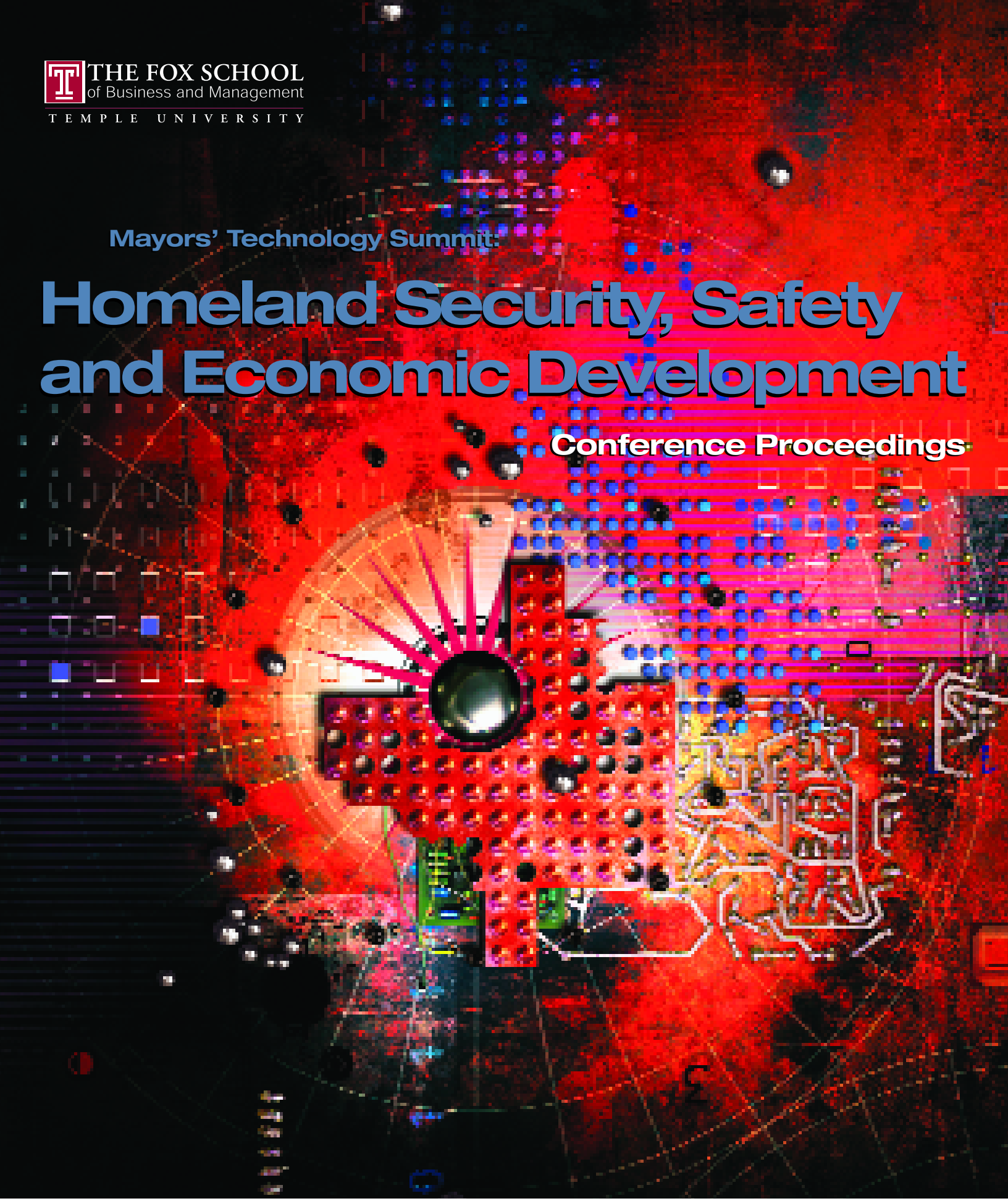
THE FOX SCHOOL
of Business and Management
TEMPLE UNIVERSITY

Mayors' Technology Summit:

Homeland Security, Safety and Economic Development

Conference Proceedings



Sponsor and Host

Center For Competitive Government
THE FOX SCHOOL of Business and Management
TEMPLE UNIVERSITY

Principal Underwriters

Battelle
The Business of Innovation

ciber
ALWAYS ABLE

Cisco Systems

HANSEN

Underwriters

INTERGRAPH

Mayors' Technology Summit:

Homeland Security, Safety, and Economic Development

Conference Venues

San Francisco, California
July 17–18, 2003

Sponsored by

The Center for Competitive Government

The Fox School of Business and Management, Temple University

The City of San Francisco, Office of the Mayor

Hosted by

The City of San Francisco
Willie L. Brown, Jr., Mayor

Principal Underwriters

Battelle

Ciber

Cisco Systems

Hansen

SBC, Inc.

Underwriters

Bechtel

Intergraph Corporation

Voyager Systems

Table of Contents

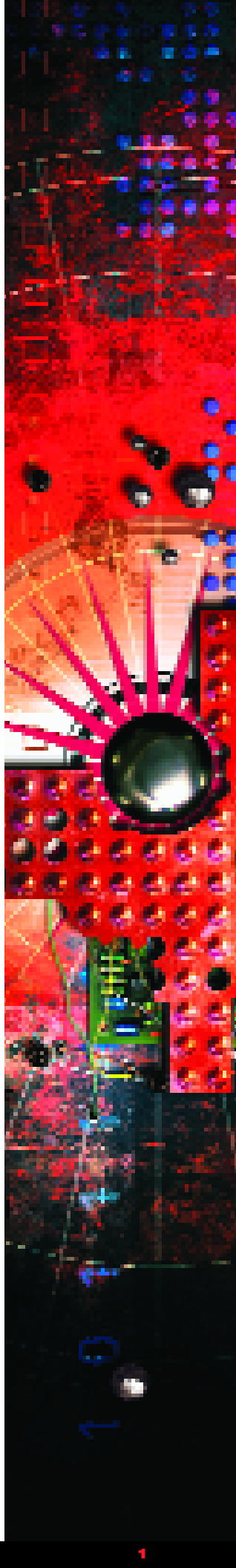


Table of Contents (continued)

The Fox School of Business and Management *Temple University*

Established in 1918, The Fox School has a distinguished tradition of preparing business leaders, professionals and entrepreneurs for successful careers. Today, it is the largest, most comprehensive business school in the Greater Philadelphia region and among the largest in the world, with over 5,500 students, over 150 full-time faculty and 42,000 alumni.

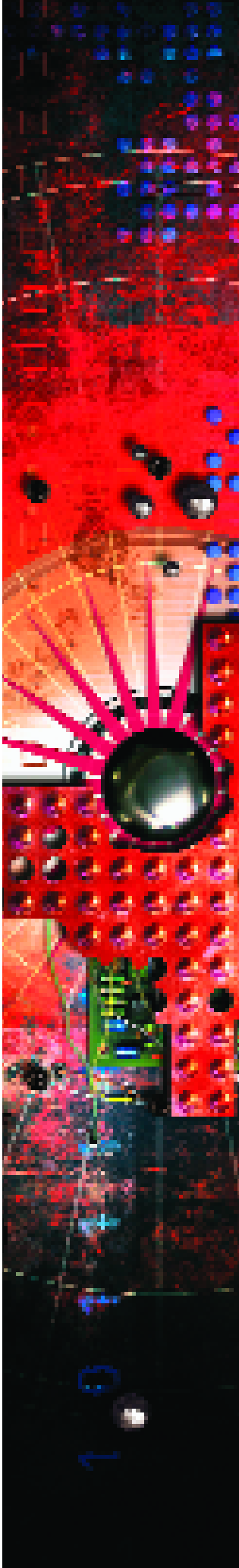
Accredited by AACSB International — the Association to Advance Collegiate Schools of Business — The Fox School offers BBA, MBA, Executive MBA, International MBA, MBA/MS, MA, MS, and PhD programs on campuses throughout the region and around the world. The Fox School's programs continue to be ranked internationally and nationally by leading business publications and organizations, such as *Computerworld*, *Financial Times*, *Forbes*, *U.S. News & World Report* and the Eastern Technology Council.

The Fox School is thoroughly committed to providing a student-centered education and professional development relevant to today's digital, global economy. That commitment is reflected in its integration of technology into the curriculum and classroom and in its encouragement of entrepreneurship and innovation in business and education. It's also evidenced by Fox's global presence and perspective with international programs such as an Executive MBA program in Tokyo; a three-continent International MBA program in Paris, Philadelphia, Tokyo and Mumbai (Bombay); the International Business program in Rome; and foreign executive training programs in China, India, Japan, Israel, Ukraine and other centers of international business and commerce throughout the world.

Supporting and enriching The Fox School's academic programs are research and outreach institutes and centers such as The Irwin L. Gross eBusiness Institute, Institute of Global Management Studies, Innovation and Entrepreneurship Institute, Advanta Center for Financial Services Studies, Center for Healthcare and Research Management, Center for Labor and Human Resource Studies, Small Business Development Center, and the Center for Competitie Government who organized this summit and brought together so many distinguished mayors, executives, and faculty in demonstration of The Fox School's commitment to scholarship, teaching and service in the practice of public and private sector management.

The Fox School is one of the 17 schools and colleges of Temple University. A leader in graduate and professional education, Temple is one of only 148 of over 3,800 higher education institutions in the U.S. designated a Doctoral/Research Extensive university by the Carnegie Foundation for the Advancement of Teaching. This distinction is based on Temple's range of programs, commitment to graduate education, and the breadth and number of doctoral degrees it awards.

Headquartered in Philadelphia, Pennsylvania, Temple is strategically located for corporate partnerships in a hub of the financial services, healthcare, information technology, pharmaceuticals/biotechnology, and tourism industries. Temple's School of Tourism and Hospitality Management, affiliated with The Fox School, offers quality undergraduate and graduate degree programs in sport and recreation management as well as in tourism and hospitality management.



A Message from Mayor Willie L. Brown, Jr.

Willie L. Brown, Jr.

It was a privilege to co-host the Mayor's Technology Summit on Homeland Security and Economic Development with the Center for Competitive Government of Temple University's Fox School of Business and Management's in San Francisco, July 17 and 18, 2003.

This Summit, which brought together mayors and CIOs of major cities, high ranking military and civilian officers from the Pentagon, and executives of leading IT companies, provided an all too rare opportunity for a substantive dialogue among public and the private sectors executives on the critical issues of applying technology to enhance homeland security and economic development while being especially mindful of the sensitive and important issues of the privacy of individuals.

These Proceedings provide a condensed version of presentations on new technology and management techniques that will help mayors prevent, respond to and recover from terrorist attacks. Continuation of similar undertakings will help prepare mayors and others directly responsible for the safety of our cities to better understand the complex issues of homeland security. Such sessions provide IT companies with information about the needs of our cities and enable the public and private sectors to create partnerships that benefit all of us.

We were fortunate that Temple University's Center for Competitive Government was our partner for this Summit. It was the Center's third annual meeting following two similar efforts co-hosted by Mayor Rudolph Giuliani of New York City.

We thank the Center for joining with us and hope that it will continue with its important missions and organize similar events in the future, and I especially urge them to continue their productive research on these vital subjects.

Sincerely,

Willie Brown, Jr.

Dean's Letter

M. Moshe Porat, Dean of The Fox School of Business at Temple University.

Information technology (IT) has been one of the driving forces of the global economy. Applications in Information Technology have mostly been focused on increased economic efficiency and improved real-time communication between the public and private sectors.

The September 11th attacks and the heightened terror alert have placed created a new priority in the application of information technology. This summit addresses the importance of improving homeland security while combining public and private sector interests in a neutral atmosphere that focuses on substance and issues, not self-interest.

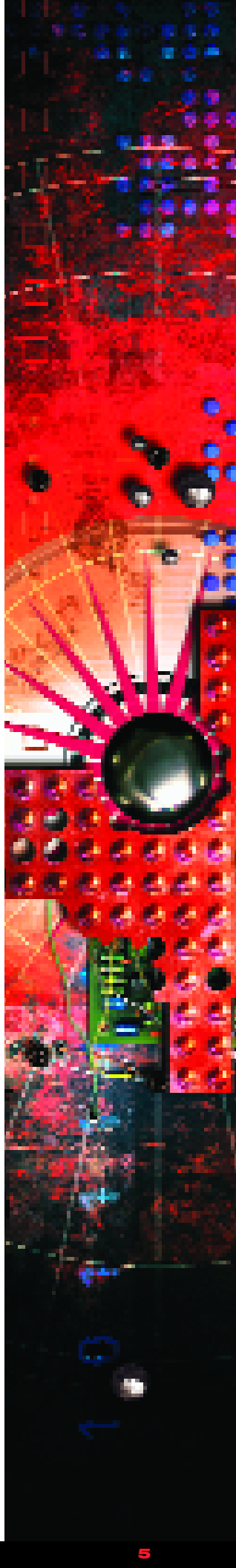
The greatest effort in improving Homeland Security and mitigating the risk of other terrorist activities can be achieved by forming a working partnership between the public and private sectors. This Summit facilitates the collaboration between Federal, State, and local governments with private sector technology firms who operate only on the cutting edge of information technology. The following presentations feature best practices in defense, safety, and homeland security used by the public sector and military, as well as the newest breakthroughs in technology that can be readily implemented at all three levels of government. The Center for Competitive Government brings together these leaders in government, business, and academia to share information and exchange ideas in an unbiased environment.

I am certain that Information Technology will become more critical as we continue to face the most important issues of public safety and terrorism. The Center for Competitive Government will continue to stay on the forefront of this knowledge development.

I want to thank Dr. Simon Hakim and Howard A. Cohen for their vision and efforts to produce this important volume and thank Temple University and the staff of the Fox School for their support.

Best regards,

M. Moshe Porat, PhD, CPCU
Dean and Joseph E. Boettner Professor
of Risk and Insurance



The Center For Competitive Government

Temple University's Center for Competitive Government is a preeminent resource for federal, state and local governments seeking to understand and implement best management practices and e-government strategies. It specializes in applying contemporary economic and management models to public sector problems and is becoming an international center for information about the management of technology to improve constituent services and reduce the cost of government.

To facilitate the development and growth of better practices, the Center conducts policy-oriented research, engages in consulting projects, develops databases, organizes conferences, and publishes reports, books, and articles related to the application of private sector principles to public sector problems. The Center has substantial experience in conducting and analyzing data from large-scale surveys for various public and private entities and has conducted specific studies on topics such as: privatization of police, correctional institutions, welfare services and airport management; public-private partnerships in free trade zones; and private toll roads.

The Center has obtained grants and has organized eight academic and professional conferences, including the highly successful "Making Government Work Conference," hosted by the city of New York and underwritten in 2000 by PricewaterhouseCoopers Endowment for the Business of Government. The Center maintains working relationships with organizations such as the Council for Public-Private Partnerships, Manhattan Institute for Public Policy, National League of Cities, Milken Institute, National Governors Association, Volunteers of America, and with mayors and governors throughout the United States and around the world.

Paul J. Andrisani, PhD, Founding Director

Professor of management Paul J. Andrisani has taught at Temple University since 1974. As Director of the Center for Labor and Human Resource Studies, he specializes in human resource management and labor market economics. His research focuses on the labor market experiences of special groups in the American economy, among them older workers, minorities, women, veterans, and persons with disabilities. He has also conducted considerable research on the economics of discrimination in employment and credit markets. His research has been funded by many government, educational and private organizations, published in numerous academic journals, and presented to various societies and professional associations and to senior management and board committees of numerous companies and government agencies. He has testified before Congress on issues of human resource management and lectured extensively throughout the U.S. and abroad. He has served as a consultant to major corporations, government agencies, and government entities. He holds a BS and MBA from the University of Delaware and earned his PhD in management science at Ohio State University.

Simon Hakim, PhD, Director

Professor of economics Simon Hakim has taught at Temple University since 1974. His research focuses on analysis of criminal behavior, police operations, and privatization of police and correctional institutions.

He is co-author of *Securing Home and Business: A Guide to the Electronic Security Industry* and co-editor of 11 books, mostly on privatization of state and local government. He was the editor for a book series on privatization of state and local services published by Greenwood Publishers. He has published over 50 scientific articles on crime and security in leading economic and criminology academic journals and more than 60 articles in trade magazines for government, and the security and insurance industries.
(see www.fox.temple.edu/~shakim)

Hakim is often interviewed, and his research findings quoted, on national TV and in major newspapers throughout the nation. He has conducted funded research projects for numerous government agencies and for major international companies.

He holds a BA in economics from Hebrew University, an MS in city and regional planning from the Technion, Israel Institute of Technology, and earned MA and PhD degrees in regional science from the University of Pennsylvania.

Willie L. Brown, Jr.

Elected as mayor of San Francisco in 1995, Willie L. Brown has shown continued vitality and economic energy in uniting San Francisco's ethnically diverse neighborhoods as well as the burgeoning business community.

As mayor, he has continued his career-long commitment to civil rights and higher education, notably by designating the address of refurbished City Hall as Dr. Carlton B. Goodlett Place, after the recently deceased San Francisco NAACP Chapter president and community activist. During the renaming ceremony and in front of a crowd of 7,000 people gathered at the 13th annual Martin Luther King Holiday rally, Mayor Brown restated his dedication for the betterment of education, continued fight for civil rights and vowed to continue representing all of the minority groups that make up San Francisco.

He has championed and signed legislation requiring all companies doing business with the city to grant equal benefits to their workers' domestic partners. His administration continues to work toward guaranteeing universal health care for its 130,000 residents currently without medical coverage.

Throughout his tenure in public office, Mayor Brown has been a tireless advocate for affirmative action. Prior to being elected mayor, he served a total of 31 years on the California State Assembly. In 1980, he was elected speaker of the assembly, a position of power second to only that of the governor and a position he held for an unprecedented 15 years.

As a state assemblyman, dozens of his bills became law including, bills that requested the United States Congress to grant citizenship to Filipino veterans of WWII and the most comprehensive education reform and financing bill.

Mayor Brown has a BA from San Francisco State University and a JD from the Hastings College of Law. He was admitted to the State Bar of California and built a thriving law practice. He has received numerous honorary degrees from Morehouse College, San Joaquin College of Law, California College of Podiatric Medicine, Atlanta University, Wilberforce University and Crown College, University of California, Santa Cruz.

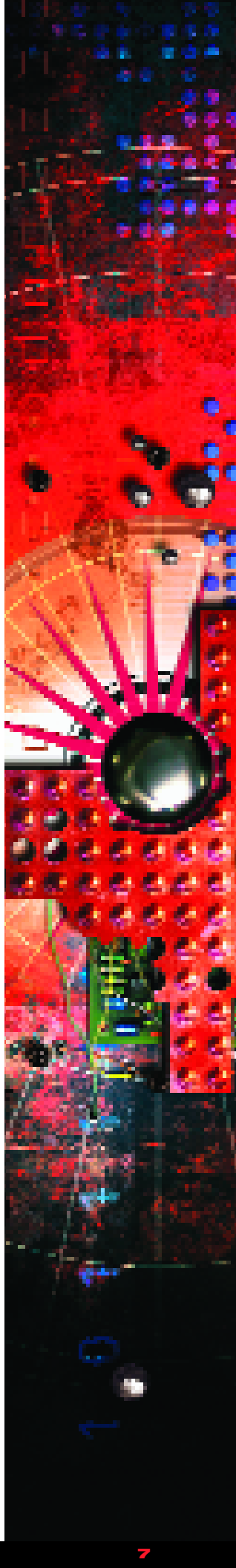
M. Moshe Porat, PhD, CPCU

Dr. M. Moshe Porat is the dean of The Fox School of Business and Management and dean of the School of Tourism and Hospitality Management at Temple University. He is also the Joseph E. Boettner Professor in Risk Management & Insurance and the former chairman of the Risk Management, Insurance and Actuarial Science department.

Prior to his academic work, Dr. Porat served as deputy general manager of Ihud Insurance Group, a large international risk management and insurance firm and as an economic and financial consultant. Dr. Porat authored several monographs and numerous articles on captives and their use in risk management, self-insurance and other financial topics. He serves on the Board of Directors of Penn-America Group Inc., and Global Technologies, Inc., and is a Board Member of America-Israel Chamber of Commerce, the Philadelphia Workforce Investment Board, The Pennsylvania Economy League and High Tech High Charter School.

Dr. Porat has received several awards for excellence in research and economic and international business initiatives. In 1998, he received the Philadelphia Mayor's Citation for his activities in connection with international programs. The Academy of International Business for his leadership and contributions to international business programs and research selected him as the 2001 International Dean of the Year. He was also awarded the 2002 Adam Smith Leadership Award for Academic Excellence and Educational Leadership by Economic Pennsylvania.

He received his undergraduate degree in economics and statistics from Tel Aviv University and his MBA from the Recanati Graduate School of Management at Tel Aviv University. He earned his PhD degree from Temple University.



Introduction

Simon Hakim, PhD, Director, Center for Competitive Government

Howard A. Cohen, Associate Dean, The Fox School of Business and Management

Professor Simon Hakim, PhD

These Proceedings exhibit the presentations of mayors, CIOs, and executives of technology companies at the Third Annual Mayors' Technology Summit that took place in San Francisco, July 17 and 18, 2003. Then Mayor Willie Brown Jr. hosted the Summit that was organized by Professor Simon Hakim of Temple University's Center for Competitive Government "CCG" and Associate Dean Howard A. Cohen, of Temple's Fox School of Business and Management. Former Secretary of State George P. Shultz was a keynote speaker at the Summit that was attended by mayors, CIOs, directors of homeland security for the State of California, Generals of the Marines Corps, ranking officers of the Coast Guard, and officials from the U.S. department of Defense, executives of the City of San Francisco, and leading multinational and technology companies, including Battelle, Ciber, Cisco Systems, Hansen, Bechtel, Integraph, SBC, Voyager Systems, Accenture, Citynet Telecommunications, Extreme Business Solutions, Human Vision, and PlanGraphics.

This Summit continued the work of our 2000 and 2001 Summits that took place in New York City hosted by then Mayor Rudolph Guliani. The 2000 Summit dealt with best management practices of municipal services, and the 2001 summit was devoted to best practices in e-government. Sponsors included, among others, the New York Stock Exchange, Cisco Systems, AOL-Time Warner, IBM's Center for the Business of Government and Enterasys Networks.

CCG deals with improving the work of government, including the introduction of business practices to the public sector. We analyze best practices and managerial and technological innovations, including the suitability of competitiveness, managed competition, privatization and public-private partnerships. We implement economic models that will achieve greater efficiency in the use of resources, and research has included innovations in police and crime control, privatizing the liquor industry in Pennsylvania, reducing congestion on the 911 lines, the introduction of competition to the delivery of adoption and foster care services, and privatization of water and wastewater facilities. Our basic finding is that greater efficiency often can be achieved by shifting from government monopoly to competitiveness and greater free choice by citizens, consumers, and constituents. Enabling consumer sovereignty in the choice of vendor should be preferred to government choice through auctions to private companies seeking to replace government in the delivery of services.

Our studies also have shown that some public services, like police response to emergency calls and adoption and foster care services achieve greater efficiency and equity when market forces are included in the process.

