stanford.

Participants in the Bio-X program are expert in biorobotics, biosensors, genetic control systems, cell and tissue imaging, image processing, signal transduction, instrumentation and medical devices, bioengineering, machine-organism interfaces, bioinformatics, high-resolution single-molecule biophysics, genomics and gene regulation, protein-folding biochemistry and modeling, chemical biology, neuroscience, biomechanical simulation, network control modeling, and microbial ecology and systems. Stanford has the great advantage of having people in all these fields working together on one campus.

## **Other Stanford Programs Related to Homeland Security**

### ***Department of Electrical Engineering***

Stanford's Department of Electrical Engineering has a research program underway focused on detecting biological agents, particularly the contamination of water. The ultimate research goal is to develop effective remote sensing systems that are portable and fully automatic, enabling the detection of a variety of known and novel biological agents before troops on the battlefield are exposed. The Department has achieved success in developing a prototype of a handheld biotector.

## **UC BERKELEY**

### **CITRIS – Center for Information Technology Research in the Interest of Society**

(CITRIS is a partnership of four UC campuses and the private sector, and is headquartered at UC Berkeley)

Centered at UC Berkeley, the Center for Information Technology Research in the Interest of Society (CITRIS) will sponsor research on problems that have a major impact on the economy and quality of life: conserving energy; education; saving lives, property, and productivity in the wake of disasters; boosting transportation efficiency; advancing diagnosis and treatment of disease; and expanding business growth. More than 100 faculty members in engineering, science, social science, and other disciplines at four UC campuses will collaborate with researchers at more than 20 supporting companies on CITRIS research.

Solutions to many of these problems have a common IT feature: at their core they depend on highly-distributed, reliable, and secure information systems that can evolve and adapt to radical changes in their environment, delivering information services that adapt to the people and organizations that need them. It is this feature that is at the heart of the initial research agenda for CITRIS. These systems, called Societal-scale Information Systems (SISs), must easily and naturally integrate devices, ranging from tiny sensors and actuators to hand-held information appliances, workstations, and room-sized cluster supercomputers.

Many CITRIS research projects have clear relevance to homeland defense. For example, sensor networks can be used to:

- Detect chemical and biological weapons;
- Allow “first responders” to get real-time information about the structural safety of a building and the location of building occupants; and
- Provide for physical security of bridges and other structures that might be subject to terrorist attack.



## **Other UC Berkeley Programs Related to Homeland Security**

### ***Bioengineering – Nano-Microscope***

The most advanced scientific tool in development in UC Berkeley's Department of Bioengineering is a nanoscopic micro-CIA (microscale confocal imaging array). The future potential of the nano-microscope includes developing a hand-held biowarfare detection device that can identify the slightest amount of biological warfare agents, or transform a microchip into an entire genomics or proteomics laboratory-on-a-chip to study genes and proteins in the quest for new disease-fighting drugs, or enable physicians to monitor their patients' health (down to a cellular level) from any location.

### ***Center for Infectious Disease and Preparedness***

Under the sponsorship of the Centers for Disease Control and Prevention, the UC Berkeley School of Public Health will be establishing the UC Berkeley Center for Infectious Disease and Preparedness to provide training and support to public health and safety systems in California and Nevada as part of a national network of such centers. UC Berkeley will be collaborating with the California Menay Institute at NASA Ames Research Center in this endeavor.

### ***Cyber-security***

U. C. Berkeley is home to some of the world's leading researchers in cyber-security, with active research programs in wireless security, encryption, security for sensor networks and other power-constrained environments, intrusion detection, and defense of the Internet against worms, viruses, and distributed denial of service attacks. Berkeley also has significant expertise in the interdependencies between cyber-infrastructure and other elements of the critical infrastructure, such as air traffic control and the electric power grid.

### ***Environmental Surveillance Technology***

UC Berkeley's Department of Electrical Engineering and Computer Science has developed miniaturized environmental sensors combined with miniature radio transmission technology ("Smart Dust") that can be spread widely over an area for surveillance and environmental monitoring. The development of "Smart Dust" has exploited UCB programs in very large scale integrated circuits, ultra-small integrated circuits and micro-electromechanical devices.

### ***Structural Engineering Research on Potential Target Infrastructure***

UC Berkeley and other UC Campuses are working on the structural engineering of target buildings, bridges and other infrastructure. Their expertise ranges from retrofitting systems, the use of carbon overlays to resist seismic and blast forces and the design and testing of lightweight, advanced composite materials to improve blast resistance. In addition, UC can provide research on impact and penetration, projective impact and explosions, blasting of steel and reinforced concrete structures, and blast resistant structural design. UC Berkeley researchers currently are looking at the steel columns from the World Trade Center in an effort to improve structural design and construction and to understand the affects of fire on future steel structures.

## UC DAVIS

### **Multi-Disciplinary Public Health Initiative**

With its research strengths in medicine, veterinary medicine, primate biology, agriculture, biotechnology, and other life sciences, UC Davis is pursuing a multi-disciplinary public health initiative that will respond to threats from new and re-emerging infectious diseases, and address the recently developing needs for bio-defense. This initiative will establish new facilities and take advantage of federal funding that is being made available to better protect the public's health and the nation's food supply. Projects include:

#### ***National Biocontainment Laboratory***

UC Davis, in collaboration with the Lawrence Livermore National Laboratory, other UC campuses, and the State Department of Health Services is seeking federal funds to construct a biosafety level 4 laboratory to study infectious diseases naturally present in western states, including those potential bioterror agents, and help respond to disease outbreaks such as anthrax or smallpox.

#### ***Regional Centers of Excellence in Biodefense and Emerging Infectious Diseases***

UC Davis is developing a proposal for a regional center under the program established by the National Institute of Allergy and Infectious Diseases. The centers will perform basic and clinical research on infectious agents, expand the pool of researchers and technical personnel trained in emerging diseases and biodefense, create regional biodefense facilities and aid the region's response to public health emergencies.

#### ***Contained Research Facility***

This facility, the first of its kind in the U.S., will be a complex of greenhouses and laboratories where research on agricultural pests and plant diseases can be carried out in a highly-secure, biologically-contained environment.

#### ***Western Institute for Food Safety and Security***

UC Davis, in partnership with the California Department of Food and Agriculture and the California Department of Health Services, will establish an institute to develop methods to identify, treat and prevent both natural and intentional food contamination.

#### ***Plant Pest and Disease Surveillance Network***

UC Davis is a key participant in a USDA funded national surveillance network to protect crop plants and agricultural ecosystems, and is a participant in the California Center for Preparedness (CCP) with Lawrence Livermore National Laboratory, and the Governor's Office of Emergency Services. The CCP will coordinate operational and communications infrastructures needed to address large-scale medical and public health events; conduct training, education and distance learning programs for first responders; serve as a clearinghouse for basic and applied research into issues concerning biodefense and homeland security; and disseminate research in biodefense and homeland security into mainstream applications in human health, animal health and agriculture.

## UC SAN FRANCISCO

### **QB3 – Institute for Quantitative Biomedical Research**

(Headquartered at UCSF Mission Bay Complex)

The Institute for Quantitative Biomedical Research is one of four California Institutes for Science and Innovation created in 2000 to promote research and innovation. QB3 currently comprises over 100 faculty scientists and their research staffs at the three participating UC campuses: UC San Francisco, UC Berkeley, and UC Santa Cruz.

QB3 promotes and enables the integration of the quantitative and biomedical sciences to further our understanding of living systems at all levels of complexity—from atoms and protein molecules to cells, tissues, organs and the entire organism. In addition to forging new avenues of research, QB3 is dedicated to training a new generation of scientists to be fluent in the quantitative and biomedical sciences.