Today all three levels of government are essential to providing homeland security. Senator Rudman's 2003 report, Homeland Security Grossly Underfunded, claimed "… the US is dangerously unprepared for another attack … The nation's preparedness for terrorism is not much better (in 2003) than they were in 2001." The report focused on

insufficient funding, and suggested spending an additional $98.4 billion over a five year period. The report noted that federal, state and local spending on homeland security for first responders needed to triple to reach minimum acceptable level.

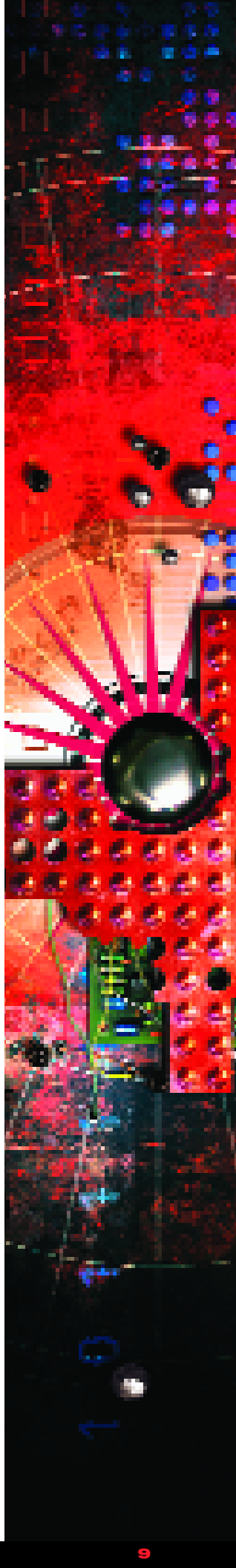
However, the answers are not merely funding increases. Rather, it has been necessary to introduce incentives for private firms to enter the "business of homeland security." Similar to other public industries it is imperative to consider public-private partnerships and exposure to market forces in the production and delivery of services while still maintaining government responsibility. In addition to the supply of services and equipment, we need to develop innovative funding schemes that are common in private markets to attract private participation in funding and production of such vital services. This is exactly the focus of our Center for Competitive Government; our mission is to research managerial and technological innovations that can be adopted by government to enhance homeland security.

The San Francisco Summit was part of that effort. We learned about innovations in the public and private sectors to improve service delivery in homeland security and public safety. Our Summit exposed the need to:

- Facilitate further contact between the public sector consumers of technology and the private providers of technology.
- Strengthen the triangle of public-private-academia to develop managerial and technological ideas in all areas.
- Introduce new technologies in homeland security and public safety, especially in communications and monitoring.
- The following presentations are an effort to continue this most essential work.

> Our basic finding is that greater efficiency often can be achieved by shifting from government monopoly to competitiveness and greater free choice by citizens, consumers, and constituents.

On the steps of City Hall (left to right): Manny Menendez, Mayor John Marks, Lewis Loeven III, Simon Hakim, Galia Hakim, Rachel Porat, Mayor Jeremy Harris, M. Moshe Porat



Reflections on Homeland Security

George P. Shultz, former Secretary of State, Thomas W. and Susan B. Ford Distinguished Fellow, Hoover Institution

We're here because we have potentially a huge problem and are trying to address it. I think there is a lot to worry about and a lot to do, but I also think that there are some good signs, and it is a mistake to be totally gloomy, that we haven't done enough and so on.

First of all, attitudes matter a lot. The fact that we're having this conference, we've heard about Seattle and Chicago and their efforts — I was pleasantly surprised to hear what DoD is prepared and organized to do. I put a lot of importance on attitude. I have been in the construction business, and a job site is inherently unsafe, people are prone to injuries. The company that I have been associated with, Bechtel, thinks it's our number one thing to worry about. If you walk onto a Bechtel job site the first thing you see is a big sign about safety; it's there every day. It's the kind of problem you don't solve — you work at it constantly. The result is that we run jobs that set records for no lost time due to accidents.

A lot of homeland security is attitude — being conscious of things. When I was Secretary of State we had problems and we got our security apparatus geared up. We found out what could be done, got people to be more alert. There were quite a few terrorist incidents that were prevented because people saw things before they happened.

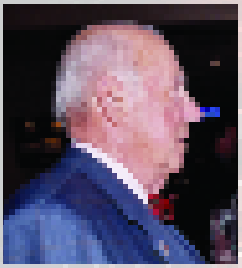
There is a tendency to think in terms of: What do we do when we get hit? That's understandable, but that's not the mentality that you want. You want to say: We're going to find out what might happen and stop it. Because with the kind of weapons that are around, the damage that can be done, you don't want to get hit. The war on terrorism is about prevention, and that's what our military is doing for us.

Let me say a word about technology. I think attitude, a sense of importance and need, has an impact on what the scientific community produces. I was fascinated to read about Dr. Todd Ritter at MIT. He has created new sensor technology that identifies pathogens quickly and without false positives. Now, that's a big thing. He may not have realized what he had unless he had the problem on his mind that, if you get hit with pathogens, you want to know what they are and have an antidote that can be distributed widely.

That's an example of what can happen. The American scientific community is ingenious, and a lot of it stems from the Department of Defense research group, which performs and sponsors basic research. It has paid off handsomely for our military, and the rest of us have also gotten huge benefits — such as the Internet. We will continue to see important innovations come out of our labs, and they will be produced by a consciousness of need.

I recount these to underscore that success is possible. I see too many people moping around, saying, "Oh, my gosh. It's inevitable — we're going to get creamed." It is not

biography



George P. Shultz *served as the 60th U.S. Secretary of State from 1982 - 1989. Following his government service, he joined Stanford University as the Jack Steele Parker Professor of International Economics at the Graduate School of Business and a distinguished fellow at the Hoover Institution.*

Prior to his appointment as U.S. Secretary of State, Shultz was chairman of President Ronald Reagan's Economic Policy Advisory Board and Secretary of the Treasury. He served in the administration of President Richard Nixon as Secretary of Labor and was then appointed director of the Office of Management and Budget. He left government service to become president and director of Bechtel Group.

Currently he is a member of the board of directors of Bechtel Group, Fremont Group, Gilead Sciences, Unext.com, and Charles Schwab & Co. He is also chairman of the International Council of J. P. Morgan Chase and on the advisory committee of Infrastructureworld.

Shultz graduated from Princeton University, receiving a BA in economics. He also earned a PhD in industrial economics from the Massachusetts Institute of Technology and holds honorary degrees from the Universities of Columbia, Notre Dame, Loyola, Pennsylvania, Rochester, Princeton, Carnegie-Mellon, City University of New York, Yeshiva, Northwestern, Technion, Tel Aviv, Weizmann Institute of Science, Baruch College of New York, Hebrew University of Jerusalem, Tbilisi State University in the Republic of Georgia, and Keio University in Tokyo.

inevitable, and we don't want to take that attitude.

When I became Secretary of the Treasury the Secret Service reported to that position. So they came in and the head of the Secret Service said, "Mr. Secretary, I have to tell you that we will do everything we can, but in the end, it's impossible to protect the President 100%." I said, "I don't want to ever hear you say that again. Your job is to get 100%. That's got to be your attitude. You tell me that in the end you can't really do it? You're already copping out." We have to have the attitude that if we organize ourselves right and we interact right we can identify things before they happen.

> As we build homeland security from the cities up as well as from Washington down, we ought to have a mentality that we are not just waiting for something to happen.

Of course if something happens we need to be able to respond and we need to train ourselves for that. For a quarter of a century or more, our country has been attacked by terrorists in barracks and embassies. Our civilians have been attacked — mostly abroad. We've done a few things, but the reality is that we have done nothing effective about it. All of a sudden on September 11th we awakened to the fact that they're at war with us. So we're at war with them.

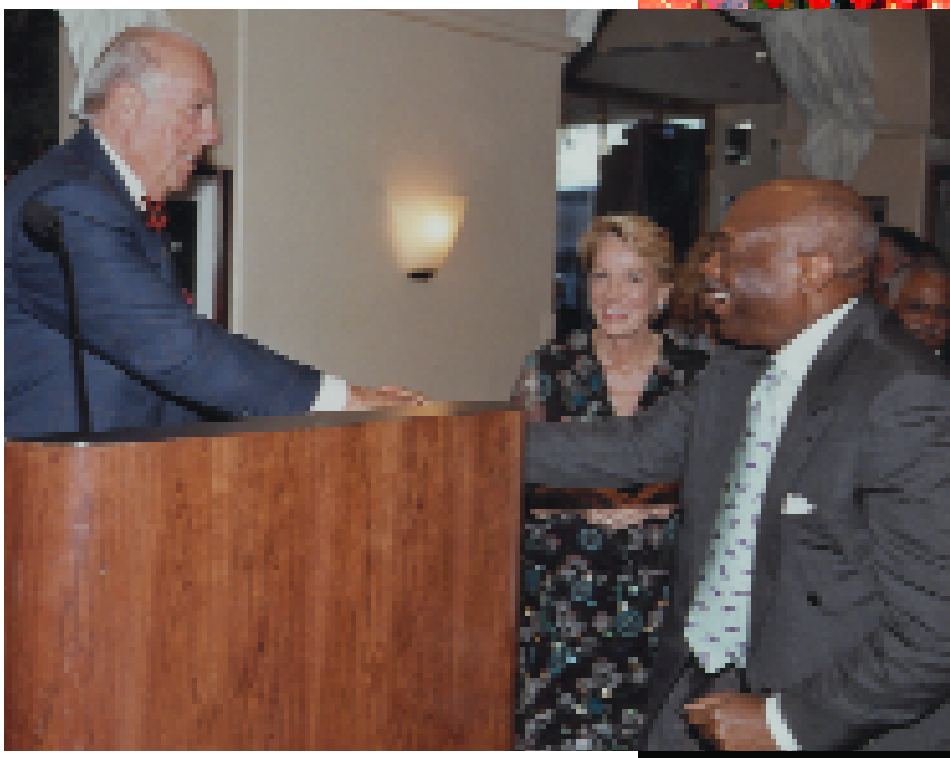
We've had the idea that we need effective law enforcement, but that doesn't work on this problem. Look at the World Trade Center bombing in 1993. It was only a few months ago that finally the perpetrator of that attack was properly convicted. It took all that time. That's not effective in stopping these events.

War is different from law enforcement. Law enforcement is passive: You wait for someone to commit a crime, you catch that person, try him, and put him in jail. War is active: We go get them before they get here. It also involves defense, which is also active in that it takes steps to prevent things from happening. Prevention is now the name of the game.

Prevention relies on intelligence; we need wonderful intelligence. Our ability to stop weapons proliferation is key in preventing major attacks here. So attention to what comes in at our docks, for instance, is very important. Find out about it before the ship gets here — not after. That's prevention.

If you manage a city and something happens, how do you organize? There should be somebody of stature in charge. I was in New York a few months ago. The mayor sent two people — one was the person in charge of antiterrorism in New York City, a retired Marine general. I listened to him talk and thought: He's a take-charge guy; he knows what he's doing. This is a man of stature who understands the nature of this beast and who can work at it. The other person, a retired CIA officer, was their intelligence person. They have people around the world and are active in the intelligence network. That's very important, to have somebody in charge and to tap into intelligence.

The people in charge need to access technological, managerial, and intelligence developments, because they are evolving. We're going to see are all kinds of useful things, and it's important to be alert to those developments. No doubt the organizations involved — the federal organizations, the Homeland Security Department — can disseminate this informa-



George Shultz and Mayor Willie L. Brown, Jr.

Left to right: Simon Hakim, Galia Hakim, Charlotte Shultz, Secretary George Shultz, Rachel Porat, and Moshe Porat.

tion, but it's good to have local people capable of receiving it.

Obviously it is very important to collaborate with first responders and assure that they work effectively together. You don't find out about that unless you practice. It reminds me of my confirmation as Secretary of State, when all these smart Foreign Service officers subjected me to tough questions. I didn't like it, but I did it. And I was glad I did it.

Before most of you were born I served in the Eisenhower administration, in the days when people paid attention to security threats and had exercises. All of us had to take part. I was an economist and said to myself, "What am I doing this for?" So a meeting was called, and who should appear but President Eisenhower, who said, "What you're doing is practicing a plan. We're seeing how we carry it out and what the bugs are, but if you get it into your head that you just follow the plan you are going to lose — because as soon as action starts, the underlying situation will be different than you assumed. And if you aren't quick enough to adjust, you won't do well. So it's important not to be locked to a plan but to a process. The process shows you what the variables are and how to adjust." That's the kind of thing we ought to keep in mind.

This is the same — try things out and see how well coordinated you are. Then you figure out: I don't have this and that, and there are certain things I'm entitled to have from the federal government or the state. If we're going to get our share we have to be aggressive. We aren't spending enough money on this subject by quite an order of magnitude. Our cities deserve more and we're going to have to do a little effective lobbying.

I want to underline this with a few things that were identified in the report "Emergency Responders: Dramatically Underfunded, Dangerously Underprepared." On average — this is not saying any particular place — fire departments have only enough radios to equip half the firefighters on a shift and breathing apparatus for only one-third. Only 10% of fire departments in the United States have the personnel and equipment to respond to a building collapse. Police departments do not have the protective gear to safely secure a site following an attack using weapons of mass destruction. Public health labs lack basic equipment and expertise to adequately respond to a chemical or biological attack. As an aside, the recent SARS episode taught us a lot. We saw the value of the Centers for Disease Control and the World Health Organization. We saw their competence and probably sensed that they are underfunded.

Most cities do not have equipment to determine what kind of hazardous material emergency responders may face. Nearly half of local health departments have no epidemiologist on staff and 75% of state laboratories report being overwhelmed by too many testing requests. In brief, that is what the task force found, based on a survey. It is a devastating indictment — we should move on these things.

Concluding, threats are focused. As we build homeland security from the cities up as well as from Washington down, we ought to have a mentality that we are not just waiting for something to happen. We have to be part of the intelligence network, to collect and connect the dots so that we prevent as well as equip ourselves for whatever might happen.

Attitude is the beginning. Attitude is important, so hats off to Mayor Willie Brown, to Temple University, and to all of you attending this conference on a subject that really matters. Thank you.

Lessons from TopOFF, Seattle's Terrorist Response Exercise

Brent Wingstrand, Assistant Chief of Police, Seattle, Washington

I will go through some of the things that we used during TopOFF, the National Response Plan exercise conducted in Seattle and Chicago in May 2003, that assisted in the planning, operation and, in some cases, after-action.

Just a little bit about TopOFF. The exercise shared by Seattle, the State of Washington and King County — as well as Chicago was an extremely ambitious undertaking. Frankly, I think it exceeded everybody's ability, because we couldn't devote enough time to the scenario, but also because of the complexity of dealing with an event that's never happened before. It involved a dispersion device commonly known as a dirty bomb — conventional explosives mixed with radiological material, that can cause if not a lot of deaths, considerable angst and cleanup costs.

To prepare, we formed a planning team and it soon became apparent that we were dealing with a tremendous number of entities. In the private sector we dealt with the Bank of America, Burlington Northern Railroad, Starbucks, Tully's, Safeco Field, the Red Cross, and all of the hospitals and ambulance companies. The private sector participants were primarily those adjacent to the site of the exercise or those helping to conduct the exercise. We did not involve the private sector nearly to the extent that they would be involved if an incident like this really occurred. I've heard the figure used that 85% of the critical infrastructure in this country is controlled and owned by the private sector. So while we in the government have the responsibility of keeping the community and our way of life safe, we need that 85% working with us.

As far as the government participants, I didn't know there were that many federal agencies; we had acronyms that I hadn't come across before. We had our own Sound Transit Authority. We had state and county and local health, Department of Energy, Coastguard, FBI, Metro, Department of Homeland Security, FEMA, and I don't know how many others involved. It presented a real challenge to the local planners as well as their federal counterparts just to keep everybody on the same page. Given the magnitude, I think we all did a pretty good job.

One thing we found is that first responders and the people they work for, which is the political system and support agencies, have to be trained together. We are quite familiar with testing police and fire response in incidents, and we've done tabletop exercises in which we tested emergency management in recovery from an earthquake or something like that. But in the case of terrorism, where you're mixing bad guys in with the destruction they perpetrated, you're combining the entire governmental system and all of the private sector non-profits. That's not going to work smoothly, even if we practice every day. But every little improvement saves lives, dollars, and gets communities back on their feet that much quicker.

An exercise like TopOFF is not a place to test new technologies. The exercise was designed

biography

*Assistant Chief **Brent Wingstrand** commands the Emergency Preparedness Bureau, which consists of the Emergency Management Operations, Homeland Security Program, and Arson/Bomb squad.*

Assistant Chief Brent Wingstrand is a 34-year veteran of the Seattle Police Department. He has previously commanded a wide variety of police functions, including: Juvenile, Gangs, the East Precinct, Domestic Violence/Special Assault, Internal Investigations, Metropolitan, Operations Executive Admin, and Violent Crimes. Chief Wingstrand has commanded the Emergency Preparedness Bureau since October of 2002. This bureau was created in April of 2002 and has citywide responsibility for prevention, preparedness, response, mitigation, and recovery regarding all disasters, including terrorism. The Emergency Preparedness Bureau formed the core Seattle planning group for the Top Off 2 national terrorism exercise.

Chief Wingstrand is a graduate of Seattle's Advanced Management program and has an AA in Law Enforcement from Green River Community College and a Bachelor's degree from the University of Puget Sound in Public Administration.

to test the systems that we have now, and the policies and procedures were clearly going to have failures along the way. In TopOFF current and new applications of existing technology were used with mixed success.

The planning group had our information technology section create a specific TopOFF e-mail account so that people within the planning group could access, read, and respond to a core of information. Federal and state planners throughout the nation could send e-mail to that address and have it acted upon. One problem was that this created another place for people to have to look to see what was waiting on their plates. The sergeant who was involved in everything and did a magnificent job, was getting about 50 TopOFF-related e-mails a day to her regular account, another huge number coming to the TopOFF account, and there was also a third location.

Another problem was that the TopOFF e-mail account was set up to record only the fact that an e-mail was open, not who had opened it. So you didn't know who had seen it, leaving the chain of command with the question: "Okay, does everybody know about this?" A lot of messages then got circulated a second time. So there clearly is room to improve the exchange of information. This is clearly within our capability.

A secure portal was set up to keep TopOFF confidential because it was a limited-notice exercise. We didn't want the world to know the script, and a secure portal was a good idea but it also added to the work. The administrator for the site could restrict access to various subcomponents on the site, so somebody would go in to start working on something and they could get four documents into it and then be denied access to a fifth. So the secure portal made it difficult to be sure that people had the access they needed. Also, passwords expired on a revolving basis. In the midst of all of the other work going on, you would find that your password had expired and you would have to renew it.

Another tool was the master scenario events list, the second-by-second script for how the event would go from beginning to end. The tool was not fully developed, so there were problems with entering information. In addition, the tool was abandoned when a new subcontractor took over in the middle of the exercise and used a different tool.

So from the standpoint of putting the scenario together, it is necessary to assure that the software has all of the bugs worked out or planners will waste a lot of time. The problem is not technology but a lack of training, not enough familiarity with, or inappropriately using, the technology. If it's a new product, it may not be fully developed. That's something that we must deal with.

> One thing that is really important for mayors or chief executive officers: how your people respond in a disaster is going to be tied directly to how you respond.

I've been trained in Project Office twice. I couldn't even log onto that system today because I haven't used it in three years. Much of the problem we have is dealing with the amount of technology that's pouring out at dinosaurs like me. It either becomes overwhelming or you don't have time with everything else going on to gain expertise. So while Project Office looked like a great tracking tool, we abandoned it. Primarily, we had insufficient administrative support to keep it going.

Another problem: early in the exercise we said, "We need to control the plume from this explosion," because we were going to have an explosion occur just south of downtown Seattle. If we didn't script it so that the plume would be carried a certain way, then all of our government buildings would have been contaminated and we'd have had to close down operations, a complication we didn't want to address in the exercise.

We developed a plume model, plugging in data to get the approximate results that we wanted. When the exercise was carried out, other agencies brought in their plume models. While I've not heard that any of the models were wrong, it's like climate forecasting — little variances in the data gave different results, and those differences caused a real breakdown initially.

I want to cover some of the elements of the exercise that worked very well. Instant ID, a

system that allowed us to create credentials for people on site in two minutes. Using a digital camera, we could take the picture, print it out, laminate it, and have their photograph and name on a visible ID they could wear. You were able to verify, from a list of authorized people, that you in fact have those people. It's great: we're going to use it at other events.

We used ArtView in digital photography to do mapping and site overviews for the work, Excel spreadsheets for all kinds of different projects, and PowerPoint — a lot of people used PowerPoint all during planning to coordinate and demonstrate.

Video was a big success. We hooked up just standard video for the Virtual News Network that was kept separate from the real media. We made good use of it. We also had live video feed into our command centers. We had a two-way Business Emergency Network through which businesses could access information on the city's site and then disseminate it to their people. The network also served as a filter for information coming back in. It was much more timely than relying on virtual newscasts. It had a lot of bugs, but we're working on it — a big-time program.

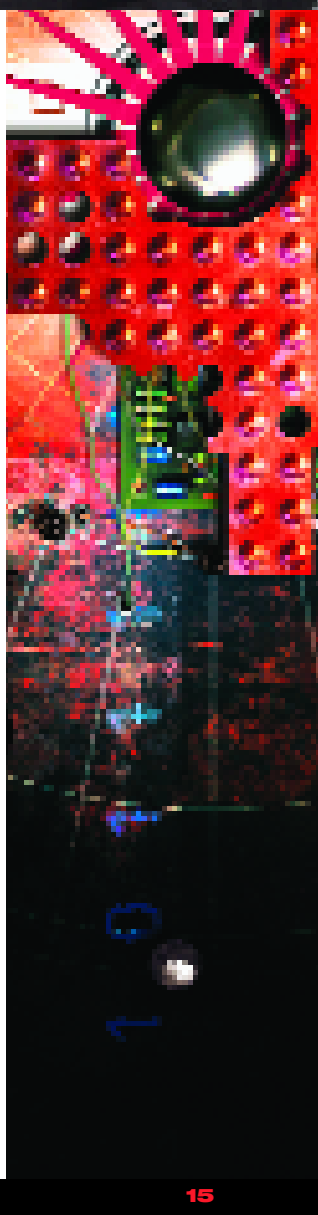
Video teleconferencing was very important. People need their mayor, governor, executive or whatever close at hand, but these individuals also need to meet with each other. Video teleconferencing, set up from all the emergency centers, worked wonderfully to keep people where they were needed, yet let them meet with their counterparts.

We had no problems with the phone system. Nextel brought in a COW — a cell on wheels, to support the cellular phone activity that increased because of the exercise.

One thing that is really important for mayors or chief executive officers: how your people respond in a disaster is going to be tied directly to how you respond. If you are familiar with the systems in place it will show to the people around you, and they will perform better. Mayor Nickels of Seattle, to his great credit, came down to our emergency operations center, put himself on the line to look silly if he made bad decisions, and tested himself. He asked tough questions and was subjected to tough questions. When the exercise took place, he was on his toes. And the people in our emergency operations center knew it, and they all performed better because of it. I know you're all very busy, but if you have emergency operations systems in place, take the time to get training in them.

Mayor Patrick McCrory and Mayor Willie L. Brown, Jr.

One more thing — Yogi Berra said the future ain't what it used to be. It's not, and we're the ones that have to figure out what it is going to be. Technology is going to take the lead, and we need to do our part to figure out how to come up with effective solutions and systems on the limited resources that we have.



The Department of Defense in Homeland Security and Homeland Defense

Peter Verga, Principal Deputy and Assistant Secretary for Homeland Defense, United States Department of Defense

It's a terrific opportunity to be here and to talk to you. I'm particularly pleased to note that Temple University is associated with this. I was a student at Temple University for three semesters before I got drafted into the Army. I have a fond spot in my heart for Temple University.

Homeland security and homeland defense are not interchangeable terms. Homeland security is a concerted national effort to prevent terrorist attacks, reduce our vulnerability to terrorist attacks, and assist in the recovery from them should they occur. Homeland defense is the protection of the United State and its domestic population from external threats and aggression.

Now, external threats and aggression can manifest themselves internally — that's what happened on September 11th. So that does not mean that we aren't concerned about that. But it's a distinction that we in the Department of Defense have to maintain as we look at our role in the overall national effort.

The national objectives outlined in the President's Strategy on Homeland Security are prevent, reduce, and minimize damage. The Department of Defense plays a role in each of these critical mission areas.

We have two major bodies — the National Security Council and the Homeland Security Council. The policies, discussions, and decisions which result in recommendations to the President come through these two forums. In the Department of Defense, we end up working both sides of that equation. On the homeland defense side, we're working with the National Security Council, the Secretary of Defense is a member of the Council, and on the homeland security side, we provide civil support as a member of the Homeland Security Council.

The fundamental difference between homeland security and homeland defense for DoD is that homeland defense refers to the missions of the Department of Defense and traditional military chain of command — from the President to the Secretary of Defense to the combatant commander, Northern Command.

On the homeland security or civil support side, DoD principally supports another federal agency. We envision domestic authorities performing domestic security — we in the Department of Defense do not want to be the nation's internal security force. The role of the military in internal security has traditionally been limited, and that has served us well over the last 228 years.

Enhancing capabilities at the lowest level of government is very important. Just as all politics are local, all disasters are local. It's going to be first responders that are going to have to handle the situation. We want them to have the best capability in terms of training, tactics,

biography

Since January 2002 ***Peter Verga*** *has been the DOD Special Assistant for Homeland Defense where he directs the DOD Homeland Security Task Force.*

He is a retired U.S. Army officer with over 26 years of service in various capacities including Operations Directorate of the Joint Chiefs of Staff, as Deputy Under Secretary of Defense (Policy Support), Deputy Under Secretary of Defense (Policy Integration), Deputy Director for Emergency Planning in the Office of the Secretary of Defense, Deputy Director of the Office of Emergency Operations of the White House Military Office, White House Staff Special Assistant to the Assistant to the President for Management and Administration.

He has been awarded the Defense Distinguished Civilian Service Award, the Defense Meritorious Civilian Service Award, the Combat Infantryman's Badge, the Defense Superior Service Medal, the Legion of Merit, four Bronze Star Medals, the Purple Heart, three Defense Meritorious Service Medals, 21 Air Medals, and the Presidential Service Badge, among others.

He holds a BS in public administration from the University of La Verne and a MS in public administration from Troy State University. He is also a graduate of the U.S. Army Command and General Staff College.

Left to right: Manny Menendez, Simon Hakim, Mayor Pat McCrory, Mayor Willie L. Brown, Jr., Mayor John Marks, Mayor Jeremy Harris, Moshe Porat, and Howard A. Cohen.

techniques, procedures, and equipment, so that they are not dependent on federal resources or ultimately Department of Defense resources.

General Buck Bedard and the great Marine Corps team that's out here working with San Francisco are carrying out that part— helping with tabletop exercises, things that the Department of Defense does well — training, exercising, planning, coordinating — that's what we're trying to pass on to the different levels of government.

Quite frankly, we may be engaged overseas defending the country, and that's why we need state, local and other levels of government to be well prepared. That's particularly important when we talk about low-density, high-demand military assets. Secretary Rumsfeld calls them things we didn't buy enough of. And we are constantly balancing low-density high-demand items — where they're deployed, how they get utilized.

When we deployed to Iraq before the war, we sent assets overseas that might have been needed in the United States should an emergency have occurred. We had to balance what was available there with what was available here. That's one of the main functions of General Bedard and the operations deputies of the different services, recommending to the Secretary about what goes where and the force structures.

This is how we see this all fitting together — homeland security, the overarching level effort, the Department of Defense homeland defense mission and civil support mission. Again, the main thing to remember is that in homeland defense, overseas DoD is in the lead. In civil support, we're in the support of another government agency.

You will notice that there is military support to civil authorities, which is DoD-speak for civilian assistance; homeland defense; in the center is emergency preparedness; and then the homeland security national mission.

There are lots of overlaps. Military operations against non-state actors and overseas — such as what's going on in Iraq — contribute to homeland security. As a matter of fact, the main DoD contribution is the global war on terrorism. We want to fight people overseas so that they can't strike us at home. That's our main mission. People ask how much is DoD spending on homeland security. It's about 400 billion dollars a year — every cent that we have is spent to keep the American people safe in their homes. That's what DoD is all about.

Military activity inside the United States can be routine, temporary, emergency, or extraordinary. Routine is what goes on every single

day in terms of the defense of our nation inside the United States — maritime surveillance, air surveillance. That's going on all the time, plus all the training and exercises like the one to be conducted in San Francisco.

Temporary operations involve military support during a limited event. The typical example is the Olympics — where the military supports civilian agencies. From our perspective, temporary operations are easy to plan because we know the duration. When the winter Olympics were going on in Salt Lake City, we had more soldiers in Utah than we did in Afghanistan and we had just started military operations in Afghanistan. But we knew how long the Olympics would last and exactly what support was needed.

> The national objectives outlined in the President's Strategy on Homeland Security are prevent, reduce, and minimize damage. The Department of Defense plays a role in each of these critical mission areas.

Emergency operations are typically inside the United States — fires, floods, hurricanes, natural disasters. The military supports civil agencies that have taken the lead in the disaster. Typically it is the Federal Emergency Management Agency, what is now the Response and Recovery Directorate of the Department of Homeland Security. If a lot of material needs to be moved coast to coast, the military has the Air Force. If there is an immediate need for beds, blankets, tents, logistical support, it is available from the Department of Defense.

Most emergency operations are in support of another federal agency and they're done on a reimbursable basis under something called the Economy Act. Congress does not appropriate money to the Department of Defense for disaster relief operations — they appropriate that money to another federal agency like FEMA. If they want us to support them, they have to pay for it and we are not a cheap way to do business.

We chose the word "extraordinary" to describe those operations in which the Department of Defense would apply military combat power inside the United States. So an attack like September 11th is exactly what we're talking about. You would use DoD combat power to take care of a hijacked aircraft that was being turned into a weapon — a pretty extraordinary circumstance. We also have specialized capability for dealing with improvised nuclear devices and things like that.

We have done some reorganization within the Department of Defense. We proposed to Congress that a new Assistant Secretary of Defense be authorized and appointed. He is the Honorable Paul McHale, a former Congressman from Pennsylvania and a Marine Reserve Officer. He is the first Assistant Secretary for Homeland Defense, supervising all homeland defense activities within the Department. Another important function is to advocate homeland defense requirements in the Department's resource allocation process. Homeland defense, while it is vital, is new in terms of descriptions and budgeting. So when the Commander of Northern Command comes up with a requirement, he needs somebody in the Office of the Secretary of Defense who will act as an advocate. That's exactly what we do. When we decide we want to do more exercises and need additional resources, that's how we would request them.

The other major organizational change was the establishment of United States Northern Command, which had been in the works prior to September 11th. The attack just reinforced the wisdom of making this change. The command is headquartered in Colorado Springs, Colorado under four-star General Ralph Eberhardt. The mission is to deter, prevent and defeat threats and aggression, a typical combatant commander's mission statement, similar to what exists for the commander of Europe or Southern Command or any of the others.

The part unique to Northern Command is: "As directed, provide military assistance to civil authorities, including consequence management." So all federal military assistance to civil authorities conducted inside the United States is now under the aegis of the Commander of Northern Command. That's good, because it unifies command.

That's not to say all military assistance comes from the DoD. The National Guard is not under federal military control but it can be called into federal service by the President. In addition to being the militia that is mentioned in the Constitution, the National Guard is the strategic reserve of the Armed Forces of the United States. Right now the units we have in Bosnia and the Sinai are all National Guard units. Many of the air crews flying are National Guard air crews. So I will make the standard pitch very sincerely for all of you who are employers, that supporting our National Guard and Reserve soldiers when they're called to active duty is vitally important to the country, and I would commend all of you for that support.

In addition to being responsible for the United States, Northern Command is also responsible for inter-military relations with Canada and Mexico. It unifies homeland defense missions of air, land, and maritime defense. One of the major reasons for forming Northern Command was that land and maritime defense were the responsibility of one combatant commander, and air defense was the responsibility of another, which violates the military principle of unit of command.

You will notice that Hawaii is not inside the Northern Command, but in the Pacific Command. So we in the Assistant Secretary's Office also work with Pacific Command to ensure that they're meeting homeland defense requirements.

The phrase "forward regions" refers to the idea that we want to defend forward. For example, if a ship with a weapon of mass destruction leaves Singapore you don't want to find it when it gets to the port of San Francisco. You want to deal with it well out to sea. So a forward defense, a layered defense, is what we want.

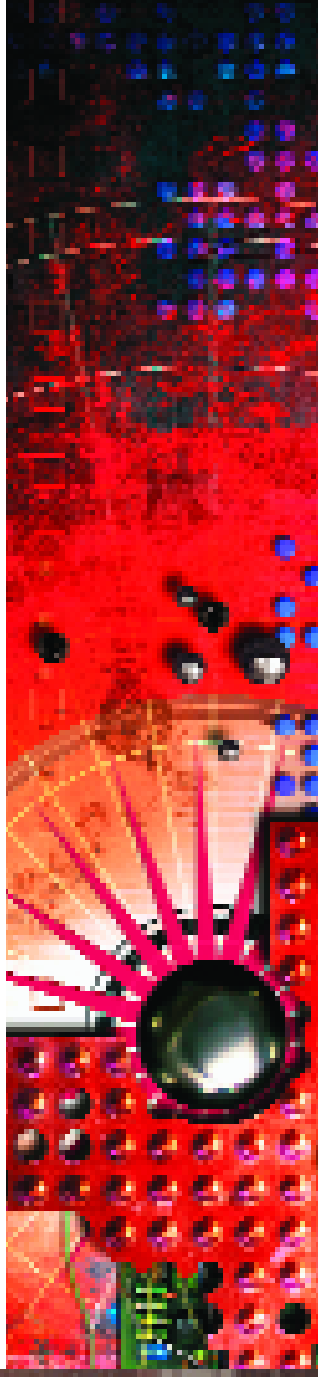
Northern Command is like all other regional combatant commanders around the world, except it includes the United States. That has some uniqueness in politics, operations, and organization. There are 54 sovereign states and territories that we have to deal with in homeland defense; executive authority for those generally resides with the governors. States' National Guards have their own chains of command when they're not in federal service. That greatly complicates the coordination process.

In a local incident you're going to get a response that expands depending on the severity and the length of time. Local is going to be first on the scene — fire, rescue, law enforcement. They're going to bring in mutual aid, hazardous materials. You then might get some state assets. Ultimately, maybe federal assets coordinated by the Department of Homeland Security, which could include DoD military capabilities.

Everybody has to be able to work together and must understand tactics, techniques, procedures, as well as the roles and missions of everyone else. Which is why tabletop exercises like one in San Francisco are particularly valuable. We in the Department place a particular emphasis on them.

We are really good at working in part of the defense equation because we have a lot of experience in it. We are not very good in this uncharted territory such as biological attacks, nuclear or radiological kinds of attacks. We also know how to accomplish homeland defense. So we've got some very good plans and processes, as well as areas in which we need to place more emphasis.

This slide shows a framework for employing the different assets — state active duty; Title XXXII, another federal status; Title X, full-time active duty by guardsmen and how FEMA would work with that; FEMA; federal coordinating officer; and defense coordinating officer.



Left to right: General Mike Myatt, Randy Smith, General Charlie Wilhelm, Charlie Giancarlo, Emil Bedard, and Peter Verga.

This is the group that coordinates federal responses to disasters. When you get into national emergency or Title X this is the DOD mission, support with an unambiguous chain of command.

Just a couple of points on things that the Department of Defense is doing in support of homeland security: we have some good information technology programs, including an advanced concept technology demonstration that helps coordinate mechanisms between command centers on the federal, state and local levels.

The development lab, MARCOR SYSCOM — Marine Corps Systems Command — has done a lot of very innovative work in command and control. MARCOR SYSCOM developed the Disaster Management Information System, which the Department turned over to the Federal Emergency Management Agency for deployment to states.

At the Naval Postgraduate School in Monterrey, a program conducted in cooperation with the Department of Homeland Security grants a Master's degree in homeland security studies for state and local first-responders. The first class started last January and there will be about 140 or so students going through the program at any given time. I would encourage you to think about that as a way of improving the professional education in this area.

We also can train people, transfer critical skills. For example, we have a system for acquisition, development, and life cycle management of plans and programs. We are training some Department of Homeland Security people in this.

Plan, Prioritize, Practice: Preparing for a Terrorist Attack

Emil R. (Buck) Bedard, Lt. Gen., Deputy Chief of Staff for Plans, Policies and Operations, United States Marine Corps

I jumped at the opportunity to talk with you, because of the criticality of what we face today and for the foreseeable future. As retired General Mike Myatt, USMC mentioned, I was in the Pentagon on 9/11.

For some who may not be aware of it, we had 2,403 Americans killed at Pearl Harbor. On September 11, 3,029 were killed, with an additional 2,400 injured. That day, as the Operations Officer of the Marine Corps, I had to immediately take an account of our people, assess the attack, relocate the command, reestablish communications, sort out medical support, provide individual security to key members of the team, and try to determine where the next attack may take place. All of this was going on at the same time, while being pressured by the media for information. This is what you would have to deal with. I would recommend to each of you — especially civic leaders and first responders — that you start by taking home two or three things that you think you can achieve in your own communities.

Let's not assume for one minute that the threat is not still active. Everything that we have gathered to date reinforces that it is. I will use Bin Laden as an example, but there are many threats, his organization probably being the most focused. From 1992 to 2001 Bin Laden's organization probably planned and executed one to two operations a year. From 1998 to 2001 and over the past two years, the frequency is almost one to two operations a month. Some have been thwarted, but my point is that this threat is alive and it's focused on the United States and its citizens, and certainly our allies as well.

I'd like to play a short film and talk about some lessons from it and how they relate to homeland defense and homeland security.

As we look at the organization of the units in Iraq, they represent the command-and-control capability, maneuver forces, aviation assets, air defense, engineers, logisticians, and entire staffs that are brought together to conduct an operation.

All of these elements are meant to blend, to rapidly tailor and task-organize any mission. That comes from training. It comes from familiarity with what you're doing and how you operate, from having equipment that meshes together — be it communications, computers, you name it. That's what we need to emphasize.

For example, we have the British division of about 20,000 forces that joined the United States Marines on our right flank, the United States Army is on the left flank — daily conducting operations with the Special Operations Command — and the integration of air across not only all of our forces but with coalition partners as well.

The things that we do every day in fighting

biography

Lt. Gen. Emil R. (Buck) Bedard *assumed the duties as the Deputy Chief of Staff for Plans, Policies, and Operations, Headquarters, U.S. Marine Corps, Washington, D.C. on July 25, 2000.*

Gen. Bedard was commissioned a second lieutenant in 1967, and designated an infantry officer. While a lieutenant, he served as a rifle platoon commander and company executive officer. He then served as Commander and Staff Officer with Schools Demonstrations Troops. Promoted to lieutenant colonel, he served as assistant operations officer, I Marine Amphibious Force, G-3 and Pacific Plans Officer, G-5.

He was advanced to brigadier general and was assigned as the President, Marine Corps University/Commanding General, Marine Corps Schools, and Marine Corps Combat Development Command. In 2000, Gen. Bedard relinquished command of II Marine Expeditionary Force and was advanced to his current rank.

His personal decorations include: Defense Superior Service Medal, Legion of Merit with Gold Star, Bronze Star with Combat V, Defense Meritorious Service Medal, Meritorious Service Medal, Air Medal with numeral 16, Navy Commendation Medal with Combat V and two Gold Stars, Navy and Marine Corps Achievement Medal, Army Achievement Medal, Combat Action Ribbon with Gold Star, and the Republic of Vietnam Cross of Gallantry with Silver Star.

He received an MS from the University of North Dakota and his formal military education includes the U.S. Army Advanced Infantry Course, Armed Forces Staff College, and Army War College.

General Emil Bedard addresses mayors and participants.

the enemy and waging a major conflict are the same things that have to take place in local communities, to blend capabilities in times of crisis.

You accomplish that in a number of ways — certainly training. I don't think you can train enough. I realize that training is expensive and takes time. But what is the cost if you don't train?

We use boundaries in the Armed Forces, but they are not meant to be restrictive. They're meant to be coordinating points. Too often, we find that people look at boundaries as restrictive — whether they are boundaries between townships, countries, services or organizations. We have to overcome that. Those boundaries are meant to coordinate, to ensure that we can respond rapidly to any crisis. We need to work hard at that, in the Department of Defense and in homeland security.

The battlefield has changed, and our ability to operate on that battlefield wherever it is — inside or outside of our country — is a challenge for all of us. We talked about the exercise that is going to be conducted here in August 2003. It grew out of a request from New York Police Commissioner Ray Kelly, who asked us to participate in a tabletop exercise to determine in various scenarios how the police force would function; how they would coordinate with other agencies, how these organizations would operate together. In a very short period — we spent two days there — a number of things came out of the exercise that increased the capability of the city of New York to respond to a future crisis. I think it was tremendous.

Now one major exercise does not make you capable of dealing with a threat. You've got to prepare continually. I think the critique of an exercise is very important — bringing all the players back together, sitting down and being very frank about what went well and spending time on what didn't go well, and then working on the shortcomings.

There is a program in North Carolina, a test between one of our major bases on the East Coast and the surrounding communities. We have the capability inside the base and in the surrounding counties in Jacksonville, North Carolina to detect chemicals, deal with them, and train military and civilian personnel in protection and treatment.

We also can detect trace amounts of radiological substances that can be used against either the local community or the base. We have a system of sensors on the local highways, along with cameras, that enable us to detect radiological releases and capture the vehicle or whatever platform released them.

We also have a Marine Corps emergency response center with nine counties in the Carolinas. It was created in 1996 to respond to hurricanes, but has expanded to deal with terrorist threats and communities throughout the United States.

Over the next day or day-and-a-half there will be a great deal of discussion on technology. We've said for years in the Marine Corps you don't man the equipment — you equip the man or the woman. With resources as they are, how can technology provide the greatest capability to deal with terrorism or a natural emergency in your municipality?

You have to prioritize. We do it in the military every day. We'd like to buy everything, and modernize every piece of gear. We're not able to because of budget limitations. What do you buy and why? How much do you spend? What does it enable you to do?

In closing, you don't want to meet your allies on the battlefield for the first time. You want to practice and work things out, establish procedures, and test those procedures.

The San Francisco Exercise: Coordinating Federal and Domestic Responses

Randy R. Smith, Retired Lt. Col., Department of Defense Branch Head, Critical Infrastructure Assurance Branch, Security Division, Plans, Policies and Operations, United States Marine Corps

I want to address the exercise planned with the City and County of San Francisco. Mr. Peter Verga and General Buck Bedard described what would happen, what you might receive, as far as Department of Defense support in an untoward situation. Unfortunately for us, Hollywood has done a much more masterful job: People are convinced that what you get is General Bruce Willis, who declares martial law and puts all the people in some kind of concentration camp.

While that movie, "The Siege," was somewhat prescient in describing what happens when terrorists attack New York City, the last half of the movie failed miserably. In reality we didn't send forces in, declare martial law or lock everybody up. So that's not what you get when we say, "We're from the federal government and we're here to help."

Why is the Marine Corps concerned about this? We are charged to be most ready when the nation is the least ready. We are concerned because our defense in the United States is completely dependent upon an interwoven critical infrastructure. Whether it's the 2.2 billion tons coming into the US ports across the country — God knows what might be found in one of those containers here in San Francisco — whether it's the 160,000 miles of interstate highway system, you need to know what that infrastructure is like and what the problems are before you're confronted with them. It's intelligence preparation for the battlefield. It's great for us to know that if we have to evacuate Washington, DC, we can count on I-95 being a nightmare going southbound when people try to leave the city. You need to know those things before the time comes.

In San Francisco, people are certainly concerned about their famous bridge. We're concerned about the bridges that get Marines from bases to deploying points, where we'd send them overseas to fight the enemy.

> Miscommunication is not funny when the local police officer asks the Marine fire team to cover him. Understanding nuances is very important.

And of course, everything depends on power, whether it's natural gas, oil or electricity. When you have an infrastructure that has evolved over time to be the most responsive at the least cost, you have an infrastructure vulnerable to terrorist organizations.

This is a short tutorial on how DoD gets to the fight. This is one of the key issues that we want to talk about when we sit down with the folks in San Francisco. What we're concerned with is once the decision is made to commit DoD forces, how does that work? We want to talk about the tactical level, when

biography

*Retiring recently from the United States Marine Corps after 25 years of active service, **Randy R. Smith** has served in a variety of high-level security and law enforcement positions.*

His military career included numerous tours of duty on both coasts and overseas, a deployment to the Persian Gulf during Operation Desert Storm, and a tour as the Head of Security for the President's Helicopter Squadron. Smith is also a graduate of the 159th Session of the FBI National Academy at Quantico, Va.

After obtaining a master's degree from the Naval War College in Newport, RI, Smith reported to the Headquarters of the Marine Corps where he ran the law enforcement and antiterrorism programs and then was responsible for establishing the new critical infrastructure protection program for the Marine Corps.

He is a graduate of California State University and his personal decorations include the Legion of Merit, Meritorious Service Medal, Navy Commendation Medal (2nd Award), Navy Achievement Medal, Combat Action Ribbon, and the Presidential Service Badge.

Ellis Stanley

the Marine Corps special-purpose marine/air/ground task force shows up to support first responders.

While Northern Command is in charge, they're going to create a joint task force to control DoD forces, and they in turn would work for the lead federal agency. We don't have Bruce Willis declaring martial law — we have a lead federal domestic agency employing those forces.

Post-September 11th, the Marine Corps created an organization focused specifically on anti-terrorism. We organized the Fourth Marine Expeditionary Brigade Anti-Terrorism to respond in a timely manner to a terrorist crisis, whether overseas or domestic.

What do they do? That this is the purpose of the exercise. The key is the command control and coordination relationships: we don't want to be strangers on the battlefield. If something happens it's important for us to understand the nuances of our major metropolitan cities, such as: how do we talk to each other? A lot of major cities talk on 800 megahertz — we don't. We speak different languages. There's a funny adage about the United States and Great Britain being a similar people separated by a common language. But miscommunication is not funny when the local police officer asks the Marine fire team to cover him. Understanding nuances is very important.

Most first responders work with the incident command system. That's not the way the Marine Corps organizes, so understanding the incident command system is important for our responders.