The goal of QB3 is to integrate efforts across disciplinary boundaries, in particular generating an expanded role for fields such as engineering, mathematics, physics, and computer science. The Institute expects to link the computational and physical tools of these areas to the analytical powers and the ability to manipulate biological systems derived from chemistry, genetics, and cell and molecular biology. The result will be a modern physiology, generated from molecular information together with bioinformatics and computational analysis, with a unique insight into the control systems that regulate phenotype and a unique ability to modify this behavior.

Research programs among QB3 investigators relevant to homeland security include:

#### ***Novel virus identification***

UC San Francisco used a specialized “virus chip” to identify the SARS virus in less than 24 hours. This technology is designed to identify novel pathogens with only a small sample of genetic material.

#### ***Web-based “microscope” for pathogen study***

UC Santa Cruz led the development of the Human Genome Browser, an online tool used to analyze and study the massive amounts of data generated by the Human Genome Project. UCSC now is proposing to create the Pathogen Browser, a web-based “microscope” that allows the analysis and comparison of Category A and some Category B pathogens, including any modifications, either genetically engineered or natural, of a pathogen compared to other known samples.

#### ***Biosensors***

UC Berkeley is using bacteria as sensors to identify biological and chemical agents at very low concentration. Bacteria are normally very sensitive to their environment, moving away from toxins and towards nutrients. UCB is learning about this capacity with the aim of harnessing it for use in nanotechnology.

## **UC SANTA CRUZ**

UC Santa Cruz, noted for creating the software that assembled the first public working draft of the human genome, is now focusing on comparative genomics, a field critical to managing data regarding genes of pathogenic organisms.

### ***Center for Biomolecular Science and Engineering (CBSE)***

UC Santa Cruz' CBSE fosters research and education intended to meet the challenges of the post-genomic era resulting from completion of the Human Genome Project and the sequencing of model organisms. The revolutionary technologies that have recently been developed to gather and analyze genomic information will help to forge a new understanding of biology, with widespread applications to medicine, agriculture, ecology and emerging infectious diseases (of paramount importance to homeland security).

## **Other UC Programs Related to Homeland Security**

### ***Cybersecurity and Security of Airports and Public Places***

Among the research areas being explored at the University of California are computer security, encryption, online secrecy, and monitoring of Internet communications, including pioneering work on "denial-of-service" attacks on the Web. UC Davis' Center for Digital Security uses physical and mathematical modeling to investigate threats to communications networks that might develop in the next five to ten years, and countermeasures to defend or "harden" networks.

UC researchers are involved in research and development related to technologies with the potential to improve security at airports and other public places. These include vision-based systems that range from face recognition systems and networks of omni-directional cameras running activity analysis algorithms that could be adapted for monitoring high-risk areas, to "augmented" reality systems for remote observation.



## **APPENDICES**



# APPENDIX A

## **BAY AREA CORPORATIONS WITH EXPERTISE RELATED TO HOMELAND SECURITY (Companies Contributing to This Report)**

### **Aanko Technologies Inc.** (Vacaville)

Aanko Technologies Inc. is a California Certified Minority and Veteran-owned Small Business. They have worked with government agencies, aviation, energy, chemical and healthcare industries, and Fortune 500 companies worldwide to devise strategies for vulnerability reduction. Aanko Technologies' services are based on its Turn Risk Into Revenue<sup>®</sup>, Assessment Methodology. This industry-based risk assessment technique aids clients in determining the where and why of investing valuable resources to protect their business interests. This process has helped increase client safety and security.

### **Ancore Corporation** (Santa Clara)

The TNA<sup>™</sup> (Thermal Neutron Analysis) and PFNA (Pulsed Fast Neutron Analysis) non intrusive inspection technologies for detecting explosives, drugs, chemical warfare agents and nuclear and radiological weapons were pioneered and patented by Ancore Corporation. Based on identifying material specific signatures, rather than shapes or configuration of objects, these technologies automatically pinpoint the contraband in carry-on items, luggage, trucks and air and sea cargo containers.

### **Applied Biosystems** (Foster City)

Applied Biosystems develops and markets instrument-based systems, reagents, software, and contract related services to the life science industry and research community. These technologies enable biological discoveries in life science research, pharmaceutical research and development, diagnostics, and agriculture. Applied Biosystems' broad portfolio of technologies, which include DNA sequencing, PCR, organic synthesis, chemiluminescence, mass spectrometry, and information management systems, enable genomics, proteomics, high throughput screening, and other molecular analyses.

### **Aquave Group** (Palo Alto)

Aquave Group is a provider of business and technology solutions that enable customers to realize the benefits of SmartCard applications. Its homeland security solution provides strong authentication, access control and secure data portability for first response personnel at the federal, state and local levels. Aquave technology reduces the risks of identity theft by terrorists, enforces the appropriate levels of security, and increases first response operation resiliency under emergency conditions.



Bay Area Corporations...(continued)

**AQUI Systems, Inc.** (Cupertino)

AQUI Systems, Inc., founded in 2001, offers patent-pending routing and navigation software that allows vehicles (mainly commercial vehicles) to travel more safely, predictably, cost efficiently and with fewer delays. AQUI's technology measures road speeds under a variety of conditions using GPS and other sensors to create future road speed estimates based on proprietary databases and analytics. Through this next generation routing software, it is possible to provide directions to the vehicles as to the best way to navigate around trouble spots.

**ARACOR** (Sunnyvale)

ARACOR's Eagle is the world's most powerful mobile and relocatable cargo inspection system. (Eagle's 6 MV x-ray source can penetrate at least 300 mm of steel.) ARACOR is developing enhanced Eagle capabilities for detecting explosives, nuclear materials and weapons of mass destruction. The Department of Defense is sponsoring development of Inspection AIDE (Analyzer for Identification of Drugs and Explosives). AIDE has been successfully tested, and ARACOR is awaiting funding to develop a prototype deployed on an Eagle. ARACOR also is working with the Department of Energy's National Nuclear Security Administration to develop and deploy an inspection method for detecting weapons of mass destruction and special nuclear materials in cargo.

**ArcSight** (Sunnyvale)

ArcSight is a leading provider of enterprise software solutions that enable large organizations to better manage their security function by integrating and optimizing the management of diverse sources of security-relevant information. By delivering complete aggregation, correlation, investigation, resolution and reporting—all within a single solution—ArcSight provides a coordinated infrastructure that maximizes security results while decreasing overall costs. ArcSight's 360° Intelligence utilizes asset-based correlation technology that allows enterprises to combine vulnerability assessment data and asset value with real time event data, improving their ability to detect true threats and attacks and react to them in real time.

**Array Networks** (Santa Clara)

Array Networks helps customers regain control of their networks, protecting their business assets and defending their companies against legal liabilities. The company's network security product line, including the Array SR, Array SP, and Array TM, helps address security compliance and assurance issues, whether mandated by government, industry or internal policy. Array's network security solutions ensure the integrity of an enterprise network by securing, monitoring, controlling and recording all internal and external Web traffic.

Bay Area Corporations...(continued)

**Aspect (San Jose)**

Aspect Communications Corporation is the leading provider of business communications solutions. Its Homeland Security solution is a mission critical communication platform that enables the gathering, analysis and dissemination of information that empowers people and systems to communicate with each other and share information. Aspect is the only company that provides the mission-critical software platform, development environment and applications that seamlessly integrate voice over IP (VoIP), traditional telephony, e-mail, voicemail, Web, fax and wireless business communications, while guaranteeing investment protection in a company's front-office, back office, Internet and telephony infrastructures.