As General Buck Bedard pointed out, we did this once before. The intention here is to work at the Office of Emergency Services level — the level where we have a cross section of agencies involved in response. We don't know, if we sent Marines in, that they would be responding just to the police department — they may be in support of the fire department, particularly if we bring our Chemical/Biological Incident Response Force. That force was created in response to the Tokyo serin gas attack, and it has proven itself time and again, most recently in helping clean up the Senate Office Building after the anthrax attack. We might be in direct support of public works. It may be heavy engineering equipment that comes in. So understanding how that works is important to us.

Who are we bringing to the fight? We're bringing forces from our higher headquarters, from Northern Command, from our Fourth Marine Expeditionary Brigade Anti-Terrorism and from our war-fighting lab. People in our 'war-fighting' lab look at critical infrastructure attack. They're kind of our red cell — they'll come in and tell us how they would take down your city's power grid, how they would drop that beautiful bridge out there. Hopefully, it'll

never happen but we do have people who plan for that.

We're concerned about weapons of mass destruction. I also want to talk about threats that are maybe less catastrophic but more probable, that might confront San Francisco today — everything from suicide bombers to truck bombers.

Having gone for a morning run through this beautiful city, I see that the buildings are very close to the road. These would be a tremendous target for a large truck bomb. It could be absolutely devastating. It may not be the device that Seattle had to confront in its test, but it could be just absolutely devastating. So we want to ensure that as part of our exercise we hit the training requirements from San Francisco's perspective.

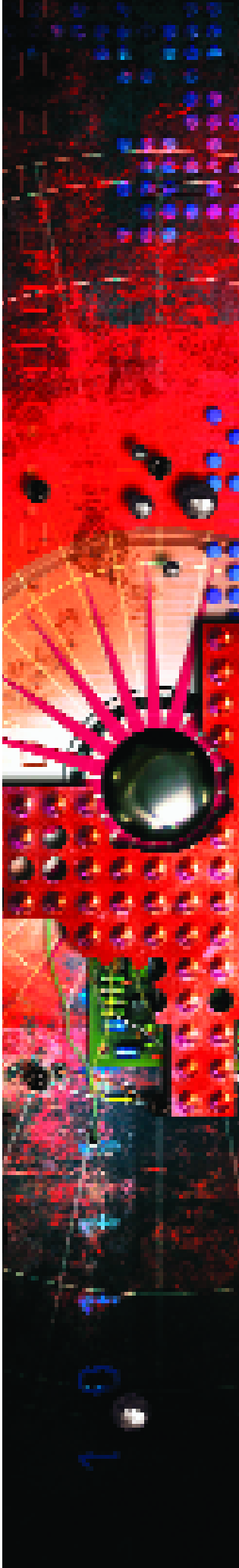
This is what it will be like. The important message is on day one it's share-and-compare techniques, tactics, and procedures. It's also somewhat of a tutorial, an opportunity to have Northern Command describe how they work, to have someone from Mr. Verga's office describe how to engage federal forces. I can assure you — when the phone rang from New York Fire Department to the Chemical/Biological Response Force on September 11th, that's not how you get them deployed. So we want to make sure that people understand exactly how the system works. Then we get down to the tactical level about Marine units in direct support of an agency in San Francisco.

For the purpose of the exercise itself, we'll actually go through a series of vignettes. We'll try to build the case to find the tipping point where the city and county would be dependent upon federal forces — because if they don't need us, obviously we're not going to show up. Then we want to find out where the Marines could best support city agencies.

When it came to the exercise in New York, there wasn't a lot that 800 Marines could do when you're talking about a 40,000-man police department. But if you're talking about substantially fewer resources, what we bring to the engagement may make a tremendous difference.

> When you have an infrastructure that has evolved over time to be the most responsive at the least cost, you have an infrastructure vulnerable to terrorist organizations.

The lessons learned at the end of the exercise are going to be turned into our Knowledge Management Tool. I brought a draft of it today. This was designed to provide a base of knowledge for our commanders who are concerned about going to Iraq or Afghanistan, and instead they have to provide military assistance to civil agencies here — what do they need to know? We're trying to build a tool that they can use in initial planning. It has been pointed out to me that this could be used in the local community as a guide to get and employ DoD forces. We certainly hope to share this, when we feel that we have a good document.



Seattle's TopOFF Experience

Greg Nickels, Mayor, Seattle, Washington

It's a pleasure to be here to talk about Seattle's experience with TopOFF — because the challenges that we face are the same challenges that all cities face, and we learn a lot from one another.

On September 11th I was at home in Seattle. It was one week before the primary election in which I took on the incumbent city attorney and the incumbent mayor. All of a sudden, the world stopped. Seven weeks after the primary I was elected mayor, so my time has been defined by the challenge of homeland security. How do we keep our city and our people safe?

While public safety has always been at the top of the agenda for local government — police and fire services are the core of what we do — this added aspect was new. I made it a priority to make Seattle the most prepared city in America. I suspect every mayor shares that goal.

TopOFF II fit very well with a couple things that we were trying to accomplish. We had recently created an emergency preparedness bureau in our police department, headed by Chief Brent Wingstrand. We had also had a bad experience a couple of years earlier when the World Trade Organization came to Seattle — the connection between elected leadership, command staff, and the people out standing post wasn't as good as it could have been. TopOFF gave us a chance to improve that connection with public safety personnel. It gave us a chance to test our systems.

We were aware that the first TopOFF didn't show the participating cities in the best light and that there was some risk to the exercise. But we decided that the benefits outweighed the risks.

We learned a lot, and I learned a lot. I've spent a lot more time in our emergency operations center than any previous mayor. It was a room that was set aside for years and never activated. In recent years, though, we've had to figure out how to make it work. That was a key part of TopOFF: How do my command staff and I work as a team in that facility to make decisions?

Chicago and Seattle were the two cities involved in TopOFF. The scenario for us was a radiological dirty bomb that had gone off downtown near Tully's Coffee Company. It happened to be a 19-acre site cleared for future light-rail and it was the only open site of that size near downtown.

During the exercise the site was very realistic. They blew up an automobile at the Yakima Firing Range, took a picture of it, and placed the pieces at our site as though the explosion had happened there. This site is very visible

biography

*Seattle Mayor **Greg Nickels** has earned a reputation for his innovative leadership to address transportation, public safety, economic opportunity and other challenges facing the city of Seattle.*

Nickels became the 51st Mayor of the city of Seattle when he took office on January 1, 2002. His priorities as mayor are to build a 21st century transportation system that can move goods and people around the region more efficiently, protect public safety, create economic opportunity and restore neighborhood vitality.

During his first year in office, Nickels worked to strengthen basic city services. He led an effort to win voter approval of an $86 million housing levy, launched a new Emergency Preparedness Bureau in the Seattle Police Department, strengthened finances at Seattle City Light, restructured departments, and pushed customer service by launching 684-CITY, a one-stop, easy-to-remember phone number for city services.

He began his public service at age 19 with the city of Seattle and in 1979 joined the office of Seattle City Councilmember Norm Rice as his legislative assistant. He served in that capacity until his successful 1987 campaign for the King County Council.

As chair of the Seattle/King County Board of Health, he earned a reputation for protecting our children. He took on the tobacco industry advertising aimed at kids and had the Marlboro Man banned from the Kingdome. He succeeded in removing graphically violent video games from Seattle Center.

Nickels has also been in the forefront of the fight for more parks and green space. Nickels has been a passionate advocate of creating a mass transit system and improving bus transit for the Seattle region. He serves on the executive committee and board of directors of Sound Transit.

Nickels graduated from the University of Washington.

Left to right: Dianah Neff, James Sudderth, Mayor Greg Nickels, Curt Levinson, and Robert C. Weil.

from I-5, the main North/South corridor in Seattle, and we were a little bit concerned going in that we would create a panic.

So we spent a fair amount of time figuring out how to communicate with our public, including those for whom English is not their first language. At the end of the day we only had six calls to 911 asking : "What in the world is going on down there?" And let me tell you, there were fires on this site. There was smoke. There were obviously lights and sirens. So we were very pleased.

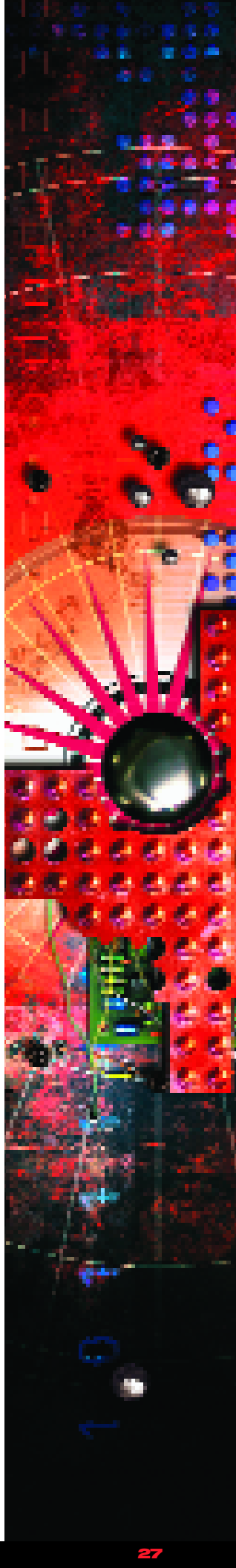
As we got into the exercise, our ability to communicate was challenged. For one, how do you get data on a radiological release in your city? How do you, as a layperson, interpret the data and make decisions?

At midnight the first night I got a call and was asked: "Do you want to evacuate this area in southern downtown?" I said, "Okay — walk me through. What is it we know? What are the risks? What are the challenges? What are the effects of making that decision?" We did that with very general information — a plume map that put a big splotch around my downtown. My question as an elected leader was: "I'm telling people to shelter in place. Most of them will follow it, but some of them are going to ignore me. What is the impact of that? How do we make sure we're not trying to shelter in place too broadly and creating a huge management challenge as a result?"

Chicago's scenario, by the way, was that a terrorist group had released a plague at a hockey game in Chicago between the Blackhawks and the Vancouver Canucks. Because of our proximity to Vancouver, we had a little contact with that scenario, too. Like Vancouver, our health care system was tested. We had live victims in the rubble. Our rubble, incidentally, was inspected and passed by the Occupational Safety and Health Administration. It may be the first OSHA-approved disaster scene in history.

During the exercise we used video teleconferencing. It's a tool that has some promise. For us, it was a little awkward because it was brand new. But there are things we can do to make it work better.

The information connections between local government and state government were also tested. We also learned a lot about working together within our organization and connecting better with external organizations, particularly with the federal agencies with which we had had limited contact.



Proactive Business Continuity Planning

Curtis K.S. Levinson, National Secure Technology and Homeland Security Practice Leader, SBC Communications

I was in New York on September 11th, 2001 visiting a client. Some things were not working that we depend on heavily, such as the public-switch phone network — the only place the telephone network was actually damaged in New York was the Verizon central office in the World Trade Center complex. The overloads that occurred elsewhere in the country were the result of excess subscriber volume. If everyone picks up the handset at the exact same minute the phone system isn't going to work.

Cellular service was not working. My two-way pager, interestingly, was able to receive but not send. US mail was not being delivered. The attacks happened early in the morning, and the postal service personnel who were on the street got off the street.

And lastly, prior to September 11th, one of the most popular business continuity and recovery strategies that we had was overnight delivery. If you needed a Sun server, a Cisco router, any hardware, it was going to get crated to you overnight. No one expected that the skies of the United States would be closed for three to five days, depending on where you were. Organizations that based their recovery strategy on overnight delivery, because they did not want to overextend budgets and warehouse space, wound up without equipment.

Things that did work included the Internet. Internet Protocol's ability to reroute kept most people on the Internet. As a security professional, one of the products that I rail against is instant messaging; however, a lot of people communicated that way on September 11th. The only way that I was able to communicate with my management and my family was from my client's desk by e-mail.

So the Internet was a survivable technology. UHF-VHF, microwave — a lot of that survived. Much of it was overloaded, and there were issues with frequency interoperability, but those technologies survived.

The other technology that worked, which had become relatively obsolete in the United States, was ham radio — amateur radio — people tapping in old Morse code and those technologies. Ham radio operators created a worldwide net. When I travel now I carry a ham radio. Alternative communication technologies are more vital than ever.

So we learned that we need to plan for public system overloads. We had not previously experienced it. We need to take into account that our cell phones may not function.

Voice over Internet Protocol is a strategy, which SBC has worked on extensively. Voice over IP on private networks is an effective backup strategy — not necessarily putting the hard phones on every desk, but there is a product called SoftPhone, which can be loaded on any PC. If it is on a notebook PC and you are connected to the Internet via high-speed broadband, that may be a very useful alternative for people who are at home or traveling or not located at a facility.

Backing up data is another huge issue. Our

biography

Curtis Levinson *leads the National Secure Technology Practice for SBC Communications, a company which provides high level services offerings in the areas of enterprise connectivity, security technology, healthcare informatics and electronic commerce. Levinson's practice includes national and multi-national clients in the U.S. and worldwide.*

Prior to joining SBC, he was the senior vice president and chief information officer of Woodside Travel Trust, a $23 billion multinational consortium. He also served as the global director of secure technology for the Computer Sciences Corporation and was one of the founding members of KPMG Information Risk Management's Secure Electronic Commerce Practice. Prior to joining KPMG, Levinson was the managing partner of LBI Consulting.

He has served as a technology advisor to Chief Justice Warren Burger, Rear Admiral Grace Hopper, The Executive Office of the President of the United States, and the Joint Chiefs of Staff. Levinson has also advised the management and leadership staffs of numerous Fortune 500 and global companies.

He is a graduate of the American University and the London School of Economics. He has also completed post-graduate coursework at the National War College, Columbia University, and the Wharton School of Business.

old mainframe paradigm of data cartridges where we back them up and store them off site — well, now we're looking at technologies like disk mirroring, maintaining live synchronized mirror images at other locations. Also, implementing electronic vaulting, skipping the tapes and instead, sending data over high bandwidth circuits to electronic vaults and storage.

In IT, assets used to mean things within the data center. Now, assets are people, applications, data, and connectivity, and we are looking at distributing them. South Manhattan will never again be the financial core that it once was because those firms that were severely damaged are distributing their assets. Those firms who are located right within the bull's-eye that starts at the White House and radiates outward in Washington DC, are distributing their assets to other locations.

> We learned that we need to plan for public system overloads. … We need to take into account that our cell phones may not function.

Business continuity historically has been viewed as disaster recovery. Now it embraces more: What do we do when there is a virus attack — the next Nimba, Code Red, Love Bug, or denial-of-service? What do we do if our systems are unavailable?

We need to move from a reactive to a proactive position in business continuity planning.

Understand what the potential scenarios are, the risks, and how we can build recovery processes into each scenario. It's hard to dissect critical processes, identify the technological dependencies, build recovery in, and then drill and rehearse until it's second nature.

What's ahead? I would have guessed that something awful would have happened by now. We know that something will happen. Cyber terrorism is just getting cranked up. Many people do not realize is that a computer virus is a cyber-terrorist attack. What would happen, heaven forbid, if a physical attack were synchronized to a cyber attack? A truck blows up somewhere and a distributed denial-of-service attack is launched on our network infrastructure — are we prepared to wage war on the physical front and the cyber front simultaneously? The definition of infrastructure assets has expanded; now we look at human capital and connectivity as an asset.

Virus protection cannot keep up. All it does is keep out the things it knows about. Some kid in a tent is going to write something that the virus filter has never seen and there is going to be an incident.

We in the Western world are arrogant. We assume that because people do not live the way we do, they're not as smart as we are. That is absolutely a mistake. They are equally skilled at technology and understand our culture and our dependence on technology far better than we understand their culture.

Terrorism is not focused on high body count, but on disruption of day-to-day activities, and our information technology infrastructure is a vulnerable target. We need to move away from our mainframe and data center-based paradigm into the network world, which is where our adversaries are. Best practices, innovation — all of the partnerships between federal, state and local need to be involved. A vendor just sent me a thumb drive, which you can buy at Staples. It holds from megabytes to gigabytes. This one has a biometric scanner on it. It encrypts data and the only way to decrypt it is to lay your thumb down. That makes transportation of protected information far easier than ever before.

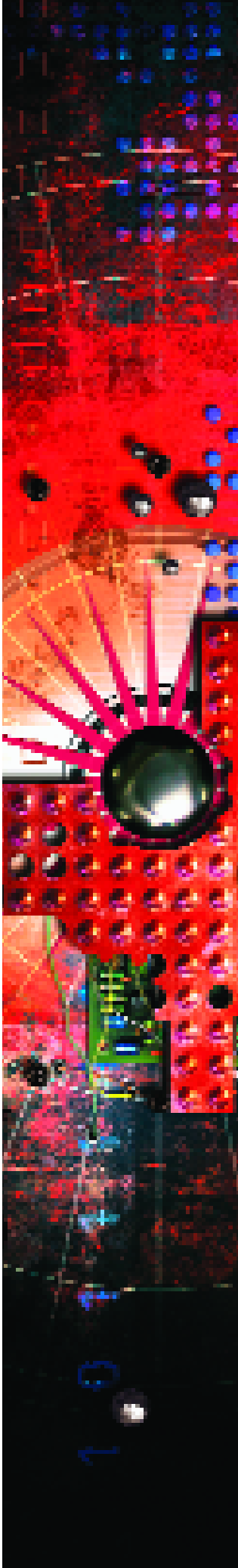
We need to embrace new technologies.

Technology — telecommunications — needs to be resilient. We need primary, secondary and tertiary paths, different media. We need to be flexible, and able to respond in a very, very short time.

When you go to the Web site, the category you do not see there is Homeland Security, yet everyone here knows there are homeland security grants. Finding them and applying for them is an obstacle that clients wrestle with.

So business continuity planning requires that we analyze business processes, identify critical functions, find technological dependencies for each, and incorporate recovery for each technological dependency. It's time-intensive, labor-intensive, it's proactive — it is very unpleasant, and it needs to be done.

Disaster is just around the corner. Any day can



Left to right: Satish Ajmani, Lewis Loeven, and Mayor Willie L. Brown, Jr.

be September 11th. We need to be practiced, prepared, and ready. We need to understand roles and responsibilities. Our corporate choreography needs to be defined and rehearsed. We need to be able to turn the battleship in a bathtub on a dime, and to respond to attacks on multiple battlefields. It is waging war in the cities and on the networks and through technology. We have to respond quickly, effectively, calmly, and clearly.

The single largest application that is critical in business continuity and recovery, which just about every client does not list as a key corporate application, is e-mail. People have general ledger, payroll, all the things they need to recover — but the connectivity provided by e-mail is absolutely critical to how our society functions today.

Consider triage — not everything can be recovered at the same minute. How are things recovered? What comes back first, second and third? Where are our dollars and energies allocated? These need to be evaluated, planned, and documented.

SBC has developed a couple of products since September 11th targeted directly to this environment. One is CAMS, the Crisis Alert Management System, which enables communication and mobilization over multiple fronts. The other is Intellicast, which provides linkage to 911 databases. And SBC, having control and ownership over 60% of the nation's telecommunications infrastructure, is positioned to provide pinpoint coordinates for response.

My practice, SBC Datacom Consulting Services, offers these proactive technologies. Security historically has been a hard sell — "Why should I pay money for something that may not happen? I haven't been hurt yet." We now know that bad things can, do, and will happen — so we provide these to help clients become proactive instead of reactive.

SBC has been involved in critical infrastructure protection since our beginning with the Bell System. We've done a huge amount of work since September 11th to make sure that our telecommunications networks are hardened, available, and redundant. We now provide this service to customers so their readiness matches our own. SBC is far more than a telephone company. It's consulting and infrastructure and services, and that all comes together in the space for critical infrastructure protection.

American Cities on the Forefront of Homeland Security: A Mayor's Perspective on Preparedness

Patrick McCrory, Mayor, Charlotte, North Carolina

One of my first experiences with the concept of Homeland Security was before September 11, 2001 when I toured the City of New York's World Trade Center Emergency Operation Center with Mayor Rudolf Giuliani and several other mayors on June 30, 2001. I'm sure there was well over 50 or 60 million dollars of technology in that incredible room to help coordinate the police, fire and other emergency responders during a crisis. The issues that we were talking about then are not any different than the issues we're talking about now. It's just the circumstances: We've seen the real thing.

As the events of September 11 unfolded, I hurried up to my office on the fifteenth floor of the Charlotte–Mecklenburg Government Center in downtown Charlotte and as I looked out of my office window at the Bank of America headquarters, 62 stories, people were voluntarily streaming out of it and every other high rise in downtown Charlotte. No matter which mayor you talk to or what city you were in that day, everyone had the thought and rationale that they would be the next terrorist target. In Charlotte the rationale was, well we're the second largest financial center in the United States. They hit the financial capital of the U.S., World Trade Center. My God, Charlotte's next. Of course, no one else was thinking that outside of Charlotte, but they were thinking of their own targets within their city.

As I worked to assess the September 11 crisis, the first thing I had to do was to get a report from our police chief, fire chief, and emergency operations director. It was a mere coincidence that at 9:00 a.m. on September 11, our fire chief and police chief were involved in a terrorist emergency response exercise at the Charlotte Coliseum. They immediately left that exercise and came to my office. An old memory came to my mind of Charlotte Fire Chief Luther Fincher coming to me three years earlier asking me to sign a federal grant application to create a regional emergency operations team, and I responded, "Ah, come on, Chief, we don't need this, we're not going to be a terrorist target here in Charlotte!" And he said, "Just sign the damn paper, Mayor!" I listened to him and I am thankful that I did.

To handle the September 11th issue locally, we had to clarify roles, determine how to communicate with each other, with the state and federal officials, and with the public. Second, we had to deal with infrastructure issues, especially transportation. Should we cancel school? We immediately put the City bus system in peak mode, so we could get the mass of people home that were streaming out of the office buildings, because we knew there was no way they were going back up in the office buildings. We also knew we had to take care of the 6,000 stranded passengers at

biography

*Mayor **Patrick McCrory** is one of only three mayors in the history of the city of Charlotte to serve a fourth term.*

McCrory has distinguished himself as a leader in the areas of public safety, economic development, housing, and transportation. He was the recipient of the national Homeownership Hero Award in 2003 recognizing his innovative work in leading Charlotte to have one of the highest homeownership rates in the country.

Since September 2001, McCrory has been called upon by President Bush and Homeland Security Director, Tom Ridge, to identify public safety partnerships between local and federal government and develop a local Citizens Corp.

McCrory serves as president of the Republican Mayors and Local Officials (RMLO) organization and as the U.S. Conference of Mayors chair for the Housing and Community Development Committee. He was also the founder and inaugural chairman of the North Carolina Metropolitan Coalition.

Founder of the Mayor's Mentoring Alliance in 1995, he was presented the 2001 Governor's Outstanding Local Official Award for his mentoring work. He is the only elected official to serve on the national board of the Afterschool Alliance and is a featured Mayor in Harvard University's Faith-based Executive Session.

McCrory graduated with a BA in political science/education and received an Honorary Doctorate in 2001 from Catawba College.

Left to right: Lewis Loeven, Mayor Pat McCrory, and Mayor Willie L. Brown, Jr.