**Cenus Technologies (Scotts Valley)**

Cenus Technologies is the leader in advanced, next generation Application Protocol (AP) routing, and is the first company to provide route optimization based on true Layer 7 (Application) based information. Cenus' core technology enables government agencies, enterprises, carriers and service providers to optimize their networks without the need to re-architect and in a manner that is non-disruptive to existing network routers, servers and other equipment and technologies. Cenus' application level routing layer is a platform for the interconnection of heterogeneous server networks either inter-agency, or inter-autonomous system, which enables the virtualization and resource aggregation of Internet-wide server networks. Cenus Technologies' platform provides breakthrough levels of performance, scalability, reliability, security, extensibility and redundancy.

**ContainerTrac (Berkeley)**

ContainerTrac's Port Automated Tracking Service (PATs) provides the maritime shipping industry with a 100% accurate automated container tracking solution which improves the safety and security of the waterfront while dramatically reducing the cost of operations for marine terminal operators. ContainerTrac's solution is a patent pending, proprietary combination of technologies that simplify retrofits onto existing container handling equipment and enables total accuracy even in densely populated container yards.

**Cylink Corporation (Santa Clara)**

Cylink develops, markets and supports a comprehensive portfolio of hardware and software security products for mission-critical private and public networks. Cylink's PrivaCy Manager provides advanced, policy-based, network security management. As a security solutions provider, Cylink partners with other network equipment vendors to provide and implement comprehensive network solutions. Cylink's key business solution focus areas are Homeland Security, including Critical Infrastructure Protection for Airports and First Responders, and Secure Storage Area Networks for Business Continuity and Disaster Recovery.

Bay Area Corporations...(continued)

**EoPlex Technologies, Inc.** (South San Francisco)

EoPlex Technologies, Inc., founded in 2001, is a private company that is commercializing a new technology for the manufacture of unique substrates, sensors, packaging, hybrid and LTCC circuits and RF components. The company's proprietary High Volume Print-Forming (HVPPF™) technology provides the ability to design and mass-produce complex 3-D circuits and substrates from metals, ceramics, polymers and combinations of these materials.

**Hewlett-Packard** (Palo Alto)

Hewlett-Packard (HP), a leading global provider of computing Internet and Intranet solutions, offers complete end-to-end solutions covering critical infrastructure, security, disaster recovery, data warehousing, and server consolidation. HP's Zero Latency Enterprise architecture, with the continuous availability and linear scalability of the underlying NonStop system, are crucial features in mission-critical areas such as intelligence, defense, and homeland security where integration with existing systems and databases preserves the government's investment in the current IT infrastructure while enhancing its capability by orders of magnitude. The HP Labs worldwide research organization maintains a sizeable team dedicated to IT Security research and draws on the talents of researchers in other areas to improve the robustness and safety of IT infrastructure.

**IBM Almaden Research Center** (San Jose)

IBM's Almaden Research Center is one of eight IBM Research laboratories worldwide. More than 500 researchers work at Almaden to enhance IBM's tradition of scientific and technical leadership through basic and applied research that creates new technologies and brings them rapidly to market. Almaden's research emphasizes areas such as data storage systems, database management, Web technologies and the fundamental physical phenomena that underlie current and future information technologies. A number of Almaden technologies—from cryptographic systems to privacy-preserving databases—can be used to help improve homeland security systems.

**IntelliVision** (San Jose)

IntelliVision has powerful leading-edge technologies that provide video intelligence and automated monitoring solutions. Its patented and unique "self-learning" technologies analyze video in real-time, and automatically identify inconsistencies and abnormalities in an environment. The product modules (or Intelligent Vision Agents): (a) analyze and track abnormal or suspicious behavior; (b) track people or objects in a scene; (c) identify unattended baggage; (d) detect weapons; (e) identify people based on federal databases; (f) eliminate piggybacking/tailgating—a prime cause of failure of access control systems; (g) automate video based monitoring, perimeter, and night-time monitoring; and (h) custom detection based on conditions unique to situation.

Bay Area Corporations...(continued)

**Intevac, Inc.** (Santa Clara)

Intevac is developing revolutionary photonics products that address potentially large commercial and military markets. The Company also produces sophisticated manufacturing equipment used in the manufacture of high technology products and is leveraging its equipment expertise to enable cost-effective production of new photonics products. Intevac's photonics products are high-speed electro-optical devices that detect light with extraordinary sensitivity. The Company's proprietary technology makes possible products such as long-range target identification systems and video cameras with night vision capability. Intevac's equipment products are designed to deposit or modify highly engineered thin-films of material on a variety of substrates. These systems are designed for continuous high volume manufacturing of precision thin-film products such as flat panel displays, magnetic media for hard drives and low-light-level cameras.

**InVision Technologies** (Newark)

InVision Technologies develops, manufactures, markets and supports explosive detection systems based on advanced Computed Tomography (CT) technology for civil aviation security. InVision's wholly-owned subsidiary, Quantum Magnetics, develops weapons, narcotics, explosives and other detection systems based on quadrupole resonance and other proprietary magnetic sensing technologies.

**Inxight** (Sunnyvale)

Inxight, founded in 1997 and spun out from Palo Alto Research Center, is considered one of the world's leading providers of Unstructured Data Management solutions for accessing, analyzing and delivering information in all major languages. Inxight enables organizations to capture, use and reuse the data most important to them. From a dedicated government business unit and an experienced system integrator channel, to R&D and technology resources, Inxight enables its government customers to share and analyze information that is critical to winning the war against terrorism.

**iPIX (Internet Picture Corporation)** (San Ramon)

iPIX patented technology delivers the most comprehensive imaging solutions on the market for use in safety planning, first response, detection, and deterrence. iPIX® holds 17 patents in its two main product lines: Immersive Imaging and Rimfire Imaging. Together, these industry-leading product lines provide an end-to-end infrastructure that captures, processes, hosts, and distributes rich media. iPIX mission-critical Immersive Imaging solutions provide the quickest and easiest way to capture the most data in a single, 360-degree-by-360-degree high-quality image. The 360-degree video solution provides high-quality immersive movies and enables viewers to independently determine their perspectives, while the NetCam solution provides digitally navigable 180-degree-by-360-degree images ideal for surveillance.

Bay Area Corporations...(continued)

**Melior Technologies** (San Francisco)

Melior Technologies is the market-defining application infrastructure software company for next-generation networking technologies. Its flagship product, the Extreme Networking platform (XN), enables agencies and companies to evolve their existing applications from static, inflexible resources to highly responsive, extensible, dynamically networked systems. Unlocking the potential of dynamic networking for enterprise applications and web services, XN provides a powerful, modular infrastructure that exponentially simplifies the integration of system resources, significantly reduces the cost of managing applications, and makes systems that are more agile, productive, and connected than systems using current networking architectures.

**Nanosys, Inc.** (Palo Alto)

Nanosys, Inc. is a rapidly growing advanced technology company, leading the burgeoning nanotechnology industry through the development of nano-enabled systems. These systems incorporate novel and patent-protected nanostructures that integrate functional complexity directly into each individual nanoparticle, enabling the low-cost fabrication of revolutionary high-value, high-performance applications in a broad range of industries from life and physical sciences to information technology and communications to renewable energy and defense. The initial applications of Nanosys' technologies include exquisitely sensitive chemical and biological sensors, high performance large area macroelectronics and lightweight high efficiency conformal photovoltaics.

**Naval Postgraduate School** (Monterey)

The Naval Postgraduate School is the Navy's "corporate" university and exists to enhance the security of the U.S.A. and increase the combat effectiveness of U.S. and Allied Armed Forces. It accomplishes this by providing post-baccalaureate degree and non-degree programs in a variety of sub-specialty areas not available through other educational institutions. It also has a large supporting research program. The student body consists of U.S. officers from all branches of the uniformed services, civilian employees of the federal government, and military officers and government civilian employees of other countries.