Charlotte-Douglas International Airport, which is US Airways' largest hub. Two of the most important phone calls I got early on that day were, first, from US Airways in Washington, to let me know that none of the planes involved were US Airways. That was a key piece of information because if the terrorists had used a US Airways plane from Washington DC, the plane would probably have come from Charlotte. The other call was from Duke Power Company, our local utility, to say they had taken precautions at the two nuclear power plants that are located within five to six miles of our city limits.

Protecting our critical facilities was a key focus. Frankly, we're still defining our critical facilities at the local, state, and national level. We immediately assumed they included the bank towers, airport, water structures, nuclear power plants, and so forth. That was extremely important, to give at least the appearance of protection. And I want to be candid: a lot of this was strictly appearance, giving the impression that we were doing something to help our citizens feel safe because we didn't know how this tragedy was going to unfold and just how it would impact Charlotte.

The last thing we talked about was communications. Everyone in every major city across the country wanted to hear from the mayor, the fire chief, and the police chief mainly to have peace of mind. These three positions had credibility because they were the most visible people, particularly from what we saw in New York City, and because of Mayor Giuliani. The main message to communicate was one of reassurance, that we had everything under control. We said it over and over again, whether we knew it or not, because we did not want panic. The role of all the leaders, whether it was military, fire chief, police chief, or mayor was to get out in front and say, "We've got our team in place, to the extent that we were even practicing today. There is no problem here. We are prepared. We are not risk-free, but we are safe."

Another key issue for all mayors was community relations. We had extremely nervous citizens in the Arab, Asian, and Jewish communities. That day and week I made sure I visited some of the Muslim mosques and Jewish synagogues. The emergency operations center, to ensure that we could communicate externally and internally.

Now that we have had a chance to reflect on our response to that horrific day, we need to address some of our challenges. One is prioritizing what we need to protect our communities at the federal, state and local level. Government officials give the appearance that we have prioritized our needs, but I don't think we really have. Prioritize what must be protected to keep society moving — that's where we need to put resources, in order to protect from, and respond to, a potential attack.

One lesson learned already is that we must have a coherent strategy, which is generally lacking. We need more money, but what are we going to spend it on, and can it be used for a dual purpose? We shouldn't buy a piece of equipment if it only serves our needs in a terrorist attack. Equipment must be available during other efforts to be cost effective such as for hazardous materials spills or hostage situations. Our strategy should improve linkage within the criminal justice system, where judges currently don't know what the sheriffs do, the sheriffs don't know what the police do, etc. How are we going to stop terrorists if we can't connect our criminal justice system? Equipment and training should address any emergency, not just terrorist events, but even natural disasters, etc. Frankly, I think the odds of a natural disaster are probably greater — we have had terrible ice storms in Charlotte in which we lost power for up to two weeks and two million people in the region were impacted. We couldn't communicate a strategy to help citizens get through the crisis because

people didn't have access to television or radio, in most instances. We have since seen the impact of massive power blackouts from what was experienced in the Northeast when there was a power grid failure.

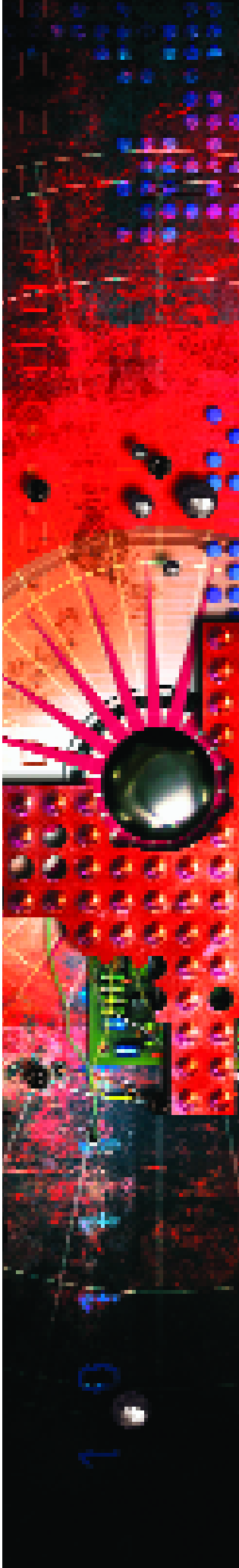
Despite the impulse to buy fancy equipment, and conduct lengthy training sessions, we must first talk among agencies and to the public because if we don't do that, we're wasting our time. We learned from the World Trade Center, for the fire and police not to be able to talk to each other on September 11 was inexcusable. Further, I hear mayors saying, "I need money from the federal government so our fire and police can talk to each other." I say, wait a minute, you should have this already, your taxpayers should be paying for it. We need to spend the federal money on things we can't do alone. We have got to think strategically and not waste this opportunity to best use the influx of federal dollars to build and improve our homeland security plans.

> Prioritize what must be protected to keep society moving — that's where we need to put resources, in order to protect from, and respond to, a potential attack.

In Charlotte, we have a real-time highway messaging system. We have all our emergency operation plans on CD-ROM, so everyone can see them. We have a geo-notification system, which directs phone calls to the appropriate citizens to direct them how to respond, for instance, when power is out. Our other mode of communications is going to be Citizens Corp, through which in an emergency situation, we can notify key neighborhood leaders who are trained on how to respond in a variety of crises, including many of our leaders in the international community. Each jurisdiction must have an alternative communications plan in place.

Many governments over the last decade have gone through a "reinventing government" process and now we must tap into the principles of that concept to use existing resources instead of trying to reinvent the wheel. To put it bluntly, there's a money grab going on right now with all the federal resources committed to homeland security. There's 3.2 billion dollars being distributed in 2003, and everyone's going after this grant or that grant. We have to have a systematic approach to ensure the funds are being used wisely, but more importantly we have to be able to prevent some events or respond properly when the next crisis occurs. For example, money has been distributed to all states, including North Carolina and when I asked our state homeland security director how North Carolina's grant would be spent, he told me he was distributing it on a per capita basis, not based on need, because that is the way it was distributed to the states. Then he said, "You know, Pat, we've got some pig farms in eastern North Carolina. Can you imagine if those got hit by the terrorists, and the environmental damage that would do?" While that statement is laughable, he didn't crack a smile! What he was doing was protecting his political base. So, maybe the money is there. The question is, are we spending it in the right way? That's the main message I want to send.

There are many lessons to learn from that fateful day of September 11, 2001, but the greatest tragedy will be not addressing those lessons and repeating past mistakes, especially when we have the resources and the collective will and support to truly protect our Homeland.



Information Management is Key to Security

Charles A. Hansen, Chairman and Chief Executive Officer, Hansen Information Technologies

Hansen Information is a private company that works with about 12 of the top 15 cities in the US, helping them establish data models and organize information to manage operations better. I talk to a lot of city councils, a lot of mayors. A year and a half ago, the FBI's National Infrastructure Protection Center called about a document we had produced from an old power user survey, from statistics that clients provide to us from their databases.

When Tom Ridge became director of Homeland Security, he asked all federal government to list critical infrastructure., and the resulting list had less than a hundred locations. For example, the FBI, which has 33 field offices and many agents who still do not have Internet access, determined their key assets through the National Infrastructure Protection Center. Since there were no standards to define key assets, some agents listed the police department or the morgue. Some decided not to put in information because it was too sensitive! This is the current status of the key asset list.

So, we took a look at our list, consisting of information from about 300 clients and 19 million work orders, as well as revenue and cost analyses. We had 37,000 bridges — of course the national bridge inventory has about 595,000 bridges. We also had information on public facilities and water treatment plants, which are critical. But the thing that the FBI was most interested in was how our clients consolidated citizen-centered information, so that when a person's address came up, they would know every asset that supported that citizen, every transaction that the citizen had done, every service request that had been called in. In some cases, confidentially, voter information is included. If it's publicly available information, you get a 'bucket" and dump it in.

Through California Department of Transportation, one of our larger clients, we discovered that nowhere in the federal government is there a definition of what a street is. The Transportation Department just wanted to see how much it cost, for example, to clean up an accident. So they have re-inventoried all of the California highways, 97,000 miles of road and 25,000 bridges, in a single database. Now we have the ability to take all of the dots and connect them. In Indianapolis, the mayor not only wanted to know the cost of fixing manholes, he wanted the cost of fixing specific manholes. Not all of this is critical, but it can help with managing cities.

biography

Charles A. Hansen *is Chairman and CEO of Sacramento-based Hansen Information Technologies. Founded in 1983, Hansen serves nearly 400 government clients supplying the world's leading public sector call center, asset management, building permit, code enforcement, licensing, and utility billing solutions, conducting over 1.2 billion transactions each year. Major clients include the cities of Atlanta, Buffalo, Chicago, Dallas, Ft. Lauderdale, Indianapolis, Las Vegas, Los Angeles, New York City, San Antonio, Seattle, Washington DC, Fairfax County, VA, Montgomery County, MD, and the State of California, Department of Transportation (Caltrans).*

As a private company that employs 250 people, with international offices in London, Melbourne, Sydney, and Toronto, Hansen maintains one of the most comprehensive databases of municipal performance information, including over 3.5 million completed service requests, 13 million completed work orders, and over $2.4 billion in labor, material, and equipment costs. Client data also includes information on over 1 million buildings, 100,000 miles of roads, 110,000 bridges, 100,000 miles of water & sewer main, 400,000 hydrants, 1 million valves, and over 160,000 miles of railroad.

Mr. Hansen is a recognized expert in the field of critical infrastructure protection, streamlining government operations, and deploying municipal web portals capable of managing high volume transactions between citizens, businesses, and local government. Each August, Mr. Hansen sponsors the Innovative Government Forum (http://www.innovativegov.com) highlighting technical case studies from leading state and local governments. Last year's conference featured Vice President Al Gore and General Barry McCaffery (U.S. Army Retired) as keynote speakers. This year's conference will feature former NYC Mayor Rudy Giuliani and Former Director of the CIA, Admiral Stansfield Turner (U.S. Navy Retired).

Mr. Hansen earned his B.S. from the University of California, Berkeley (1978), where he rowed collegiate crew, and earned his M.B.A. from the Anderson School of Management at UCLA (1982). Mr. Hansen lives in Carmichael, California with his wife and three children. In his spare time Chuck plays Baritone Sax with Sacramento-based R&B funk band, Hip Service (http://www.hipservice.com).

I want to make five points about security systems. First thing, consolidate your data silos, the points of information that you have out there. Do you realize the US government has yet to consolidate a dozen different terrorist watch lists? After September 11, we learned that Mohammed Atta had 16 street addresses. We also learned that there were over a hundred different locations for information about the buildings in New York City affected by the attacks. So just collecting the information was impossible. Years ago, fire fighters would draw schematics of the inside of buildings. Today, we can make sure buildings provide digital files and layouts for public records, so that first responders can have updated maps when they go to a site. On September 11, there were no maps available for the Pentagon, none. Bringing hundreds of pieces of information together digitally, making it available, is the first barrier we have to break down.

Bringing hundreds of pieces of information together digitally, making it available, is the first barrier we have to break down.

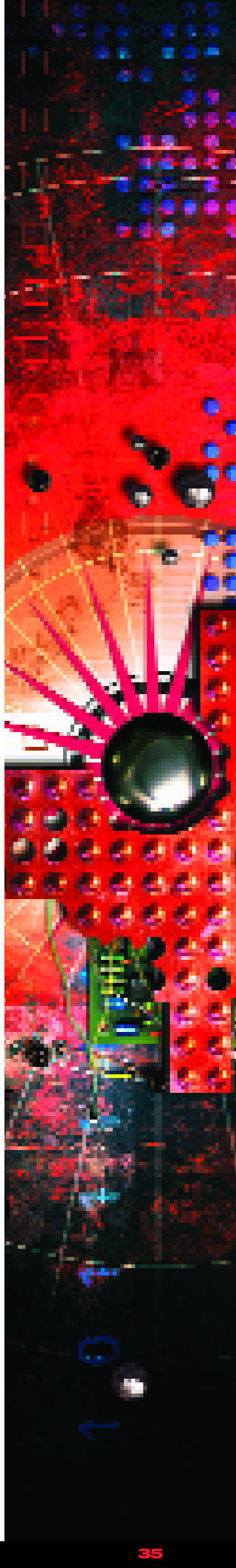
Number two, identify your critical infrastructure. We've created a foundation for identifying assets. I don't want to say critical assets, because that's going to be less than one percent. There are hundreds of potential hot spots in our communities. In that California Transportation Department example, how a local government defines that road is going to be different from how the state government or private entities defines it. We need to be on the same page. Again, everyone's got a sanitary sewage system, but some parts are more important than others, such as the parts underneath airports — the easiest way to get in to the airport. Take a look at your 24-inch and 36-inch storm drains, it is easy to go in there. We can stick a TV camera in there and video is stored, so you already have information on what it looks like. We need to combine traditional assets that we work with every day with other critical information.

Third, manage everyday information. I believe there are more than ten million targets of opportunity in the US yet to be identified. Citizen action centers and emergency call centers were overwhelmed on 9/11. Even today, 40% of all 911 calls are for non-emergencies. Normal citizen transactions —parades, permits, graffiti removal, code enforcement violations, all of the business things that we deal with have to be accommodated in the data model. For example, addresses — the record number I've seen, in a medium-size city of 150,000, was 200 file locations for a citizen's address. There is no way to find a Mohammed Atta with 16 addresses if we have addresses in hundreds of locations. Identifying and eliminating those disconnects is key. Normal transactions have to be well managed to deal with homeland security, so that when an emergency happens, information flows effectively. It has been said that if 20 agencies put their citizen services on line but they don't work together, it just digitizes the confusion. It still means the citizen has to walk through 20 doors. This is where people have to roll up their sleeves. It's not an easy area to fake. It takes work, and it is essential.

Fourth, architecture is changing. It's getting a lot easier to deploy information. It is becoming simpler to make things available, so any device, in any location, has access. You cannot deploy a first-responder system that requires software to be downloaded onto the PC to make the application run, and expect it to work all the time.

Last one, five. Don't reduce staff, increase revenue. This is a business. Homeland security is costing us $138 million as U.S. cities struggle with payroll cuts, service reductions, tax increases. We see more business management of city government. You either have to raise existing fees or create new ones, reduce or hold the line on services. Do you know what people do, what their activities are? This is activity-based costing, measuring performance. Finally, what do you want to do with critical assets? You don't necessarily want to pay less for them, but perhaps to get more for your investment.

So, consolidate your data; identify your critical assets; create your citizen action centers; manage information; understand the technologies that are out there; and don't cut staff, increase revenue. We need government to be very powerful. We're going to get there, but how? I'm convinced, as we look at privatization, understand our cost of doing business, each of the businesses that we operate can help. We need to work together and stay on top of performance, we can't say that enough.



PDAs on Patrol: Technology Takes to the Street

John Abraham, Officer and Safety Coordinator, Seattle Police Department

Thank you for this opportunity to give you the results of the study that was performed in Seattle on the use of personal digital devices in law enforcement and officer safety.

I am a full-time police officer, a motorcycle officer in the city of Seattle. I split my time between working traffic and the Safety Office. I am responsible for the workplace safety of 1,250 sworn officers and over 600 support staff.

We in the Seattle Police Department recognize the need for critical information on the scene. Using secure wireless technology, authorized officials can gain access to any priority data source within seconds. Information captured may be put into a database, analyzed, and instantaneously retrieved. This is an asset to an officer because our data network can be overloaded due to warrant verification through that system, which can take an extended amount of time. We found officers in the street that waited 20 to 25 minutes for a name or license plate inquiry to come back. That's unsafe. That situation aggravates the person behind the wheel, who expects to only be held a couple of minutes for a traffic violation, and the officer, who has maybe had an extremely long day, wearing body armor, a wool uniform, and carrying 25 pounds of additional equipment. It does not build a good relationship with the public.

Here is what can result from a traffic stop. Timothy McVeigh was captured because a state trooper pulled him over. Ted Bundy was caught because a Seattle police officer had previously stopped his Volkswagen in Seattle and had him identified, so it was referenced at a later date. David Berkowitz was captured because of a parking violation in New York City. Malvo and Mohammed were captured by a truck driver that had seen the car parked at a rest stop and advised the appropriate authorities. Aileen Wuornos, the only known female serial killer, was captured driving the truck of one of her victims. Last but not least, Kenneth Bianchi, the Hillside Strangler. He committed several homicides in the LA area, then moved to Washington state and killed two college students. He was captured because his vehicle was recognized.

All of these were traffic-related incidents. In the United States, we lose approximately 150 police officers a year, about 30% of them the direct or indirect result of a traffic stop or a domestic violence situation. Traffic stops are a potential threat to police officers, and information is necessary.

In our study, each product was tested by the same nine officers, so the input was consistent. They told me exactly what was right and wrong with each, and which was best overall. The study took place over 18 months, but subtract changeover periods and it was a six-month program. A software application called Choice Point gave us the ability to do name checks using Social Security, date of birth, last known address, phone numbers, name, partial name, partial name partial date of birth, partial Social Security number partial name.

We took people that did not have access to mobile computers or data terminals. So, we had detectives, a couple of motorcycle cops, and a couple of bicycle units — people who work with the public on a regular basis, but do

biography

*For the last 17 years, **John Abraham** has been an officer for the Seattle Police Department, and for the last two years has served as its safety coordinator, responsible for the workplace safety of 1,250 sworn officers and more than 600 staffed civilians.*

Prior to his current duties, he was the deputy sheriff with the Clallam County Sheriff's Department and worked as the head of security for the Pacific Northwest Region ITT Rainier Timber. Abraham also served in the U.S. Navy for 13 years.

His instructor certifications include: Emergency Vehicle Operation, UPS Smith System Vehicle Operation, Radar and Lidar Handheld Speed Measuring Devices, Lidar Technician, Scuba Diving, Fitness Coordinator, Glock Firearms Armorer OSHA Instructor in Rules Regulations and Standards, and Traffic Safety.

He is a member of the International Association of Chiefs of Police, Washington Association of Sheriffs and Police Chiefs, Washington Governors Safety and Health Advisory Board and the International Critical Incident Stress Foundation.

Randy Smith

not have access to the equipment necessary to run names.

During the test we received 9,682 queries. That includes probably 8,000 queries that would not have been run without this tool. The reason is that officers are not going to bother with data, run a name or a plate, because of time. They need to be on the street. We made over 400 misdemeanor arrests during that time, 55 felony arrests, over 600 Department of Corrections contacts. Whenever you run a person in Washington who is on parole or probation, it goes through the Washington Crime Network and the transmission is forwarded automatically to his or her parole or probation officer. This allows them to know if somebody is in violation of parole or probation. For example, if a sex offender is near a school on a regular basis, and a proactive officer keeps seeing this person or his vehicle and continues to run him, this will produce a stat sheet for his probation or parole officer to possibly revoke or change the conditions of parole or probation.

During the test, 75 suspended vehicles were taken off the road. When we stop a driver with a suspended license, we can impound the vehicle. The driver gets a suspended license ticket and he gets back into the system. Hopefully we can prevent him from driving in the future and causing some kind of situation.

The officers involved in these stops knew that the people were violators that needed to be handled in a specific way. They maintained control of the situation.

Units were tested for usage and versatility in the street. I would suggest that you get something that can withstand a drop from a shirt pocket to the deck. We lost two Palm 7Xs when they dropped from officers' pockets. Research those that are more durable, understanding that the more rugged ones are also more expensive.

I asked my officers to tell me what they thought of the PDA. This tool turned out to be more valuable than we ever imagined. It was directly responsible for us making more than 30 felony arrests, at least 25 documented Department of Corrections arrests, and a multitude of misdemeanor arrests. Having the ability to run a name gets some information immediately. Remember I told you it took 20 to 22 minutes to get a name back, if the data system was extremely busy? This way, the name comes back in somewhere between 8 to 15 seconds. By the time you've written the name on the traffic violation, you have their report back. So if they have a warrant, if they have a suspended driver's license, the ball-game changes. You can call in an additional unit, and take care of this situation peacefully.

Peacefully, that's the key. We highly recommend this tool be issued to officers. It allows them to identify people who provide false information warrants and court orders in an expedient manner, without tying up additional patrol resources or ID section. This is critical in Seattle, because we have had to reduce forces. There is a move to make us more in touch with the public. So we're trying to have our officers spend more time on the street, rather than in patrol cars. This tool permits an officer to park his or her vehicle and still be in control, check names, and be in touch with business owners and the public.

PDAs give us access to all the information necessary for officers to do their job in a safe, timely, and professional manner. I cannot emphasize safety enough. The reason I took on this project was because I've been to too many police funerals. They have assisted us in making numerous arrests, enable officers to run names more quickly and get information about outstanding warrants, case numbers and warrants numbers. Having PDAs makes stops of suspicious persons easier, and allows us to detain people for less time.

PDAs give us access to all the information necessary for officers to do their job in a safe, timely, and professional manner.

For those concerned with cost efficiency, this technology gives us more bang for the buck. There was a Drug Enforcement Agency study involving 1,350 special agents over a 24-hour period, average wage $50,000. They calculated 3.8 million dollars in time saved — time when they could be doing something else on the street. It greatly enhances proactive involvement, rapid access to accurate information, and prevention. That is crucial. Secure wireless information technology and the rapid access to accurate data that it provides enables you to prevent crime because you have information. Equipment such as a combined phone, pager, wireless PDA with walkie-talkie capabilities provide common, interoperable communications platforms for all users. It is a cost-effective way to enhance safety. Thank you very much.

Information Technology and Homeland Security: The Federal Perspective

Mark Forman, Administrator, U.S. Office of E-Government and Information Technology

Thank you for the warm welcome. It is my pleasure to participate in this excellent set of meetings on homeland security. I would like to bring the federal government's perspective to the discussion. Today, we are at the cusp of transforming the way government works. Our current technology and management knowledge allow this change, and the need for homeland security demands it. I want to focus today on federal initiatives for managing information technology (IT), particularly on initiatives that integrate enable federal, state, and local governments to work together effectively.

Let me begin with an overview of the President's Management Agenda, aligned with the administration's overall management general reform approach, comprising five components. The first component is developing strategic management of human capital, which will become increasingly important as 50% of the federal workforce becomes eligible for retirement in the next five years. The second component is financial performance management, which addresses the federal government's chronic problems in erroneous payments, financial management systems, and other areas of accountability as had the rest of the country. The third component is competitive sourcing, public-private competition for commercial functions, which we are just starting to address federally. The fourth component is performance integration, which ties budgeting and spending to program results. The fifth is expanding e-government, which is the component I am responsible for. E-government is focused on modernizing the federal government.

E-Government

The purpose of e-government, as in the entire management agenda, is to make government more citizen-centered and less agency-centered. The 58 billion dollars we spend on IT result in a difference in government's service to citizens. A key result I see is making government — typically thought of as slow and bureaucratic — work faster through IT. It's as simple as shrinking decision making time from weeks down to hours.

biography

*On April 16, 2003, **Mark Forman** was appointed by President George W. Bush to be the administrator for the Office of E-Government and Information Technology. He is the first person in the federal government to fulfill responsibilities normally associated with a corporate chief information officer.*

Previously Forman was associate director for IT and E-Government at the Office of Management Budget (OMB). Under his leadership, the U.S. federal government has received broad recognition for its successful use of technology and e-government.

He is charged with managing over $58 billion in IT investments and leading the President's e-Government Initiative to create a more productive, citizen-centric government. He also leads the development and implementation of federal information technology policy, and is responsible for a variety of oversight functions statutorily assigned to OMB.