**NEC** (Cupertino)

NEC is a worldwide leader in enterprise security management. For decades, it has served the law enforcement market providing biometric matching systems and IT solutions that help to solve crimes and secure our communities. Its fingerprint recognition system is currently installed in over 60% of U.S. law enforcement agencies. NEC is now creating new solutions that meet the increased demands of aviation and airport security. Its SmartCatch Vision is real time Video Intelligence Software that detects, tracks and identifies active and static objects within video streams. It offers real time behavior recognition and analysis, anomaly detection, and automatic alarm verification.

Bay Area Corporations...(continued)

**Network Associates, Inc.** (Santa Clara)

Network Associates, Inc. creates best-of-breed computer security solutions that prevent intrusions on networks and protect computer systems from the next generation of blended attacks and threats. Offering two families of products, McAfee System Protection Solutions, securing desktops and servers, and McAfee Network Protection Solutions, ensuring the protection and performance of the corporate network, Network Associates offers computer security to large enterprises, governments, small and medium sized businesses, and consumers. These two product portfolios incorporate Network Associates leading McAfee, Sniffer and Magic product lines.

**Oracle Corporation** (Redwood City)

For more than 25 years, Oracle Corporation has been a partner to the most important organizations, such as the U.S. Department of Defense, that rely on the company's technologies in protecting the most vital data assets. Oracle has already proved it delivers the necessary solutions to address any organization's homeland security needs through functional and technical expertise; infrastructure technology for information assurance, business continuity and collaboration; specific solutions tailored for the unique needs of the public sector; leadership in national initiatives; and industry-standardized technologies.

**Palo Alto Research Center (PARC)** (Palo Alto)

The Palo Alto Research Center (PARC), a subsidiary of Xerox Corporation, conducts pioneering research in physical, computational, and social sciences. With inventions such as laser printing, Ethernet, the graphical user interface, and ubiquitous computing, PARC has been one of the premier sources of technology leadership and industry vision for more than 30 years. PARC's current research includes areas such as wireless sensor networks, robotics, security, UV light sources for bio-agent detection, and intelligence analysis using advanced linguistic and information visualization technologies. PARC also has one of the world's most highly-regarded programs for information security.

Bay Area Corporations...(continued)

**piXlogic** (Los Altos)

piXlogic has developed breakthrough software that can “see” the logical visual contents of digital images and video. The information is automatically indexed, and repositories of pictures/videos can be searched and organized. The piXlogic software automates processes that today are otherwise performed manually, and makes searching for specific image content easier, faster, cheaper, and more accurate. It automatically identifies the shapes in a picture, and creates a comprehensive and very compact record of the contents of the image. In addition to its search capabilities, the software can also be used to automatically add keyword metadata to images based on visual content. In a live video context, the software can be used to monitor live feeds and trigger events when things of interest to users appear in the field of view. It is also capable of recognizing text in an image/video. piXlogic supports applications in the fields of Digital Asset Management, Security, and Mobile devices.

**RAE Systems** (Sunnyvale)

RAE Systems is a leading provider of “smart sensing” network platforms and a wide range of chemical and radiation hazardous environment sensors that enable first responders, military and government organizations to better respond to terrorist events and hazardous material accidents. RAE Systems’ comprehensive, market-leading technology offering includes single and multiple sensor atmospheric monitors, photoionization detectors, radiation detectors, gas detection tubes, sampling pumps and wirelessly connected gas detection and security monitoring devices. Its monitors are used in civilian and government atmospheric monitoring programs in over 50 countries.

**Ramsesrisk** (San Jose)

Ramsesrisk is an Enterprise Risk Management (ERM) software company specializing in assessing, mitigating and managing risk for organizations. Ramses provides both qualitative and quantitative assessment solutions, particularly analyzing and “scoring” threats and vulnerabilities of an asset as related to the probability of a terrorist attack. Another solution analyzes the strengths and weaknesses of client’s cyber security and offers the technology to create comprehensive, Integrated Risk Management (IRM) best practices. Ramsesrisk is a wholly owned subsidiary of Visuale, Inc.

**Recognition Systems, Inc. (An Ingersoll Rand Business)** (Campbell)

Recognition Systems, Inc., (RSI) a division of Ingersoll-Rand, is the world’s leading supplier of Biometric access control, time and attendance, and personal identification products. The Recognition Systems HandReaders verify a person’s identity in less than one second, based on the unique size and shape of the hand. Installations include San Francisco International Airport where, since 1991, their 18,000 employees have used Hand Readers to gain access to the entire airfield. At Ben Gurion International Airport in Israel over two million passengers have used RSI technology to speed through immigration.

Bay Area Corporations...(continued)

**Sanctum, Inc.** (Santa Clara)

Founded in 1997, Sanctum, Inc. is the recognized leader for Web application security solutions. Sanctum software solutions provide automatic enforcement of intended business processes, ensuring the protection of core information and data. By detecting and defending against any unauthorized behavior, Sanctum protects customers against malicious cybercriminal activity—from theft of intellectual property and customer data, to e-commerce fraud and Web site defacement—even if a site has unknown security holes or flaws. Sanctum’s solutions complete an organization’s security infrastructure, assure regulatory compliance and create sustainable ROI. Sanctum’s customers include industry leaders in finance, retailing, healthcare, government and telecommunications.

**Silicon Graphics Inc. (SGI)** (Mountain View)

Silicon Graphics, the world leader in computer graphics systems technologies, has developed a variety of Immersive Visualization and Visual Area Networking technologies ideally suited to allow officials to rapidly assimilate the growing and diverse amounts of data regarding security threats that is being collected, and turn this data into information in support of rapid decision-making. With Visual Area Networking, the right visual information can be sent to the right person at the right time.

**SocialTech, Inc.** (Burlingame)

SocialTech, a nonprofit organization, has built the nation’s largest authority-based alert system linking nearly 2,000 law enforcement agencies at the federal, state, county, and local levels. By integrating the resources of industry, philanthropy, and government, a shared solution linking multiple independent authorities is achieved. The solution is deeply rooted at the community level to build a deeply populated address book of alert recipients and high daily use and value for all authorities. Technology partners Unisys and Microsoft provide the necessary scalability, reliability, security, and interoperability for a national alert solution.

**Vasona Technology, Inc.** (Los Altos)

Vasona Technology is a women owned and operated digital signage company, focused primarily on the homeland security market. Vasona’s objective is to deploy a digital messaging network to provide timely and accurate information in times of crisis or emergency. Vasona’s solution, PASS<sup>®</sup>, an “Intelligent Public Alert System,” facilitates rapid and orderly communication of security information, directions, or evacuation procedures during emergency situations at airports and transportation centers, hospitals, corporate campuses, and other public facilities. The system can operate as a single location or vast networks across geographic areas containing hundreds of locations.



Bay Area Corporations...(continued)

**VaxGen, Inc.** (Brisbane)

VaxGen, Inc. is a biopharmaceutical company engaged in the development, manufacture and commercialization of biologic products for the prevention and treatment of human infectious disease. The company is developing preventive vaccines against anthrax, smallpox and HIV.

VaxGen has been funded by the National Institute of Allergy and Infectious Diseases (NIAID), a part of the National Institutes of Health (NIH), to develop a modern, recombinant anthrax vaccine (rPA) and to create a feasibility plan to manufacture an emergency stockpile of 25 million doses. Under an agreement with the Chemo-Sero Therapeutic Research Institute (Kaketsuken) of Japan, VaxGen has begun development of a potentially safer smallpox vaccine. VaxGen is also the largest shareholder in Celltrion, Inc., a joint venture formed to build biopharmaceutical manufacturing operations.

**VeriSign, Inc.** (Mountain View)

VeriSign is the leading provider of digital trust services enabling commerce and communication with confidence. VeriSign's digital trust services create a trusted environment through four core offerings— Web presence services, security services, payment services, and telecommunications services—powered by a global infrastructure that manages more than five billion network connections and transactions a day. VeriSign provides exceptional cybersecurity services through its Managed Security Services, Managed DNS and Managed PKI services.

**Visuale** (San Jose)

Visuale is an integrated, Internet based Business Process Management (BPMS) software company specializing in creating “Best Practices Business Processes” without programming. Software solutions are built dynamically by Visuale's software platform by evaluating the visual model of the business situation requiring solution. Visuale offers an integrated and comprehensive security model for access control, escalation and event notification, including Biometrics. The technology allows the integration and extension of existing IT solutions, increasing ROI on prior IT investments. In the present climate of “new uncertainties,” processes must align IT with operations and also be agile.

## **APPENDIX B**

### **BAY AREA LEADING RESEARCH UNIVERSITIES**

#### **Stanford University**

Stanford is a premier research university, with programs exploring the frontiers of knowledge in physics, chemistry, biology, medicine, engineering, earth sciences, math, computational sciences and other fields. Founded more than 100 years ago, Stanford has 14,000 undergraduate and graduate students and 10,000 faculty and staff members, all of whom help the university fulfill its mission of teaching, learning and research.

#### **University of California, Berkeley**

The University of California, Berkeley, founded in 1868, enjoys an international reputation for excellence in research. Its achievements are reflected in its extraordinary impact on the Bay Area, the State of California, the nation and the world in a broad range of areas from biotechnology to computer technologies. Its five colleges and nine professional schools enroll over 33,000 students in more than 100 academic departments and interdepartmental groups. According to the National Research Council, Berkeley ranks first nationally in the number of graduate programs in the top 10 in their fields.

#### **University of California, Davis**

University of California, Davis, is particularly noted for its strengths in biology, agricultural and environmental sciences, human and animal health and biotechnology. It also has well-recognized and growing programs in areas such as nanoscience, computer security, neuroscience, transportation and biomedical engineering. Its School of Veterinary Medicine is the largest in the nation and the only one in the UC system. UC Davis manages a number of research facilities including the California National Primate Research Center, the Bodega Marine Laboratory and the McClellan Nuclear Radiation Center. It enrolls over 29,000 undergraduate and graduate students and has almost 26,000 faculty and staff.

#### **University of California, San Francisco**

The University of California, San Francisco, is one of the world's premier institutions in the health sciences—distinguished for biomedical research, education of health care professionals, and advancement of new techniques to diagnose and treat disease. UCSF is the only campus in the 10-campus UC system devoted exclusively to the health sciences. Based on the importance of its research achievements, UCSF continues to be one of the prime recipients of national research funding.

Bay Area Leading Research Universities (continued)

**University of California, Santa Cruz**

Enrolling students since 1965, UC Santa Cruz emphasizes undergraduate and graduate education enhanced by leading-edge research. Particularly distinguished are programs related to the Jack Baskin School of Engineering, the Center for Ocean Health, the National Center for Adaptive Optics, and the Santa Cruz Institute for Particle Physics. UC Santa Cruz is ranked No. 1 for research impact in astrophysics among the top 100 federally funded U.S. universities, and No. 2 worldwide for research impact in the physical sciences.

## **APPENDIX C**

### **BAY AREA NATIONAL RESEARCH LABORATORIES AND INDEPENDENT RESEARCH INSTITUTIONS**

#### **National Research Laboratories**

##### **NASA Ames Research Center**

Ames Research Center, one of ten field installations of the National Aeronautics and Space Administration, is located in the heart of California's Silicon Valley at the core of the research cluster of high-tech companies, universities and laboratories that define the region's character. With over \$3 billion in capital equipment, 3,500 research personnel and a \$700 million annual budget, Ames' economic impact is significant. Ames plays a critical role in virtually all NASA missions in support of America's space and aeronautics programs. As a leader in information technology research with a focus on supercomputing, networking and intelligent systems, Ames conducts the critical R&D and develops the enabling technologies that make NASA missions possible. Ames works collaboratively with the FAA, conducting research in air traffic management to make safer, cheaper and more efficient air travel a reality. Ames' research in astrobiology focuses on the effects of gravity on living things, and the nature and distribution of stars, planets and life in the universe. Ames is also a leader in nanotechnology, fundamental space biology, biotechnology, aerospace and thermal protection systems, and human factors research. The center conducts information and education outreach, forms collaborative partnerships and fosters commercial application of NASA technologies. Ames is developing NASA Research Park and, in the future, will be home to the California Air and Space Center, a showcase for 21st century, hands-on, interactive education and learning.

##### **Ernest Orlando Lawrence Berkeley National Laboratory (Berkeley Lab)**

Berkeley Lab, an unclassified Department of Energy facility managed by the University of California, has the core mission to provide national scientific leadership and technological innovation, including performing leading multi-disciplinary research in the energy sciences, high performance computing, environment, advanced materials, nanotechnology, physics, and biosciences.

##### **Lawrence Livermore National Laboratory (LLNL)**

LLNL is a Department of Energy national laboratory managed by the University of California. Its mission is to apply science and technology in the national interest, with a focus on stockpile stewardship, nonproliferation and counterterrorism, energy and environment, and bioscience.

## National Research Laboratories (continued)

### **Sandia National Laboratories**

Sandia National Laboratories is the largest federal research and development laboratory in the U.S. With major facilities in Albuquerque, NM, Livermore, CA, Tonopah, NV and Kauai, HI, Sandia's principal missions are in national defense, homeland security, energy technologies, and support to the Department of Defense and the intelligence community. Sandia pursues "science with the mission in mind" and has strong capabilities in the physical, engineering, and computational sciences and most recently in biotechnology. Sandia is a National Nuclear Security Administration lab managed by Lockheed Martin Corp.

### **Stanford Linear Accelerator Center (SLAC)**

The Stanford Linear Accelerator Center is a national laboratory operated by Stanford University on behalf of the U.S. Department of Energy. Its mission is to design, construct and operate state-of-the-art electron accelerators and related experimental facilities for use in high energy physics and synchrotron radiation research.

## **Independent Research Institutions**

### **Buck Institute for Age Research**

The Buck Institute for Age Research, a nonprofit, independent research institute completed phase one of construction and opened its research facility and first laboratory in 1999. When completed, the Institute, located on a 488-acre site in Novato, Marin County, and designed by the renowned architect, I. M. Pei, will consist of four laboratories and a support and educational facility covering 355,000 square feet. The primary scientific focus of the Institute will be the major neurodegenerative diseases which most affect persons of advanced age.

### **Electric Power Research Institute (EPRI)**

The Electric Power Research Institute (EPRI), headquartered in Palo Alto, California, was established in 1973 as a non-profit center for public interest energy and environmental research. EPRI's collaborative science and technology development program now spans nearly every area of power generation, delivery and use. More than 1,000 energy organizations and public institutions in 40 countries draw on EPRI's global network of technical and business expertise.

### **Monterey Bay Aquarium Research Institute (MBARI)**

The Monterey Bay Aquarium Research Institute (MBARI) was founded in 1987 by David Packard. The mission of MBARI is to achieve and maintain a position as a world center for advanced research and education in ocean science and technology, and to do so through the development of better instruments, systems, and methods for scientific research in the deep waters of the ocean.

### **SRI International**

SRI International is one of the world's leading independent, non-profit research and technology development organizations. Founded as the Stanford Research Institute in 1946, SRI is known for its innovations in information technology, communications, engineering, pharmaceuticals, biotechnology, chemistry, physics, and for research in the public policy areas of education, health, and economic development. For decades SRI has conducted basic research and development in a range of areas that support the nation's defense and intelligence needs, including new energy sources, advanced materials, signal processing, and innovative tactical training systems. SRI has pioneered network security, intrusion detection, information extraction, planning and reasoning systems, image processing, the next generation of computer science, artificial intelligence, systems design, speech recognition, and other forms of human-computer interaction.