Forman also oversees Executive branch CIOs and directs the activities of the federal CIO Council, as well as chairing or being a member of several key IT-related boards including the President's Critical Infrastructure Board. To improve results from federal IT spending, Forman created a framework that couples cross-agency teamwork and leadership with a government-wide IT budget decision process built around a results-driven modernization blueprint. He also led the successful definition and development of about 30 multi-agency e-government and e-business initiatives.

Prior to joining OMB, Forman was a vice president of e-business in Unisys Global Industries, where he was responsible for global public sector e-business and e-government initiatives. Prior to joining Unisys, he was a principal at IBM Global Services where he was responsible for definition and deployment of the global public sector e-business strategy.

Before joining IBM, Forman was the senior professional staff member on the majority staff of the Senate Governmental Affairs Committee. He was also the senior advisor to the U.S. Senate on federal acquisition and procurement issues and information technology issues.

Forman is a senior fellow of the John C. Stennis Center for Public Service. He holds a MA from the Harris Graduate School of Public Policy Studies at the University of Chicago and a BA from Ohio State University.

E-government means more than just putting up websites. It means using digital technologies to transform the way we do business, making our services better and more efficient. It also means using market-based approaches, in some cases outsourcing management and services, and focusing on results more than on spending. E-government initiatives are unique because they always impact other components of is tied to the rest of the management agenda; for example, if we using technology to improve our business processes, that change will help federal workers be more productive, and to improve financial performance, we need better productivity from our IT. Overall, the purpose of e-government is being used for making the federal government simpler and to unify government organizations, thus improving efficiency, effectiveness and service quality.

With the advent of the Internet, the way people work has changed, and the federal government has not fully understood that yet. The federal government is still largely paper-based. Yet in the private sector, people have adapted to a real-time environment where decisions are made rapidly because information is shared and business processes are conducted on-line.

Mark Forman and Lewis Loeven

People's interaction with government has changed from a physical to an electronic one; every week, half of the people in America are on-line dealing with a government websites. So we need to focus not just on having more IT but on working together, government with government, agency with agency, to reach citizens the way they expect to reach us.

Services to Citizens

A well-managed e-government approach has to look at what our citizens — our customers — want. They want services and information that are easier to access. Hence we focus on simplification. They also want better coordination of information across federal, state, and local levels, which e-government can provide and is required for homeland security. To give citizens better services, the Administration has adopted a four-part e-government strategy over the past two years. First, to reduce redundancy across federal agencies, we have created "one-stop shops" such as FirstGov.gov, our official web portal. Whether you're in state and local government, a business, or a citizen, you can access the portal's easy-to-use, consolidated services.

Second, we have highlighted government-to-government cooperation, a key feature of FirstGov. We have leveraged the technology to reformulate the way governments work together, from grants management to disaster planning. For example, we are working to make grant processes simpler and focused on getting better results.

Third, because most federal transactions are with the business community, we are simplifying and putting these transactions on-line (over 8,000 right now), making them easier to carry out. The Paperwork Elimination Act requires that by October 2003, all our transactions be electronic, from grants management to disaster planning. We are thus running the risk of merely shifting the bureaucratic burden on-line. So, instead we are leveraging e-business approaches to reduce the burden on business as we put transactions on-line.

Fourth, as the fourth part of the strategy, we are integrating our administrative processes so that there is no unnecessary paper passing, even electronically. This means that the federal government is applying technology to simplify and integrate functions

such as purchasing, payroll, recruitment, and security clearances.

To implement the strategy, we chose 400 key redundant agency projects and consolidated them down to 24 cross-agency projects, thus simplifying and unifying federal services around the customer. We organized these projects into four portfolios, in line with the four-part e-government strategy. I will be highlighting the government-to-government projects, since we are focusing efforts on restructuring the way governments work together. But there is other important projects consolidation work, such as e-authentication, which allows us to define consistently the trustworthyiness of the parties involved in transactions as government goes on-line across many agencies. In these efforts, we have learned that restructuring government services is complicated — because the government is! A key issue is redundancy in IT, withthat several agencies involved inperform the same workline of business because of the structures of their appropriations bills. I know state and local governments are dealing with the same sorts of issues. Grappling with these complexities is necessary to modernizing government processes.

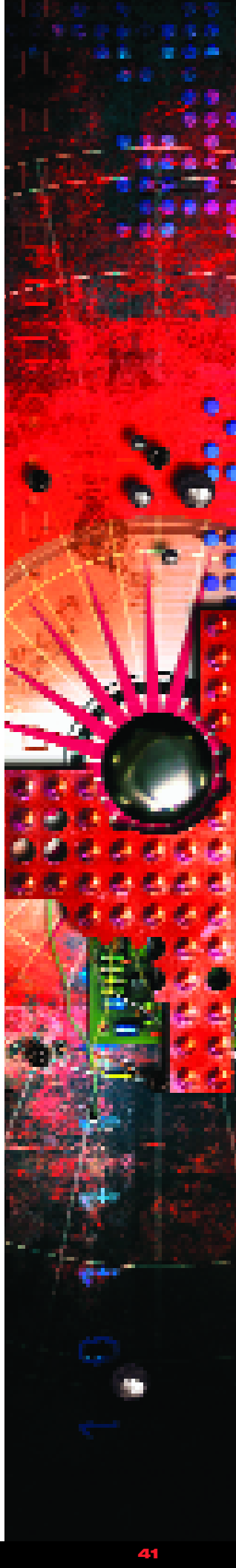
> The purpose of e-government, as in the entire management agenda, is to make government more citizen-centered and less agency-centered.

Modernizing Federal Government Processes

Although in consolidating access to services, we have solved a number of IT management problems. We know that IT solutions alone will not make government run more effectively. We also need to address problems with underlying organizational issues, which we is a key focused on first in modernizing the federal government processes. Another important component has been reducing redundant buying by reforming our business architecture to get economies of scale and interoperability. Also, because of the cost overruns in many programs, we have looked at changes in program management. Since the federal government has so much invested in IT, we have had to set some priorities, figuring out the relationship between organization change, process redesign, and use of IT. What we call these "modernization blueprints" has guided our work on priorities.

Another key element of modernization has been reducing "islands of automation." In June of 2001, we found that the government already had 22,000 websites. Thus, it was almost as hard dealing with the government on-line as in person! The fact is that federal government depends on local and state governments to deliver services. So we have focused on simplifying and unifying these independent separate IT investments sites, not only to improve citizen services but because homeland security demands that our people can use their computers to work together can talk to each other effectively. For example, if there is a terrorist threat that has to be dealt with by sharing information, there has to be organized processes and interoperable IT available, working through IT, to allow that. Also related to homeland security, of course, is cybersecurity. It has been a challenge to make communications across organizations secure, and we continue to make progress using a structured approach to alleviating cyber-security issues.

We have made significant progress in our modernization efforts, with 23 of the 24 cross-agency projects making key deployments. Any resistance to change hasn't come from the average federal employee, but from those intimidated by changes in the bureaucratic culture they have been successful dealing with. Nevertheless, we have worked as a team and seen important results. For instance, FirstGov has changed from an inefficient search engine to an efficient "three clicks to service" model. The numbers tell the story; in 2001, 6.7 million Americans tried to get service at FirstGov; this year we're running 6 million a month. We are also seeing good results in business-to-government transactions. Almost 50% of all businesses were on-line doing transactions with us in January 2003. And the partnerships across agencies that allow make efforts like FirstGov successful, to work have created increasing been driving partnerships teamwork within the agencies.



We are also making measurable progress in cybersecurity. We have gone from about 30% of systems secured to 50 or 60 percent, with a goal of 80 percent in 2003. 60 percent is a failing grade — I'd like to see us get a B! Interestingly, we're finding that when IT projects did not build in security from the beginning, we have had to do costly patching. But, when we can build it in from the start, it actually costs less. We are trying to make progress in IT workforce reformsreduction too. Over 80 percent of the federal IT workforce comes from the vendor community. I want the federal employees who work in IT workforce to focus on project management, because that's what drives the re-engineering that makes us more effective.

Our future work will remain dedicated to improving policy results. We want to reduce the cycle time, the response time of government, which is — very important in providing dealing with homeland security threats. We want to get errors out of our IT systems that affect results. Also important are cost controls, for example in the software used by many agencies. We established an enterprise licensing initiative that combines the purchasing power of agencies to reduce the prices of widely used software. And more broadly, the E-Government Act commits us to using IT to foster ongoing dialogue with state, local, and tribal governments and to find innovative ways to collaborate.

Government-to-Government Projects

To finish, I want to focus on our initiatives linking government to government, some of which are relevant to homeland security. These were identified two years ago through focus groups made up of state and local government officials.

- *Grants.gov.* This project, already operational, creates one portal for all federal grant customers, making it easier for potential recipients at other government levels to learn about and apply for grants. This eliminates waste, for example the need for governments to hire "bounty hunters" to find grants. Also, grants have been managed so that we don't know which grants best meet recipients' needs; this project addresses that problem. www.Grants.gov is currently in its pilot phase, with the "find grants" capability. By October 2003, we hope to launch the "apply" capability for the bulk of grant moneys. This will allow governments to complete joint applications or use a single integrated application, eliminating wasteful paper-based processes.
- *E-vital.* This project, just rolling out beyond the initial states, just getting started, will establish common electronic processes for federal and state agencies to process, verify, and share birth and death record information. Accurate and consistent vital statistics are important for homeland security and for avoiding waste through erroneous payments to deceased recipients.
- *Disaster management.* This initiative is crucial to homeland security. It allows us to provide federal, state, and local emergency managers with on-line access to disaster management information and to planning and response tools. After September 11, state and local first responders told us that figuring out who to work with in the Federal Government was taking so much time that it hurt their ability to save lives and protect property. So we have been working to simplify and unify that process. We have established a consolidated website, www.Disasterhelp.gov, that which gives all jurisdictions a toolkit for interoperability. The site pulls together geographic and disaster response tools, making it simpler for federal, state, and local first responders to work together, for example through secure instant messaging. Now we are testing the interoperability system through disaster preparedness exercises. We have also been working to simplify and unify the processes that first responders use in working with the federal government.
- *Geospatial One-Stop.* Here we have consolidated information so federal, and state, and local agencies can have a single point of access to geographic data. Studies showed that 50 percent of governments' geospatial information was redundant, so we developed standards for interoperability of that data. We also constructed a portal, www.Geodata.gov that gives governments and citizens access to basic frameworks and tools for sharing data on geospatial categories like transportation and climate. Thus, data will no longer have to be

collected and purchased separately. This unification is important for disaster planning, environmental response, and infrastructure decisions related important to homeland security. I'm not a geographic information systems expert, but I'm told that this project is revolutionary and extremely useful.

- *Project Safecom.* This initiative is intended to help federal, state, local, and tribal public safety agencies improve response through more effective and efficient interoperable wireless communications. Again, we are addressing an issue very important to homeland security. When we started the initiative, we had over a thousand interoperability wireless pilots under way; we saw that it was unrealistic to reach interoperability with so many projects. Project Safecom will. We realized we have to identify the key elements of IT architecture and applications and then work to unify wireless communications systems. The radio and voice piece is important, but local governments and law enforcement officials tell us that the essential information they need for public safety comes from computers at the base station. For a fraction of the cost of most trunk radio systems, we can use IT to get much better data directly to first responders. But we still need to construct interoperability—decide on systems architecture, requirements, and agreements between jurisdictions. Most importantly, this initiative has to develop from the local level up. In all five initiatives, in fact, we are trying to change the top-down way the federal government has worked in the past.

So, of the five projects only Safecom and E-vital are non-operational. However, they are very close to full implementation. In June 2003, the Safecom project held the kick-off meeting for its IT architecture work. State and local public safety associations, county managers associations, the National League of Cities, and the National Association of State CIOs are all involved in working on the architecture.

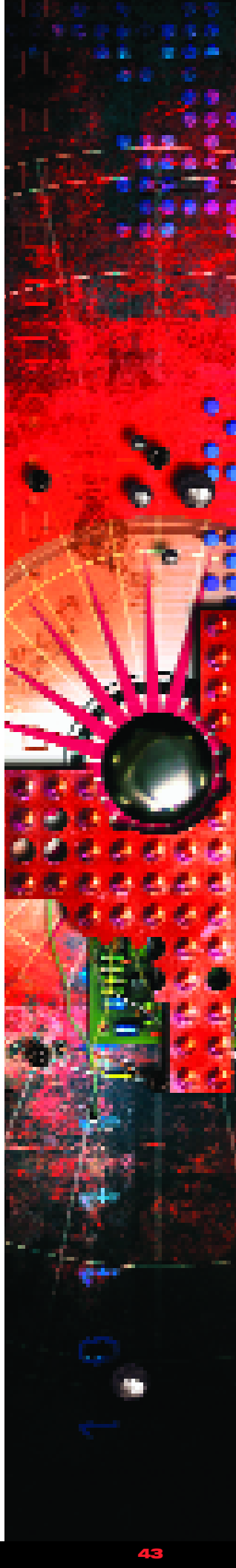
Other Key E-Government Projects

Two other major projects deserve notice, one in the government-to-citizen and one in the government-to-business area.

- *GovBenefits.* This initiative provides a single point of on-line access for citizens, community organizations, or faith-based organizations to determine their eligibility for government benefits and services. As an example of the integration involved, there about 410 federal programs for social services, and each had been providing its information separately. on the Internet. www.GovBenefits.gov is intended to reduce that 400-stop shopping to one-stop shopping. Any citizen seek and find relevant federal benefits programs are now accessible through use of the GovBenefits eligibility-screening tool. Most state and local government benefits programs are tied to GovBenefits, and we have been working with states and some localities on an integrated benefits application form. This form can be used by cCitizens, organizations, and caseworkers can use the GovBenefits tools.
- *Business Compliance One-Stop.* This initiative aims to reduce the burden on businesses by making it easier to find, understand, and comply with relevant laws and regulations. For example, in business licensing, you need federal, state, and local licenses for transportation and other aspects of your business. We want to reduce the paperwork burden involved in that, so we've been working to get all government levels to integrate their processes. This project is also working to harmonize reporting requirements in a variety of areas.

Conclusion

We have a lot of exciting working going forward in e-government. How do we drive that change at the federal level? All of the items on the President's Management Agenda, and the agencies involved, are scored on their status and progress every quarter. When an agency or agenda item is not making progress, that gets the President's attention, since he is very concerned about the quality of government management. So there is accountability for results at the highest level, and that motivates change. Also, when an agency is not progressing in my area, e-government, we know why, because the scoring is based on key quantitative measures. So we can analyze the agency and understand how to improve efforts, looking at chronic problems



that may be preventing modernization.

But to move forward, we not only have to assess our own work but also work with others, work with all of you, to get the "breakthrough thinking" we need to innovate. This is not government business as usual, but when we're dealing with things as important as homeland security or Internet access to services, business as usual is not an option. We are finding that once we break through to new ways of operating like those I've shown you today, we do get big performance improvements. And that requires your help. Jointly, we do business cases for each IT initiative. So if you're interested any of the projects I've presented, I encourage you to get involved in our initiatives, whether in business case development or, helping us deploy e-government solutions. We especially encourage you to work with us on the disaster management and wireless communications projects. We have a very open-door policy.

We are already working with many groups, as I've mentioned — governments, businesses, and organizations like PTI, a technology nonprofit funded by a lot of local governments. We look forward to collaborating with many of you. We know that we can't create e-government magically; we need the ideas and assistance of everyone involved. I thank you very much for your attention.

Information Sharing and Emergency Response—A Portal Approach Supports An Extended City Government Enterprise

John Antenucci, President and CEO, PlanGraphics

In the atmosphere of increased risk and threat, U.S. cities must look beyond traditional approaches and legacy information systems. The current environment requires an integrated approach to information technology that supports planning, response, and recovery to man-induced and natural catastrophic events. At the same time, recognizing the financial constraints that cities must operate within, the most effective system for disaster planning and response must serve other city functions on a daily and operational basis.

There are powerful benefits to cities that commit to this integrated enterprise approach:

- Clearly, the investments made are leveraged over a broad range of city functions—yielding a cost efficiency not otherwise achievable.
- Information is collected once and shared many times assuming consistency across the enterprise.
- The security and control to information assets may be managed centrally or by individual data custodian agencies as required.
- The natural propensity of agencies to "stovepipe" and duplicate data collection and maintenance, as well as computer application development, is thwarted in lieu of a more collaborative approach and multiplied benefits.

Underlying this integrated enterprise approach to disaster planning, response, and recovery systems (DPRRS) are the spatial and temporal attributes of the information assets which are critical factors since all events occur at a specific time and place.

Though the integrated enterprise DPRRS relies on spatial information, its operational requirements go far beyond the functions typically associated with geographic information systems (GIS).

The requirements call for a data-centric approach, utilizing virtual or physical data warehouses and repositories. To provide the highest levels of flexibility within a diverse or "extended enterprise"[1] common in emergency response situations, the data-centric approach is complemented by a "portal" architecture. Using the portal architecture as the backbone (see Figure 1) of the DPRRS assures that legacy applications and databases can be brought together in a common operating environment while allowing the original custodians of the data or applications to maintain relevant levels of control and security. The requirements for a data-centric approach also go beyond the traditional view of geographic information to include a wide

[1]Extended Enterprise—Traditionally the term "enterprise" information system describes deployment and use of a system throughout a public or private entity, e.g., city, utility, and involved multiple agencies or departments. In today's environment, the "enterprise" of an entity typically goes far beyond its own organizational structure. As an example, a city government's extended enterprise may include other cities, the surrounding counties, and state and federal agencies, as well as its vendors, citizens, business community, and visitors.

biography

John Antenucci *is the founder, president and CEO of PlanGraphics, a systems integration and implementation company that provides a broad range of services in the design and implementation of systems where spatial information is a key attribute.*

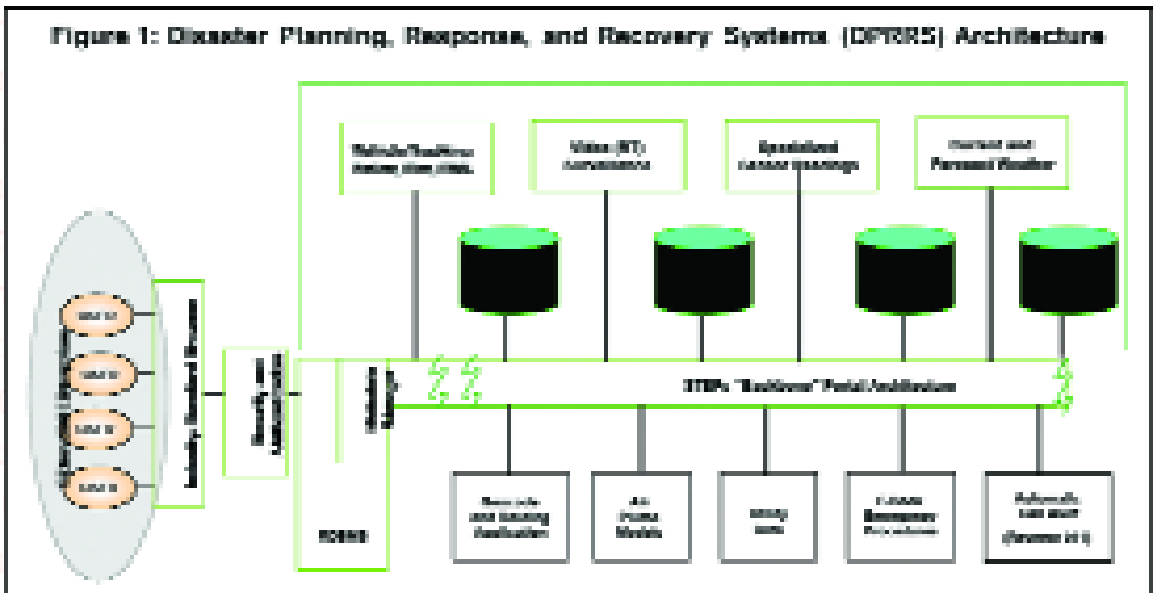
He remains active in the delivery of client services, which include strategic planning for geographic information systems (GIS) product and service suppliers, as well as end users of technology; management and financial studies for public and private organizations; and technology innovations and technology transfer programs, both domestic and international.

He has worked closely with senior executives of some of the nation's largest aerospace and defense industries aiding the commercialization of dual use technologies with particular emphasis on spatial information management and application systems.

Prior to founding PlanGraphics, Antenucci served as president of AM/FM International (now GITA), a professional association for utility industry users of GIS.

In addition to taking on numerous leadership roles in professional organizations such as the National Academy of Sciences Advisory Committee, he is also a published author. He co-authored the foundational text, Geographic Information Systems — A Guide to the Technology *and the* Manual of GeoSpatial Science and Technology.

Antenucci holds both an MS in civil engineering/water resources and a bachelor's degree in civil engineering from Catholic University.



range of rich content and unstructured data, as well as conventional alphanumeric databases. The rich content and unstructured data may include aerial photography, building/structure photographs, engineering drawings, real-time surveillance video, linkages and URLs to other systems, real-time sensor data, and more.

PlanGraphics' enterprise portal architecture as applied to DPRRS, is called STEPs (Spatial Templates for Emergency Preparedness). STEPs provides a robust and flexible environment for accessing, sharing, and distributing data and applications while recognizing and assuring the security (and, if necessary, encryption) of data and applications within the authorization level of each unique user. Equally important, the database environment supports both physically centralized and virtual data warehouses reflecting the nature of the data (static, dynamic, real-time) and the institutional considerations of participating organizations.

The STEPs architecture can be quite straightforward and its implementation equally so. The primary components include:

User Access	Standard Industry Browser (e.g., Netscape)
Computing Device	"Low-end" desktop or laptop, PDA, etc.
Database	Server hosting security, authentication, and encryption application (if required), metadata manager and metadata, (optionally) retains static data, data translators, URL pointers
Database (cont'd)	
Data Warehouse	Virtual and/or physical, function of institutional environments and DPRRS requirements
Application Suite	Variable, a function of DPRRS requirements
Network	Hard-wired, e.g., Ethernet, Internet, intranet (wired and wireless), secured and unsecured, redundant if required

STEPs' rapid deployment is facilitated by a relational database hosted metadata manager and a series of "templates" that provide "preconfigured" access to data and applications supporting the DPRRS.

These templates function as "tabs" to an "index file" allowing an inexperienced user (as are most first responders and those called to support an event) to quickly access the required information or application with little or no prior knowledge of the sources, formats, or technical details and as little as one hour of orientation to the operations of STEPs.