## **APPENDIX D**

### **BAY AREA NEW RESEARCH COMPLEXES**

#### **Mission Bay and UCSF Mission Bay (San Francisco)**

UC San Francisco's new 43-acre life sciences campus will be a premier center of scientific discovery and for teaching and research into improving human health. UCSF Mission Bay, located near downtown San Francisco is the focal point of the 303-acre Mission Bay biotechnology development by the Catellus Development Corporation.

The new campus is an addition to a network of UCSF locations. The Mission Bay campus will allow UCSF to double its research space, speed the pace of biomedical discovery, and help prepare a new generation of students.

The first building at UCSF Mission Bay opened in January 2003 when 900 faculty and staff moved into Genentech Hall. Genentech Hall houses programs in structural and chemical biology, as well as the Molecular Design Institute and the Center for Advanced Technology. Another research facility is scheduled for occupancy in fall of 2003 for programs in neuroscience, developmental biology, and genetics. In 2004, a Community Center and headquarters building for the California Institute for Quantitative Biomedical Research (QB3) are expected to be completed. The campus will continue to be built in phases over the next 15 years, leading to 20 structures and a population of 9,100 at full build-out projected for 2020.

UCSF Mission Bay is the anchor of the greater Mission Bay project. The overall project is expected to include a technology zone of biotechnology, applied life science, and pharmaceutical businesses surrounding the UCSF campus.



## Bay Area New Research Complexes (continued)

### **NASA Research Park (Moffett Field)**

The 213-acre NASA Research Park (NRP) will be a dynamic world-class shared-use campus developed by NASA Ames Research Center in collaboration with academia, industry and nonprofit organizations with shared goals in support of NASA's mission. Within the NRP, new laboratories, offices, classrooms, auditoriums, museums, a training and conference center, open space, a burrowing owl preserve and limited retail facilities are being planned.

Major partners currently involved in the NRP endeavor include: The University of California, Santa Cruz; Carnegie Mellon University; San Jose State University; Foothill-De Anza Community College District; California Air and Space; National Association for Equal Opportunity in Higher Education (NAFEO); Women In Science, Technology, Engineering, and Mathematics (WiSTEM); Girvan Institute of Technology and the Space Technology Center.

By pursuing strategic collaborative research partnerships within the disciplines of astrobiology, biotechnology, information technology and nanotechnology, NASA Ames Research Center will be even better positioned to provide research leadership well into the 21st century.

### **UCSC Silicon Valley Center**

Located in the NASA Research Park, the Silicon Valley Center is operated on behalf of the UC System by its Santa Cruz Campus. Its mission is to develop collaborative programs with NASA Ames, serve as a portal into the research capabilities of the UC System for NASA's research programs and become, over time, a major Ames' source of outside research expertise. In addition, the Silicon Valley Center serves as a planing center for the development of a proposed 2,000 student educational and research center in the NASA Research Park directly focused on the needs of Silicon Valley.

## APPENDIX E

### AUTHORS OF SECTION I ESSAYS

#### *William A. Barletta, PhD*

Dr. Barletta is Director of the Accelerator and Fusion Research Division at the Lawrence Berkeley National Laboratory. He is responsible for a large and varied program of research in accelerator physics and related technologies supporting High Energy Physics, the Advanced Light Source, Heavy Ion Inertial Fusion, and Ion Beam Technologies. He also serves as LBNL's Director of Homeland Security and Non-Proliferation.

Dr. Barletta is an Editor of Nuclear Instruments and Methods A, Chairman of the Board of Governors of the US Particle Accelerator School, Member of the Governing Board of the Virtual National Laboratory for Heavy Ion Fusion, Member of the Steering Committee of the US-LHC Accelerator Collaboration and of the Very Large Hadron Collider Collaboration, and Member of the Executive Committee of the Division of Physics of Beams of the American Physical Society. His recent research has concentrated on high energy colliders, ultra-short pulse X-ray sources, high gain free electron lasers, and generation and application of neutron sources and bright ion beams to nanotechnology.

Prior to joining the Berkeley Lab in 1993, Dr. Barletta was Assistant Laboratory Associate Director for Programs at the Lawrence Livermore National Laboratory (LLNL), a Visiting Professor of Physics at UCLA, and an Instructor of Physics at Yale University.

Dr. Barletta received a BSEE with Highest Distinction from the University of Rhode Island. He was a Woodrow Wilson scholar and a Research Assistant at the Enrico Fermi Institute of the University of Chicago, where he received a MS and PhD in high energy physics.

Authors of Section I Essays (continued)

***Frances Edwards-Winslow, PhD***

Dr. Edwards-Winslow has served as Director of the Office of Emergency Services in San Jose for eleven years, including one year as Acting Assistant Chief in the San Jose Fire Department. She also is Director of San Jose's Metropolitan Medical Task Force (MMTF), a terrorism response unit that includes police, fire and medical personnel, and she holds the designation of Certified Emergency Manager (CEM), earned through a program sponsored by FEMA and the International Association of Emergency Managers.

Dr. Edwards-Winslow was named Public Official of the Year 2002 by *Governing Magazine*. She represented emergency management on the five-night "Bio-War" series on ABC's "Nightline with Ted Koppel" in October, 1999.

She is a member of the Stanford University Working Group on Chemical and Biological Warfare, the Executive Session on Domestic Preparedness at the Kennedy School of Government at Harvard University, the National Academy of Sciences Institute of Medicine MMTF review committee, and the US-Germany Counterterrorism Project.

She has written a chapter in *First to Respond*, to be published by MIT Press in 2003, has written two chapters and co-authored a third in the *Handbook of Crisis and Disaster Management*, published by Marcel Dekker in 2001, and has written a chapter in *The New Terror*, published by Stanford University Press in 1999. She is a columnist for the American Society for Public Administration's OnLine Newsletter, and her invited commentary on the events of 9-11 was published in the *Public Administration Times* and widely reprinted.

Dr. Edwards-Winslow has a PhD in public administration, and a Certificate in Hazardous Materials Management.

Authors of Section I Essays (continued)

***Peter Friedland, PhD***

Dr. Friedland is the Assistant Director for Technology at NASA's Ames Research Center. He received undergraduate degrees in Electrical Engineering and Chemistry from Princeton University in 1974 and his PhD in Computer Science from Stanford University in 1979.

While a graduate student and a Senior Research Scientist at Stanford, he was part of the group that invented expert systems; his own specialty was the application of artificial intelligence to problems in molecular biology. During this time he also co-founded the first bio-informatics company, Intelligenetics, and one of the first expert systems companies, Teknowledge. From 1987 until 1995, Friedland worked at NASA Ames, founding and managing NASA's first intelligent systems R&D laboratory. This group achieved international recognition both for its contributions to fundamental computer science and for its direct applications to NASA missions. These included an expert scheduling system for use in coordinating the human and materiel resources used to process Space Shuttle Orbiters at Kennedy Space Center, the first PC-based astronaut assistant tool to fly in space, and a wide variety of tools to assist in the process of scientific data analysis.

In 1995, Dr. Friedland left Ames to found and manage Intraspect Software, a company that was soon among the market leaders in the growing field of knowledge management and collaboration technology. In 2003, he rejoined Ames in his current position.

Authors of Section I Essays (continued)

***Nicholas Imparato, PhD***

Dr. Imparato is a Professor of Management and Marketing, University of San Francisco and a Research Fellow, Hoover Institution, Stanford University. He received his BA from St. Bonaventure University and PhD at Bowling Green State University.