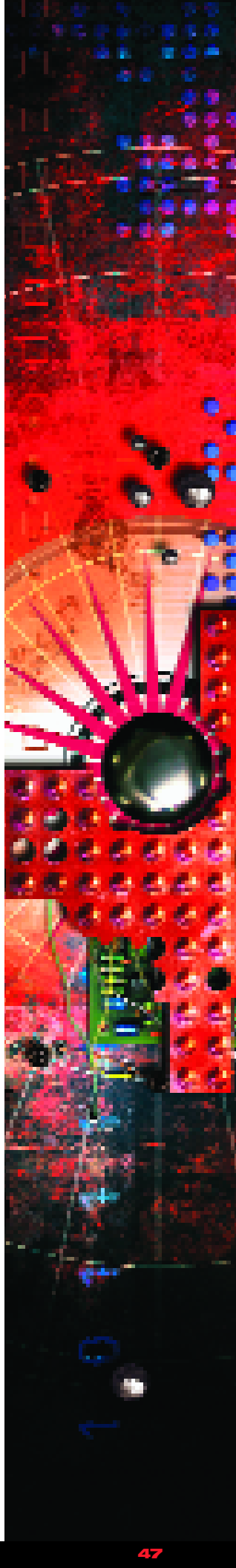
Table 1: STEPs Template Functionality

Template (function)	Fairfax County	New York City	Oracle World	Note
GIS (all themes)	•	•	•	ESRI, Intergraph, Smallworld, MapInfo, et al.
CAD	•	•	•	AutoCAD, Bentley
Aerial Imagery	•	•	•	Skyline software
E-book		•	•	ICTS procedure handbook
Geocoding	•	•	•	Navtech, GDT client databases
Asset Records	•	•	•	Underground utilities
Asset Images	•	•	•	Utility components, structures landmarks
Routing		•	•	Shortest path by transport method
Vehicle Tracking	•	•	•	Based on GPS
Weather	•	•	•	Current and forecast
Air Dispersion Model	•	•	•	Static and dynamic
Building Characteristics		•	•	From real property management systems
Census/ Socio-economic	•	•	•	Federal and local sources
E-notification	•	•	•	Alert technologies
Event Management	•	•	•	E-spatial
Chemical Hazard			•	Compressus

STEPs is typically implemented in three steps:

1. Requirements definition
2. Prototype deployment
3. Incremented deployment (content, security, range of contributors/users).

Prototypes can be deployed within 90 days in most operating environments following the definitional stage. Federal and state funds can be used to implement STEPs as an enhancement or an extension to emergency operations centers.



Teaching Old Equipment New Tricks: Bridging Communications Barriers

Charlie Giancarlo, Senior Vice President and General Manager, Switching, Voice and Storage, Cisco Systems Inc.; President, Cisco-Linksys LLC

Cisco was once described as the arms supplier to the Internet revolution. But as in most revolutions, the bureaucracy is the last to find out and continues as it had before. A lot of our work with the DoD and agencies in Washington still involves specific networks — where it's not an issue of national defense, secrecy or confidentiality. Those organizations couldn't share information if they wanted to, other than by voice or fax. You want the ability to share information and the security to limit the sharing to specific organizations or individuals.

We see similar opportunities to improve communication between public and private sector agencies, not just in a national emergency but under normal circumstances, to allow the public safety organizations to be more productive with the equipment and systems they have today.

biography

Charlie Giancarlo *holds several key roles within Cisco Systems, Inc., a worldwide leader in networking for the Internet. He leads four groups in the Cisco development organization, including the technology team responsible for Network Switching, as well as groups focused on emerging technologies and new markets: voice, storage and security. Giancarlo also chairs the Cisco Enterprise Business Council and is responsible for developing and executing Cisco's business strategies.*

In addition, he is president of Cisco-Linksys, LLC, an independent division of Cisco that was acquired in early 2003, providing wired and wireless products for the high growth consumer and the SOHO networking market.

Prior to joining Cisco, Giancarlo was vice president of marketing and corporate development for Kalpana, Inc. He was also a cofounder and vice president of marketing for Adaptive Corporation, which developed the industry's first Asynchronous Transfer Mode (ATM) product for the LAN market.

Giancarlo holds an MBA from Harvard and an MS and BS in electrical engineering from the University of California at Berkeley and Brown University, respectively.

We know that there are increasing demands and responsibilities on organizations — police are not only expected to respond to traditional trouble but in circumstances such as terrorist attacks, truck bombs, and so forth. We have growing concerns about technology interoperability — different agencies, organizations, operating on different frequencies, radios, systems, and the difficulty of coordinating action.

Communications is something that we do very well: we pick up the telephone and can talk with almost any other person in the world. But when we talk on the systems that we use on the job, that ease of communication stops.

We are all facing a budget crunch. Even if we weren't, we would need to leverage existing communication systems instead of replacing them every time there is new technology. The Internet has largely done this in the commercial arena. The Internet started out working on DDS lines between universities, then between companies on T1 lines, optical fiber, and Ethernet lines. It operates on dial-up lines, which is how the Internet first reached consumers. It also operates on DSL, cable and satellite systems.

The Internet leveraged the technology that was in place, enabling everyone to communicate on a worldwide basis. Why are we not doing this in our public safety systems? Generally, they are proprietary systems — applications designed for an ambulance or a police car or a helicopter — and only available for that system itself. Everything was integrated and couldn't be leveraged for any other things.

Instead of upgrading equipment, we can use each separately to pass the same type of data and then tie them together with a security system. So you can use existing equipment for new and advanced data — whether it is voice or the video systems of the future.

What we're suggesting is to go from proprietary systems to standards-based systems, from text-based or voice-based applications to rich media, depending on the processing power that you have at the end point. To go

Left to right: Simon Hakim, Charlie Giancarlo, and Moshe Porat in front of Cisco's police car.

from proprietary data for specific communications equipment to information that can be shared locally among different public safety providers — police, fire, and ambulance — or under emergency circumstances, nationally. Instead of changing the radios or other end-point equipment, use what is in place, but put on Internet Protocol data and tie it together at the core, something the commercial environment has been doing for years. It is then available in a format that can be shared not only among agencies, but also with public and commercially-based services.

In an environment based upon Internet Protocol, you have device independence. You can use Palms, radios, scanners, IP phones, IP-based radios and 80211 wireless, which is becoming extremely popular. Access is transparent. This can operate on any radio system, public or private.

Then you have a high-performance standards-based network that can be shared among governmental functions because it's a standard IP network. If security is needed, you can put secure protocol on top of that. And I'll remind you that on 9/11 the one thing that continued operating in Lower Manhattan was the 80211 wireless network and the Internet. There were a number of firms in Lower Manhattan using Internet phones when regular phone service was out.

> Communications is something that we do very well: we pick up the telephone and can talk with almost any other person in the world. But when we talk on the systems that we use on the job, that ease of communication stops.

The Internet was developed to survive a nuclear attack, so it is very resilient. It has a standard database and computing infrastructure that can be shared with specialized devices and standard PCs.

Over time we can develop policies regarding where information is shared. For police radio traffic, the policy may be that it stays within the local force unless certain events occur or unless a certain type of call occurs. If it's a medical emergency, the policy could change to share radio traffic with the local ambulance capability. If it involves fire, radio traffic can include the fire emergency teams and so forth.

The applications are quite varied. To share voice traffic among different forces on

different radios, you broadcast or multicast to the appropriate radio at the appropriate time. You have kept the equipment in place, but you've enabled it to share information. It is a lot less expensive. We can also provide database access, sharing the same data on a variety of equipment. Then of course you need to consider things such as identity verification.

Video monitoring is quite interesting. We have a deployment in Seal Beach in which police cruisers use 80211 — called WiFi. They can roll up to businesses that have video-monitoring equipment let's say, in a warehouse. Because they have the security keys to the network in the warehouse, they can observe the video on a monitor in their squad car. They see the bad guys real-time before they have to rush into the building. The same capability enables the police to do fleet management when they roll into the garage; 80211 is connected to the equipment in the car and they are able to assess its condition as they come in.

We believe that by going to a common infrastructure, data format and protocol, and providing access through existing equipment, you take agencies beyond the narrow confines of proprietary applications to achieve increased safety, operational efficiency, enhanced information sharing among agencies, and real-time resource allocation.

Take,for example,a police cruiser that is used in Buffalo Grove. It is enabled with a mobile access router, a small device designed for a harsh environment that can take a variety of radios and/or physical connections. Regardless of where the vehicle is or how fast it's going, it picks the best connection available, automatically makes sure it has connectivity, and enables all the devices in the car to talk to the network — private or public, whatever it might be.

As long as there is an Internet Protocol connection, there is rich data communication to that vehicle — voice, data or video. The routers are also enabled with 80211, so they can work either in or around the squad cars or the device. Things can be set up quite easily.

Once the infrastructure is in place it's not very expensive or difficult to add new applications.

Once the infrastructure is in place it's not very expensive or difficult to add new applications. An example of this is NASA: When the astronauts were up in the shuttle they communicated with earth by radio through Internet Protocol, going into computers and various systems. Two years ago we sent up an IP telephone. By adding that device, the astronauts could call any individual telephone on the planet, including their families. So instead of having to ship up a central-office switch, a complex telephone system, an IP telephone was able to create an entirely new application.

Once the Internet Protocol infrastructure is in place in a public safety environment, the ability to share valuable information multiplies by the number of agencies that get onto that infrastructure.

Technology shouldn't get in the way of interagency communications. A lot of the infrastructure in place today can be used if what we settle on standards for information and protocols that operate over those devices. We believe that will allow us to access information anywhere at any time.

Homeland Security and the Private Sector: Enhancing Capabilities

Charles Wilhelm, Retired Gen., United States Marine Corps, Director of Homeland Security, Battelle Corporation

I'd like to express personal and professional thanks to the City of San Francisco and to Temple University for seizing the initiative and conducting a conference that we really need.

I've been employed by the Battelle Memorial Institute, which employs 16,000 people at over 70 locations worldwide, the majority of them scientists and technologists. We manage the Pacific Northwest National Lab in Richland, Washington, Oakridge National Laboratory in Tennessee, Brookhaven National Laboratory on Long Island, and we co-manage the National Renewable Energy Lab in Golden, Colorado. This means that Battelle has immediate access to cutting-edge technology emerging from these Department of Energy laboratories. We are one of the leading entities in the world in dealing with chemical and biological threats and have been for quite some time.

The dominant culture within Battelle is the United States Army Chemical Corps.

They are intellectual heavyweights: microbiologists, chemists, physicists — and really, they've pointed the way for a lot of the developments between the first Persian Gulf war and the second Persian Gulf war.

It occurred to me that only a general can lose a war and only a rifleman can win one. What does that have to do with this audience? The mayors of our cities are the riflemen in homeland security — the very important business of protecting our nation. Ultimately you have to win the war, and in this war failure is not an option.

I want to talk from a private sector standpoint about homeland security, defining the challenge as we at Battelle see it, then talk about solutions, and about Battelle's flagship program, designed solely and exclusively for application at the state and local level. It is not Department of Homeland Security or Washington D.C. focused.

Everyone in this room is a manager. We identify a need or a requirement and then we design an organization, make a plan, and execute it. We tend to do this sequentially. Today, however, we find ourselves in the position of having to organize, plan, and execute simultaneously, and this is true at every level — whether it's Secretary Tom Ridge in DHS, a governor, or a mayor. It's not easy because our processes and procedures — the way we approve budgets, allocate resources — are sequential processes, and they are not fast enough to meet the need.

We're confronted with chemical, biological, radiological and nuclear threats while we do in-stride reorganizations and try to fill infinite requirements with finite resources. Time is not on our side. I am shocked that as much time as has passed since 9/11 without a second event. If you had suggested to me that we were going to cross the border from Kuwait into Iraq, take down that regime, and suffer no pain in the homeland I would have taken exception with your statement. Well, old generals were wrong again, thank God.

biography

Charles E. Wilhelm, *a retired four-star Marine Corps General, is vice president and director for Battelle's Office of Homeland Security, one of the world's largest independent, nonprofit research and development organizations. Wilhelm is responsible for homeland security issues within Battelle's government market sectors.*

After a distinguished 38-year career in the military, Wilhelm retired. A career infantry officer and a veteran of combat operations in Vietnam, Lebanon, the Persian Gulf and Somalia, Wilhelm commanded Marine units at every level, from Rifle Platoon and Company Commander in Vietnam to Commander of the II Marine Expeditionary Force and all Marine forces in the Atlantic, Europe and South America. In his final military assignment, he served as Commander of the United States Southern Command where he was responsible for all U.S. military activities with the 32 nations of the Caribbean and Central and South America.

Wilhelm is a graduate of Florida Southern College and holds an MS from Salve Regina College. He is also graduate of the Army Infantry Officer's Advance Course and graduated with highest distinction from the Naval War College.

Charlie Wilhelm and Simon Hakim

Last December, we had to be concerned with not only the Iraq theater of operations, but what might happen in the United States. Why? Because all of our forces weren't in Iraq. We had aircraft, armor, command and control mechanisms and transportation assets that were still in the United States. Suppose the major ports and airfields through which those commodities and troops had to flow were closed off. We would be in one hell of a mess.

We started to come up with the worst case scenarios, and we wondered, how does Saddam Hussein see this? We talked about a countervailing strategy — simply stated, we take Basra, he does San Francisco. Tit for tat across the board, to test our national resilience and inflict real pain on the United States.

It didn't happen — again, thank God. Why? Maybe a combination of two things — perhaps I underestimated the effectiveness of our three-letter organizations. We may also have overestimated the level of organization and the capabilities of those who wish us ill.

Nevertheless, time is not on our side. We don't know when it's going to happen, but when it happens it will probably not be the event that we expected. We present a target-rich environment to terrorists — 361 ports, 429 commercial airlines, two-and-a-half million railcars, 7,500 miles of land borders and 95,000 miles of coastline. Look at the farmlands that make us the best-fed nation in the world, and think about the effects of a biological event on our food chain. Then you get to our most lucrative target our cities.

In 1985 Mike Myatt was the Director of Expeditionary Warfare on the Navy staff and he wrote a document entitled "Chaos in the Literals," about the places where we would most probably find conflict in the 10 or 20 years that followed. The centerpiece was the importance of cities in homeland security. Where are major ports? Where are major airfields? The answer is they're either in the middle of or contiguous to cities.

To think about homeland security, I use four Ps — the first one is **P**revent the act from taking place. If that fails, then we have to be **P**repared to respond. My fatalistic notion is the events will occur, and the events will occur in cities. So there's really no place for us to go and nothing to do but to confront the **P**roblem. The last P to me is the one that's most important. At the end of all of this we've got to **P**revail. If the event occurs we have to have the mechanisms in place so that a handful of political radicals or religious extremists won't succeed.

So the notion that I've presented to Battelle — "Find a place you can play in the top three and you'll be supporting number four" — is a way to think about it.

How do we meet these challenges? This is a huge information technology enterprise, and I want to share a couple of observations from a meeting that I had with Secretary Frank Libutti, who is responsible for information analysis and infrastructure protection in Department of Homeland Security. He said, "I've got only one focus, and that focus is down. I have to put an information structure in place that collects vast amounts of information, then synthesizes that down into digestible pieces that first-responders can work with. I've got to get it to them in a timely way, and I've got to create an operational picture that is the same from coast to coast."

The real challenge as I see it is that we have a 283-million-man army. We have to have the information technology to educate our population. People have to see the threat in a common, constructive way. Public/private alliances to me are absolutely essential — this

is a collective enterprise or we don't make it, in my view.

Resources will be a challenge and time is always against us. So I think what we have to look for are those really comprehensive, synergistic, end-to-end solutions. We cannot focus on piecemeal solutions. We have to take comprehensive approaches, to think in terms of systems of systems. They may be imperfect. They may be 60% or 70% solutions. But if we address only a part of the problem, we will be hit in the part we didn't think about.

Let's talk about the division of labor among federal, state and local levels. These [items on the slide] are not meant to be exclusionary entries. It's not to say that medical and bio-terrorism preparedness is purely a federal undertaking. But to solve the problem that's where we have to start, and we haven't gotten off to a very good start.

For example, I really liked it when the Centers for Disease Control said, "Within 30 days we're going to provide smallpox vaccinations to a half-million first responders. Then we're going to up to 10 million so we're ready for that threat when it appears." Ten weeks later they had done only 50,000 and had hit a couple of roadblocks. One was the lack of confidence on the part of the hospitals and the medical institutions that the resources would be there to execute the plan, and another was the health service workers who were concerned about the effects.

Are there technical solutions to that? You bet there are — better vaccines. Right now it takes us 18 months to protect a soldier, airman, marine or sailor from anthrax — a total of six shots with an annual booster. We've got to do better than that. How do we achieve the required capabilities? I don't think there's anyone that can touch us in terms of our science and technology capabilities. But they have to be leveraged. We have to have a sense of priorities. I've asked security leaders: "What's going to cause you not to sleep tonight?" The answer in almost every case is, in this order: biological, chemical, radiological, or nuclear event. Bio jumps to the top in every case. So those are the places where we have to start.

Providing integrated and cost-effective solutions — the key is to move forward as fast as we can on a broad front addressing as much of the threat as we can. Get the 60% solution in the hands of the first responder now. Chart the course to a 75% solution and have an idea about how to get to 90%. Forget about the last 10%. Nobody is going to wait for it and it's more than likely too expensive. And the technology is moving too fast. Researchers don't like that — they're perfectionists, but they've got to be realists.

It isn't all technology. There are simple common-sense measures we need to take. I don't think people know what numbers to call when they see a possible terrorist threat. We need to improve societal discipline. I get angry when I hear somebody moaning because they have to stand in a line at an airport. The price of security is inconvenience, America. Live with it. We need to stress that to people.

Left to right: Mayor Jeremy Harris, Manny Menendez and John Marks.

I will close with Battelle's SPEAR Program — the Statewide Program for Emergency Preparedness and Response. It focuses on threats, providing comprehensive solutions. It contains 13 components, and integrates 13 systems and enterprises to meet broad needs on a broad front.

The objectives, as are indicated on the chart here — again, this is a program that was conceived, designed, developed and is being implemented solely at the state and local level. We recognize that cooperation is important. Adjacent cities don't need to match each other capability for capability. It is important to achieve regional solutions, complementing each other rather than competing at the state and local level. If we're proximate, we can share capabilities.

The best, fastest and most comprehensive capabilities at the lowest cost is the answer. This is a problem we can't admire — we've got to solve it. Start with a comprehensive risk assessment. Risk assessments were done under FEMA protocols, but need to be updated. Identify critical gaps, prioritize them, and then start to fill them.

A very important point — it is very much community-focused and it recognizes economic and fiscal realities. It is market-sensitive and vendor-neutral. It tries to find a local supplier of services.

We need to take things that we have now — handheld radios, repeaters, computer systems and software — and make them work together. That's exactly what SPEAR does: It takes all of these previous investments and it makes them work with each other.

The last point is probably the most important one where SPEAR is concerned. It is scalable and flexible. When we go into a city or a state there are going to be unequal needs and resources. A program has to prioritize requirements with local leaders, determine the range and depth of capabilities required, and design a solution for that jurisdiction. You can shift priorities as threats change.

The SPEAR focus is to protect the public and then preserve critical infrastructure. It is functioning in a number of regions right now. The SPEAR program starts with a risk and vulnerability assessment. It provides for surveillance and detection; critical infrastructure protection; equipment acquisition and training; communications and interoperability of communication systems; medical preparedness; planning, training, exercising, and public protection; response and recovery planning; continuity of government and operations; and risk communications. It also addresses agro-terrorism and the important issue of sustainability. These programs have to be kept vital over time.

> We're confronted with chemical, biological, radiological and nuclear threats while we do in-stride reorganizations and try to fill infinite requirements with finite resources. Time is not on our side.

This is where SPEAR is today: Alabama, Georgia, Iowa, and Illinois. In other areas, we are in the process of sealing the deal, and in still others, we have ongoing dialogues. We have four corporate partners in this program: Olive Tree deals largely with non-governmental organizations based in Utah; Titan; WebMethod; and Duberry Davis. The solutions lie in coalitions, industry coalitions where we complement each other. Battelle is not big enough to be the prime contractor, but we have niche capabilities that complement the efforts of larger organizations.

E-Government Innovation in Honolulu

Jeremy Harris, Mayor, Honolulu, Hawaii

In 1998 the City of Honolulu embarked on a long-range program to expand and improve public services through the application of digital technology. Our goal was to create a "paperless city," where barriers to interdepartmental communication were broken down, operational efficiencies maximized, and citizen access to information and services was easier and more seamless than ever before.

The decision to modernize was driven by necessity. Between 1994 and 2002 city revenues plummeted, as real property values suffered from the prolonged effects of the burst of the Japanese "bubble" economy. While the national economy grew at an annual average rate of about 4 percent between 1992 and 1999, Hawaii's economy shrank by an annual average of 0.3 percent. Honolulu's tourism-based economy was also hit hard by the Asian currency crisis of 1997-1998, which cut into international visitor arrivals.

By the end of the decade the city faced three choices: cut services, raise taxes, or increase government efficiency. The latter option was the only one that made sense during tough economic times. So we set out to reorganize government, increase operating efficiencies, and reduce our workforce by leveraging technology. Technology was one of the tools that allowed us to build a smarter, more responsive government with increased police, fire, refuse collection and transit service—all of which were enhanced without raising property taxes. We continued to hold the line on spending as the city's fiscal condition worsened. By 2002, real property tax revenues were down $62 million from what they were in 1994.

Though city revenues have declined over the past decade, Honolulu has significantly advanced its e-government capabilities. In 2001, a comprehensive review of e-government applications in 223 American cities led the Civic Resource Group to determine that Honolulu had one of the best Web sites among cities of comparable size. Last year, for the second consecutive year, the Center for Digital Government's Digital Cities Survey ranked Honolulu first among cities with populations greater than 250,000 for using digital technologies to improve the delivery of services.

While the attention we've received has been gratifying, there's more to the expansion of e-government than an award-winning Web site. Honolulu's quest for greater efficiency through technology is rooted in discussions I had with our chief information officer more than a half decade ago about the role we expected technology to play in the city's future. Out of those conversations came a plan to make Honolulu one of the most digitally advanced cities in the country.

The IT vision developed for Honolulu featured three main components. First, we

biography

*The eleventh mayor of the twelfth largest municipality in our nation, Mayor **Jeremy Harris** is characterized as one of our nation's most dynamic urban leaders. Born on December 7, 1950 in Wilmington, Delaware, Harris says his life began when he came to Honolulu as a student more than thirty years ago. He earned two related undergraduate degrees in biology at the University of Hawaii and a master's degree in Population and Environmental Biology, specializing in urban ecosystems, at the University of California at Irvine.*

He began his professional career as an instructor at Kauai Community College, teaching oceanography and conducting reef walks and classes for keiki *and* kupuna. *He also served as a Marine Advisor with the Sea Grant Program at the University of Hawaii.*

Mayor Jeremy Harris first ventured into politics as a delegate to the 1978 Hawaii Constitutional Convention. At the age of 29, he was elected to a seat on the Kauai County Council in 1979, and served as Council Chairman for two years. In 1984, he joined the Honolulu City and County government as Executive Assistant to the Mayor, and was soon promoted to Deputy Managing Director and then Managing Director. Harris holds the distinction of being the city's longest serving Managing Director, having held that post from 1986 until 1994.

Upon the former Mayor's resignation in July 1994, Harris became Acting Mayor of Honolulu. He was elected Mayor in a September 1994 Special Election and was re-elected in November 1996 and again for a second full term in September 2000.

set about building a more responsive, customer-centered government to deliver public services more conveniently and cost-effectively. We sought to accomplish this, not with the intention of meeting customer expectations, but with surpassing them. In an increasingly interconnected world where people shopped, retrieved information, and accessed financial and other vital services online, the time had come to make city services easier to access as well.