Dr. Imparato has authored, co-authored and edited numerous publications dealing with the interplay between public policy and business strategy, as well as with broad management issues (such as innovation and change, leadership and revenue growth). He served as a contributing editor for *Intelligent Enterprise* magazine and wrote its national “Business Impact” column from 1998 to 2003. Currently, he is a frequent contributor to *Security Technology and Design* and other security oriented magazines with articles focusing on technology developments, industry trends and public policy.

Dr. Imparato has served as a member of the Board of Directors of both public and closely held companies. Currently, he is a member of the Board of Advisors of several Silicon Valley firms and consults across a range of industries.

His extensive international experience includes engagements in the Middle East, Eastern Europe, Asia, the European Union and South America.

Dr. Imparato was honored in 1995 with the Tops in Marketing Award, Sales and Marketing Executives International, a recognition normally given to CEOs of prominent Fortune 500 firms. In 2001 he was given special recognition by the Bishop Gassis Sudan Relief Fund (formerly the Sudan Relief and Rescue Fund), Washington D.C., for “raising the awareness of the plight of the people of Sudan.”

Dr. Imparato serves as a co-leader of the BASIC Homeland Security Team.

Authors of Section I Essays (continued)

***Sunne Wright McPeak***

Ms. McPeak has been President and CEO of the Bay Area Council since 1996. The Bay Area Council is a non-profit regional organization representing more than 275 of the Bay Area's major employers. The mission of the Council is to continually strengthen the economy and improve quality of life in the nine-county Bay Area. Ms. McPeak is a respected and sought out authority on a wide variety of social and economic issues in the Bay Area.

Prior to the Bay Area Council, Ms. McPeak served as the president of the Bay Area Economic Forum where, among other efforts, she helped lead the Bay Area Defense Conversion Action Team (BADCAT), a partnership dedicated to converting the numerous closed military bases in the Bay Area. Prior to taking on the leadership of regional organizations, Ms. McPeak served a total of 15 years as a member of the Contra Costa County Board of Supervisors.

Vigorously active in public service, Ms. McPeak chairs or serves on the board of numerous public and private organizations. She is one of five Directors of the California Consumer Power and Conservation Financing Authority (California Power Authority). The *San Francisco Business Times* named her one of the 100 Most Influential Women in Business in 1998, 1999, 2000, 2001, 2002 and 2003. She was named a "Women Who Could be President" honoree in 1997 by the League of Women Voters of San Francisco.

Ms. McPeak is a graduate of the University of California, Santa Barbara and holds a Master of Public Health degree from the University of California, Berkeley.

Authors of Section I Essays (continued)

***Joseph N. Miniace***

Mr. Miniace is President and Chief Executive Officer of the Pacific Maritime Association (PMA), with headquarters in San Francisco. He has over 30 years of experience in labor relations and human resources in the transportation and health care industries.

As President of PMA, Mr. Miniace directs the association's principal business activity, negotiating and administering maritime labor agreements with the International Longshore and Warehouse Union (ILWU) on the West Coast of the United States.

Mr. Miniace serves as Vice-Chairman of MARAD's Marine Transportation System National Advisory Council, is an Advisory Panel Member of Stanford Law School's International Labor Studies Project and is a member of the Board of Directors of the California Chamber of Commerce, the Bay Area Council, and the Bay Area Economic Forum.

Mr. Miniace began his career in the transportation industry labor relations in 1967 at Ford Motor Company, having responsibility for the total labor relations and human resource activity in the 5,200-person unionized manufacturing unit. He was part of Ford's initiation of an exemplary partnership with the United Auto Workers (UAW), a partnership that is an ongoing model for labor relations throughout the country.

Mr. Miniace was a member of the White House Advance Staff under President Ford and has served as adjunct professor at three major universities. Mr. Miniace holds a BA degree from Creighton University in Omaha, Nebraska, and an MS in business management from New York University.

Authors of Section I Essays (continued)

***Robert J. T. Morris, PhD***

Dr. Morris is the Director of the IBM Almaden Research Center in San Jose, California. At this lab he oversees more than 500 scientists and engineers doing exploratory and applied research in hardware and software areas, such as nanotechnology, materials science, storage systems, data management, Web technologies and user interfaces. Dr. Morris is also vice president for personal systems research, guiding the direction of IBM's worldwide research in this area. A computer scientist, he has more than 20 years experience in the IT industry.

In 2002, Dr. Morris was named chairman of the Bay Area Science and Innovation Consortium, a collaboration of the region's major research universities, national laboratories, independent research institutions, and research and development-driven businesses.

Dr. Morris also represents IBM on the Government University Industry Research Roundtable, which is sponsored by the National Academies. He is a member of the IBM Academy of Technology and a Fellow of the IEEE. Dr. Morris was an editor of the IEEE Transactions on Computers from 1986–1991. He twice served as vice-chair for the International Conference on Distributed Computer Systems and has served on advisory boards for several universities. He has published more than 50 articles in computer science, electrical engineering and mathematics literature, and has received 11 patents.

Dr. Morris holds a PhD in computer science from the University of California at Los Angeles.



Authors of Section I Essays (continued)

***Jeanne B. Perkins***

Jeanne Perkins is the Earthquake Program Manager for the Association of Bay Area Governments (ABAG). Ms. Perkins has served as the principal investigator for several research projects focusing on earthquake preparedness issues in the Bay Area and funded by the National Science Foundation, the U.S. Geological Survey, Caltrans, the California Office of Emergency Services and others.

Ms. Perkins has produced ground shaking and liquefaction maps showing the earthquake hazard in the San Francisco Bay Area. She also is involved in a number of projects looking at the impacts of earthquakes on housing, as well as how homeowners can improve the safety of their homes. Other recent projects involve looking at the impacts of earthquakes on highways, roads, and airports, as well as speeding up the recovery of our transportation system following future earthquakes and other disasters.

Authors of Section I Essays (continued)

***Joe Raguso***

Mr. Raguso is Vice President of Strategic Partnerships at SRI International, a leading independent research institute based in Silicon Valley.

Prior to joining SRI International, Mr. Raguso served as California's Deputy Secretary of Science, Technology and Innovation, and managed a division of the Technology, Trade, and Commerce Agency that acted as the critical information epicenter for technology policy in California state government, advising both the Governor and the Legislature on issues critical to California's economy and quality of life. At the federal level, Raguso served in the Clinton Administration as a Deputy Assistant Secretary of the Office of Technology Policy.

Mr. Raguso has served as President and CEO of the San Diego Regional Technology Alliance (SDRTA), where he worked to grow and finance new technology companies in the San Diego region. Mr. Raguso also served in the Office of Science and Technology Policy and Projects at the University of California, San Diego (UCSD) where he developed strategic partnerships with private industry and federal agencies to advance the research goals of UCSD and the region's growing technology-dependent economy.

As a scientist and engineer, Mr. Raguso has worked for IBM and Galileo Electro-Optics Corporation. His educational background includes a Master's degree in Technology and Policy from Massachusetts Institute of Technology and graduate and undergraduate degrees in engineering.

Authors of Section I Essays (continued)

***Ronald E. Stoltz, PhD***

Dr. Stoltz is a graduate of MIT with a PhD in Material Science and Engineering. He was awarded a French Office of Foreign Affairs Fellowship and a Fellowship at the National Science Foundation, where he continued his research following his PhD.

Dr. Stoltz' early research work focused on failure modes in modern aircraft and environmental effects on materials, and eventually on the integration of advanced manufacturing techniques in military hardware.

During his 25 years with Sandia National Laboratories, Dr. Stoltz has managed basic and applied research, developed programs in the design of materials and coating, and was instrumental in establishing Sandia's Integrated Manufacturing Technology Laboratory. He also has served as a corporate program manager for Sandia's nuclear weapons business unit.

He has been a member of the Advisory Committee to the School of Engineering at Chico State University, has served on the Technical Board of the Los Angeles California Manufacturing Extension Center and on the board of Manex (the NIST manufacturing extension center in Northern California), and he currently serves on the board of the East Bay's Economic Development Alliance for Business.

Dr. Stoltz also has a Minor in Political Science/Public Policy. For the past six years he has managed the Congressional Relations function at Sandia's branch laboratory in Livermore, CA. He has dealt with issues of foreign involvement in the microelectronics industry, with technology and policy issues involved in advanced deterrence systems, and most recently with the start-up of the Department of Homeland Security. Dr. Stoltz has worked with the Bay Area Economic Forum BASIC project almost since its inception.

Authors of Section I Essays (continued)

***Jay Stowsky, PhD***

Dr. Jay Stowsky is Executive Director of the UC Berkeley project on Information Technology and Homeland Security (ITHS), based at the Goldman School of Public Policy, and is Co-Director of Research at the Berkeley Roundtable on the International Economy (BRIE), also at UC Berkeley.

Previously, Dr. Stowsky served as Associate Dean at UC Berkeley's Haas School of Business and Director of Research Policy for the University of California system, a position that oversees research relationships between the UC campuses and the three UC-managed Department of Energy national laboratories.

Prior to joining UC, Dr. Stowsky served in the Clinton Administration as Senior Economist for Science and Technology Policy on the staff of the White House Council of Economic Advisers (CEA) and as the CEA's Interim Chief of Staff.

Dr. Stowsky has authored several studies of U.S. technology policy, including "Secrets to Share or Shield: New Dilemmas for Military R&D in the Digital Age." His research interests include national innovation systems, comparative science and technology policy, economic geography, and the commercial impact of military research and development, as well as public-sector management.

Dr. Stowsky received his undergraduate degree and PhD from UC Berkeley and has a Master's in Public Policy from Harvard.

Authors of Section I Essays (continued)

***Roger W. Werne, PhD***

Since 1999 Dr. Werne has been Chief Engineer for the NAI Directorate, being responsible for strategic technology development and overseeing the quality management and project engineering needs associated with the proliferation prevention and mitigation of weapons of mass destruction(WMD).

In 1995, Dr. Werne co-founded ITI Medical Technologies, a medical device start-up company focused in the field of Magnetic Resonance Image(MRI) guided surgery, a new minimally invasive surgical paradigm. Under Dr. Werne's leadership, ITI developed, marketed and sold, an innovative, FDA approved, line of surgical instruments and developed six patents.

Prior to joining ITI, Dr. Werne was Associate Director for Engineering and Technology Transfer at LLNL. He was responsible for an organization of approximately 2,500 people that supported virtually all Laboratory Programs including nuclear weapons, nonproliferation and arms control, advanced conventional defense, inertial confinement and magnetic fusion, energy, transportation, advanced manufacturing, and biotechnology.

Dr. Werne received his PhD in Solid Mechanics from the University of California at Berkeley and has been associated with LLNL for over 30 years. He is a Fellow of the American Society of Mechanical Engineers, a member of the UC External Advisory Committee for the Engineering Sciences and Applications Division at Los Alamos National Laboratory, and a consultant to several private companies in the field of instruments for MRI guided surgery.

## **APPENDIX F**

**BASIC gratefully acknowledges the financial contribution of Reed Smith Crosby Heafey supporting the production of this report.**

### *Reed Smith Crosby Heafey*

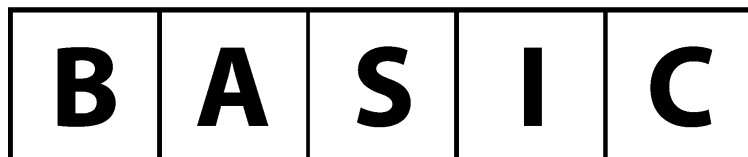
Reed Smith Crosby Heafey's Homeland Security practice group has assembled an interdisciplinary team of professionals whose purpose is to conduct vulnerability assessments and minimize risk for private sector companies and public sector organizations. Leaders of these organizations owe a duty of care to protect their people and organizations against the potential direct or indirect impact any terrorist act might have upon their operations. Risk assessment, risk management, risk mitigation, disaster recovery, and continuity planning—usually practiced in the event of natural disaster—are now more urgent assignments, given the specter of intentional acts of terror aimed at disrupting commerce and society. These concerns are of especial importance for leaders who face personal legal exposure for failure to plan for the worst eventualities.

Focused on two distinct sets of issues—(1) personal liability of officers, directors and organizational leaders in the private and public sectors; and (2) the cost-effectiveness of current and future risk-avoidance measures—this team has developed procedures that allow private and public sector leaders to undertake risk assessment, risk avoidance, and continuity planning under the protection of confidential attorney-client privilege.

Currently, there are few if any adequate protections for keeping the findings or decisions regarding these efforts confidential. The team's approach addresses this shortcoming by attempting to allow these leaders to undertake risk assessment, risk avoidance, and continuity planning in a confidential setting not otherwise available under existing law. To the extent that this process involves communications by and between clients and Reed Smith and its expert and consultant team members, made for the purposes of securing or delivering legal advice, these communications may be protected under the attorney-client privilege subject to the restrictions and limitations of applicable law.



## APPENDIX G



### BAY AREA SCIENCE AND INNOVATION CONSORTIUM

#### BOARD OF DIRECTORS

##### *Chairman*

**Dr. Robert J. T. Morris**, Director, IBM Almaden Research Center

**Dr. Michael R. Anastasio**, Director, Lawrence Livermore National Laboratory

**Dr. Michael Arbige**, Chairman, Bay Area Bioscience Center;  
Senior VP for Technology, Genencor International

**Mr. Samuel H. Armacost**, Chairman of the Board, SRI International

**Dr. Robert M. Berdahl**, Chancellor, UC Berkeley

**Mr. G. Steven Burrill**, Chief Executive Officer, Burrill & Company

**Mr. Keith Carson**, Chairman, Economic Development Alliance for Business (EDAB)

**Chancellor M.R.C. Greenwood**, UC Santa Cruz

**Mr. G. Scott Hubbard**, Director, NASA Ames Research Center

**Dr. Miriam John**, Vice President, Sandia California National Laboratories

**Dr. Regis Kelly**, Executive Vice Chancellor, Research, UC San Francisco

**Dr. C. Judson King**, Provost and Senior Vice President of Academic Affairs,  
UC Office of the President

**Dr. Charles Kruger**, Vice Provost & Dean of Research & Graduate Policy,  
Stanford University

**Mr. Dick Lampman**, Senior Vice President Research,  
Director, Hewlett-Packard Laboratories

**Mr. Lenny Mendonca**, Chairman, McKinsey Global Institute

**Mr. Aram M. Mika**, Vice President, Advanced Technology Center,  
Lockheed Martin Missiles & Space

**Dr. Robert T. Parry**, President & CEO, Federal Reserve Bank of San Francisco

**Mr. George Scalise**, President, Semiconductor Industry Association

**Dr. Charles V. Shank**, Director,  
Ernest Orlando Lawrence Berkeley National Laboratory

**Dr. Larry N. Vanderhoef**, Chancellor, UC Davis

##### **Planning Committee Leader**

**Mr. William E. Berry**, Deputy Director, UC Silicon Valley Center







**BAY AREA SCIENCE AND INNOVATION CONSORTIUM**

**200 Pine Street, Suite 300  
San Francisco, CA 94104  
Phone: (415) 981-7117  
Fax: (415) 981-6408  
Email: [basic@bayeconfor.org](mailto:basic@bayeconfor.org)  
[www.bayeconfor.org/BASIC](http://www.bayeconfor.org/BASIC)**