Second, we wanted to wean the city away from its longstanding dependence on paper. The ability to publish documents in digital form significantly reduces the cost of storing, retrieving, and transferring information. Moreover, the paper trail creates unnecessary barriers to communication by separating the data essential to city functions along departmental lines. For many cities, the result can be a bureaucratic and highly decentralized operational structure. Computer technology helps remove the barriers to information flow and encourages interconnectedness throughout the city system.

The third component of Honolulu's IT vision was the development of a user-friendly Internet portal to promote tourism and international business. Our city has responded to an increasingly competitive global travel and tourism environment by marketing Oahu as a strategically located island paradise that offers numerous advantages to international businesses beyond sun and surf. The Internet provides not only increased visibility but also tremendous flexibility in spreading the word to visitors and entrepreneurs throughout the world. Perhaps the most widely acclaimed of Honolulu's Web-based marketing initiatives is our sophisticated geographic information system (GIS) that provides visitors and investors with site-specific, detailed information about commercial real estate opportunities on the island of Oahu. The enhanced GIS is one of the reasons our Web site has become such an important part of the city's economic development plan.

Last year, for the second consecutive year, the Center for Digital Government's Digital Cities Survey ranked Honolulu first among cities with populations greater than 250,000 for using digital technologies to improve the delivery of services.

Customer Service

Not long ago the people of Honolulu had no choice but to renew motor vehicle registrations by mail, stand in line at City Hall to pay property taxes and apply for permits, and get their information about city programs and services over the telephone.

While many citizens still rely on traditional modes of delivery, for a growing number of islanders the Internet has become a more convenient way of doing business. As technology improves and more people are made aware of the range of services available to them online, we're confident they'll take advantage of the electronic alternative.

The trend is encouraging. Over the past two years our city has processed approximately 11,000 motor vehicle registration renewals online at an estimated savings in mailing and processing costs of $10,000 per year. While that's still only 1.4 percent of the total number of renewals per year, online service is growing at a terrific rate. The total number of online registration renewals in 2002 was up more than 326 percent over the previous calendar year. Equally encouraging are surveys suggesting that up to 60 percent of Oahu's 876,000 people has access to the Internet. Such figures have led us to believe that we've only begun to realize the potential of technology to improve the quality of life on our island. The less time people spend in their cars on their way to City Hall and standing in line once they get there, the more time they'll have to spend with their families and enjoy the natural beauty of Hawaii.

Honolulu's "satellite" city hall system may be revolutionized in the years ahead as the acceptance of online service delivery grows. Currently, the city operates 11 permanent satellite offices in neighborhoods and communities on Oahu, in addition to two mobile satellites serving citizens in outlying areas. Our island is a lot bigger than many people realize. All together, the City and County of Honolulu encompasses an area of

about 600 square miles. Hence, the rationale for the satellite system has been to bring services closer to where people live, instead of making them drive to the downtown area where the majority of government offices are located.

The growth of Internet service delivery may eventually allow us to rethink this sprawling, bricks and motor customer service operation and reassign the 92 full-time employees that staff the facilities. But we're not there yet. The total number of customer service transactions executed by the city in 2002 was just over 1 million. A realistic near-term goal would be to increase the number of online transactions to 10 percent of the total.

Public education will help stimulate acceptance of the Internet as a primary means of service delivery. At the same time, we recognize that some people prefer face-to-face interaction with city government, and we intend to honor that preference. Accordingly, the city has recently modified its on-site payment system to keep lines to a minimum and expedite the flow of transactions at our satellites. Under the old system, customers had to wait in line at a separate cashier station after getting their licenses, permits or registrations. Now, all customer service representatives take care of business transactions and accept payment at the same time. By adapting a point-of-sale software system to existing workstations, the city was able to forego the purchase of more expensive registers. This single innovation has enhanced customer service and resulted in a one-time savings to taxpayers of more than $2.6 million.

Public Safety

Digital technology has revolutionized law enforcement and disaster management, dramatically reducing response times and making it easier to send and retrieve information critical to our city's first responders.

In recent years, Honolulu has moved aggressively to equip law enforcement personnel with the technology they need to do their important work more effectively. In 1998 the city obtained $9 million in matching funds from the federal government to reengineer the Honolulu Police Department's electronic workflow system and take advantage of new methods of acquiring, sharing and storing information. Our goal was to minimize the time officers spent doing paperwork manually so the bulk of their energies could be devoted to community policing.

With the introduction of a state-of-the-art computer-aided dispatch (CAD) system and installation of mobile data computer terminals in the city's fleet of patrol vehicles, HPD communication systems are as advanced as anywhere in the country.

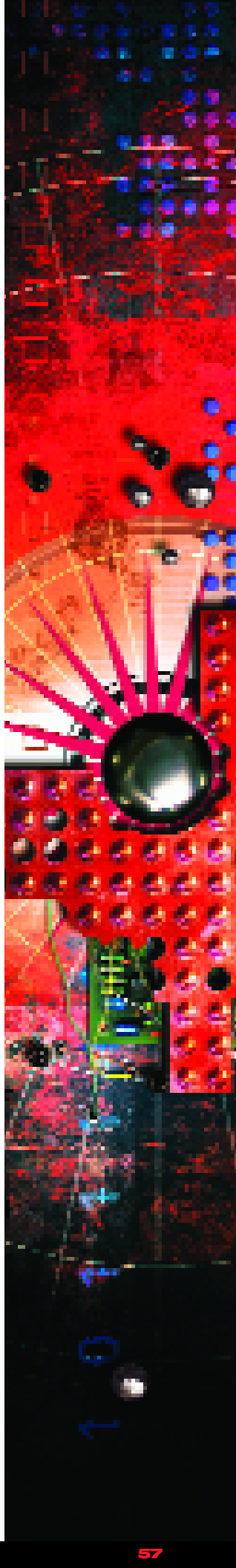
The primary link between dispatchers and our officers in the field, the CAD system has streamlined the call process and significantly reduced response time. Voice communication remains an essential part of the dispatch process, as there is no substitute for human contact in the immediate aftermath of serious incidents. The CAD system augments voice communication and promotes speed and efficiency by enabling dispatchers to transmit volumes of information crucial to police investigations using voice-less data transmission.

Police investigation procedures have been refined through the use of mobile data terminals in squad cars. These on-board computers allow officers to electronically transmit their reports to the Department's records management system. Because of the integration of automated field reporting with HPD's records management system, detectives are able to access information in a fraction of the time it used to take. The city is currently field-testing additional enhancements to mobile field reporting. By the end of this year it will be possible for officers to call up mug shots and other graphic data from their patrol vehicles.

Such advances are part of the broader reengineering of systems in Honolulu's emergency response complex. Along with police reports, data from fire and emergency services is stored in computers at our Emergency Operating Center at the heart of the city's Civil Defense Agency. There, city personnel are able to track the locations of emergency response vehicles using global positioning satellite (GPS) technology. The result is coordinated response to emergencies of all kinds.

The Paperless City

Honolulu's digital revolution involves more than selling services over the Internet and upgrading emergency communication systems. Much of our modernization is aimed



at creating a workplace where data are organized and shared across departmental lines. It's also about enabling and empowering city employees to adapt to the changing demands of the information age.

Last year we launched a multi-year project to address the need for departments to electronically store, retrieve, share and manage the documents they work with. Though still in an early stage of development, the Integrated Imaging and Document Managing System has improved productivity, eliminated duplication, and uncovered "islands" of useful data embedded in the paper files of many departments and agencies. By creating a common repository for electronic documents, teamwork is encouraged and decision-making processes are enhanced.

Part of this same initiative is our Web-based workflow system that allows city employees to complete more than 80 forms by computer and route them electronically through the approval process. The electronic workflow initiative has simplified and streamlined the routing process citywide at a projected one-year savings of $250,000. It is a particularly significant development for paper-intensive departments such as human resources, where reduced processing times and integrity of data are vitally important to personnel management.

The process of tracking and approving city permits was among the most labor-intensive of activities under the old manual system. Today the city uses an automated program that allows users to track permits as they move through the review process. The Automated Permit Tracking and Managing System, commonly known as POSSE, is used by city agencies to monitor operations related to the review, approval, inspection and enforcement of departmental permits. The system allows managers to monitor the progress of city construction projects, permit review times, inspector's mileage and personnel workloads.

The POSSE system has recently been expanded to allow private businesses and the general public access to permit records and information over the Internet. The Department of Planning and Permitting has deployed the Honolulu Internet Permit System (HIPS) Web site that provides Internet access to parcel and permit data stored in the POSSE system. Customers can now research permits and land records and check on the status of application reviews in real time. The system also provides expanded access to agencies and individuals through the city's intranet system, allowing users to access detailed information related to city construction projects.

Honolulu has also developed one of the most comprehensive GIS databases of any city of its size. The Honolulu Land Information System (HoLIS) is an enterprise-wide system serving over 15 city departments with land use, permit, tax, infrastructure and environmental data. A central repository for data pertinent to each of our city departments has eliminated duplication and cut the time required to access information related to zoning, property boundaries, tax assessment, ownership records, sewer hookups, demographics, flood zones and much more.

Tourism and Economic Development

The idea of devoting significant portions of Honolulu's Web site to the promotion of tourism and economic development on the island of Oahu has been several years in the making. We set out to build a versatile marketing tool that would allow us to convey a vivid image of our city to the rest of the world, promote awareness of our island's history and diverse cultures, and provide a wealth of information to perspective visitors.

We wanted to create an interactive, educational experience that would overturn the prevailing image of government sites as cold and impersonal. Honolulu's presence on the World Wide Web once consisted of a few simple pages listing city departments and telephone numbers. Today, our Web site features 18,000 pages that act as a virtual extension of the city itself — a user-friendly cyber-oasis reflecting the beauty of our land and the warmth of our aloha spirit. Overall, the Web's ability to enhance our brand recognition in the international community has been dramatic. The site averages about 9 million "hits" a month—three times as many as a year ago. Surveys indicate that up to 60 percent of the people who visit our site live outside Hawaii, many of them in Canada and Japan.

The Internet's use as a business development tool is of potentially greater benefit than its application in tourism marketing. Within the last year, Honolulu has launched a site

featuring the latest in GIS, Internet and database technologies. This sophisticated application allows businesses to access information needed to make informed investment decisions. The new Economic Development Property Locator allows users to view, create and print maps, perform site-selection searches, develop custom demographic radius reports, and locate commercial or business properties.

More flexible and powerful than most government Web sites, the GIS-based application allows users to access data that might otherwise take weeks and thousands of dollars to assemble. In addition to providing site-specific map overlays, the application provides everything from rental rates, sales prices, and information on square-footage and development incentives. Since its development, landscape architects, land-use attorneys, real estate appraisers and a host of other specialized users have found it to be an invaluable resource. Business owners find it useful for obtaining demographic information used in determining optimal retail site locations and doing target marketing. Even Hollywood movie studios have used the system to do background on perspective shooting locations.

Sophisticated business and economic development resources like this can be cost prohibitive for the public sector acting alone. By developing public-private partnerships, cities can leverage their limited resources in ways that serve the greater community. The property locator was made possible through a partnership between the city, the Honolulu Board of Realtors, and Enterprise Honolulu, a non-profit economic development organization that attracts new business to the island of Oahu.

> The Web's ability to enhance our brand recognition in the international community has been dramatic. The site averages about 9 million "hits" a month — three times as many as a year ago. Surveys indicate that up to 60 percent of the people who visit our site live outside Hawaii, many of them in Canada and Japan.

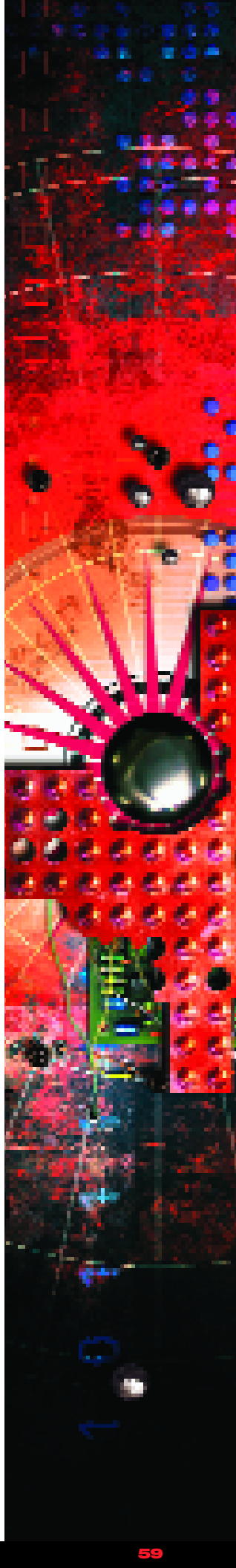
Community Access

No vision for e-government would be complete without considering the issue of digital democracy. As cities across the country explore new ways of improving the quality of citizens' lives through digital technology, decision makers are considering its potential to stimulate public awareness and greater involvement in community affairs. Improved efficiency and cost effectiveness are vitally important — especially at a time when city budgets are stretched to the limit — but we must be mindful as well of the Internet's capacity to open new doors to the democratic process.

Honolulu is among a growing number of American cities using IT to promote civic discourse. We provide live Webcasts of city council meetings, encourage the submission of electronic testimony at hearings and committees, and make it easier for constituents to keep in touch with their elected officials via e-mail. We've also responded to the challenges of citizen disinterest and apathy by using the Internet to educate young people about how local government is structured, how a bill becomes an ordinance, and how anyone can have a voice in deciding the outcome of urban issues.

In 1998 our city took the concept of participatory government a step further with the establishment of what we call Community Visioning. This unique process enables thousands of people in communities throughout the island to work with planning and design professionals in setting priorities for public works projects in their areas. Vision groups have been given the financial and material resources to bring dozens of ideas to fruition — everything from the construction of underground utility lines to traffic management systems. The response to this experiment in democratization has been nothing short of spectacular.

IT plays an important part in facilitating the flow of information between citizens and design professionals. The city has made Smart Boards available at public meetings, with special software that allows citizens to review



design options with project planners and architects without meeting face-to-face. This technology has revolutionized the process of citizen participation by making it possible for city officials and consultants to work with multiple vision groups across the island.

While Community Visioning has been an empowering experience for many of our citizens, there are many people in Honolulu whose personal circumstances prevent them from meaningful involvement in public affairs. The city is exploring ways to help them overcome obstacles to technology use that are often exacerbated by poverty, physical disability, geographic remoteness or lack of computer training.

One initiative that has generated broad community support is our Neighborhood Online project, a collaborative effort between the city's IT and Parks Departments. This program places computers in district parks throughout the island of Oahu, where Internet access, word processing, spreadsheet, and printer services are offered to the public free of charge. With the establishment of Neighborhood Online many of our park facilities have been transformed into community centers, were people of all ages gather to learn computer skills in a relaxed and informal setting.

Smart Government

The quest for smarter and more responsive government is the driving force behind IT advances in the City and County of Honolulu. While budget limitations have prevented us moving as quickly or aggressively as we have wanted to, every effort has been made to give investment in digital technology the emphasis it deserves. Anything less would be false economy.

Cities of all sizes will be expected, in the years ahead, to adopt disciplined and creative approaches to the application of IT as they confront the ongoing challenge of doing more with less. In Honolulu, that means setting realistic priorities, writing more of our software programs in-house, and forging public-private partnerships to achieve the goals we set for our community. Privatization is an option that may be expected to come under increased scrutiny.

The modernization of city government is not without uncertainty. But we can be sure that as new technologies are developed and the demand for government efficiency increases, cities will be expected to deliver services in increasingly convenient, customer-centered, and cost-effective ways. We must respond to these rising expectations with confidence and a commitment to improved public service. The future of our cities depends on it.

Participating Mayors, Executives, and Academics

Officer John Abraham
Safety Coordinator
Seattle Police Department

Satish Ajmani
CIO of Santa Clara County
San Jose, CA

Peter Alexander
VP Marketing
Cisco Systems

Robert Aldrich
Commandant of the
Marine Corps
U.S. Marine Corps

Irma Anderson
Mayor
Richmond, CA

John C. Antenucci
President and CEO
Plangraphics, Inc.

Alan Arakawa
Mayor
City of Maui, HI

Theresa A. Barton
Franklin County Judge
City of Frankfort

Eric Bayer
Sales Executive
Intergraph Corporation

Gary Becker
Mayor
Racine, WI

Lt. Gen. Emil "Buck" Bedard
Strategic Initiatives Group
Plans, Policies, and Operations
U.S. Marine Corps

Willie L. Brown, Jr.
Mayor
San Francisco, CA

Lt. Col. William Brown
Strategic Initiatives Group
Plans, Policies, and Operations
U.S. Marine Corps

Ed Burns
President, State and Local
Government
CIBER, Inc.

Captain Christopher Bushek
Action Officer
Critical Infrastructure Assurance
Branch
U.S. Marine Corps

Bob Campbell
VP, SBC West GEM Sales

Paul de la Cerda
Emergency Preparedness
Department
City of Los Angeles

Steve Choi
Director, Government Business
Marketing
SBC Communications, Inc

Tom Cochran
Executive Director
US Mayors Enterprises

Howard Cohen
Associate Dean, Development
and External Relations
Fox School of Business

Terry Cross
Vice Admiral, USCG
Alameda, CA 94501

Shawn Dainas
Corporate Communications
SBC Communications, Inc

Steve Darragh
Sales Director
SBC West GEM Sales
SBC Communications, Inc.

Kieran Doorley
Director of Technology
CIBER, Inc.

Deborah Edgerly
City Manager
Oakland, CA

Peter Ettinger
Senior Vice President
CityNet Communications

John Featherstone
VP, Business Development
Voyager Systems, Inc.

Denzel Fisher
Senior Analyst, West Coast
Operations
Battelle

Chris Flatmore
Assistant IT Director
City of San Mateo, CA

Mark Forman
CIO
Federal Government
The Office of Management and
Budget

Ray Geoffroy
Strategic Initiatives Group
Plans, Policies, and Operations
U.S. Marine Corps

Charlie Giancarlo
Senior Vice President
Cisco Systems

Gonzalo Gonzales
CIO
City of Vallejo, CA

Javier Gonzales
Associate Partner
Accenture

Bill Gresham
LtCol USMC
U.S. Marine Corps

Simon Hakim
Director, Center for Competitive
Government
Fox School of Business

Chuck Hansen
President and CEO
Hansen Technologies

Jeremy Harris
Mayor
Honolulu, HI

Bailey Hartmeyer
Regional VP, SBC Federal Sales
SBC Communications, Inc.

Greg Hilz
Director of Strategic Business
RoseTel System Corp.

Tony Homfray
Hansen Technologies

Anthony Intintoli
Mayor
Vallejo, CA

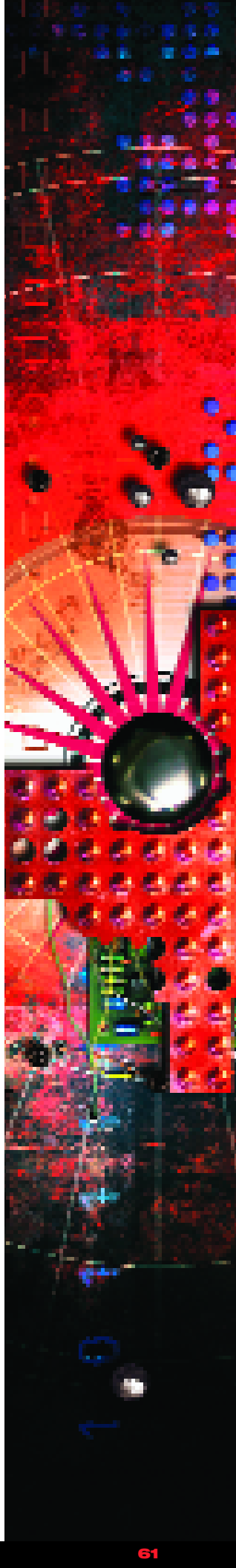
Dennis John
Director, City of Racine
Racine, WI

Jay Klohe
Senior Global Account Manager,
Federal Sales
SBC Communications, Inc.

Kathryn Kretschmer-Weyland
COO
US Mayors Enterprises
US Conference of Mayors

Michael Langley
Vice President, Public Sector
Plangraphics, Inc.

Sue Leonard
Integration Solutions Executive
SBC Communications, Inc.



Curtis Levinson
Homeland Security Practice Manager
SBC Communications, Inc.

Michael Levy
Deputy Director
California Office of Homeland Security

Dave Lieberth
Deputy Mayor
Akron, OH

Lewis W. Loeven, III
CIO and Executive Director
Department of Telecommunications and Information Services
City and County of San Francisco

Evelyn Lord
Mayor
Beaumont, TX

Chris Maloney
CEO and President
Voyager Systems, Inc.

John Maltbie
City of San Mateo
County Manager
San Mateo, CA

John Marks
Mayor
Tallahassee, FL

David Martinez
City of Vallejo
Vallejo, CA

Ronald Massey
Financial Director
City of Corpus Christi
Corpus Christi, TX

Patrick McCrory
Mayor
Charlotte, NC

Manny Menendez
Director of Economic Development
City of Honolulu
Honolulu, HI 96813

Gary Murray
President
Human Vision

Samuel Lloyd Neal
Mayor
Corpus Christi, TX

Dianah Neff
CIO
Philadelphia, PA

Greg Nickels
Mayor
Seattle, WA

Marc O'Conner
Director of Sales, Western Region
Intergraph Corporation

Rob Peglar
Corporate Architect
XIOtech Corporation

M. Moshe Porat
Dean
Fox School of Business

Jim Primrose
STAMP Project Manager
Extreme Business Solutions

Ed Reno III
Homeland Security Director,
SBC Communications, Inc.

Major F. Riddick
Business Partner
Human Vision

Kevin Ryan
President and Executive Director of Business Development
FranTech Strategies International

Russ Salter
Deputy Director
Emergency Preparedness and Response
Battelle Memorial Institute

Major Roberta Shea
Strategic Initiatives Group
Plans, Policies, and Operations
U.S. Marine Corps

Heidi Sieck
Telecommunications and Policy Advisor & Communications Director
City and County of San Francisco, CA

Randy R. Smith
Head, Critical Infrastructure Assurance Branch
U.S. Marine Corps

Ed Somers
Chief of Staff
US Mayors Enterprises
US Conference of Mayors

Ellis Stanley
General Manager
Emergency Preparedness Department
City of Los Angeles, CA

James Sudderth
Bechtel Corporation

Shah Talukder
Director of Marketing-Public Safety
Cisco Systems

Dennis Terry
Chief of Staff
City of Hammond
Hammond, IN

George Vinson
Director
California Office of Homeland Security

Drew Watson
Senior Analyst, Asymmetrical Threat Solutions
Battelle Memorial Institute

Captain Robert C. Weil
Executive Assistant, Maritime Homeland Security-USCG
Coast Guard Island

Peter Verga
Principal Deputy
Assistant Secretary of Defense for Homeland Defense
U.S. Department of Defense

George Vinson
Director
California Office of Homeland Security

General Charles Wilhelm
VP and Director
Department of Homeland Safety
Battelle Memorial Institute

Dan Williams
VP Business Development
Extreme Business Solutions

Brent Wingstrand
Assistant Chief
Seattle Police Department
Seattle, WA

Don Wollweber
Associate Director, SBC Government Business Marketing
SBC Communications, Inc.

Fred Wright
City of Vallejo
Vallejo, CA

The Center for Competitive Government at Temple University

Publications

The Center for Competitive Government publishes regularly on privatization topics as part of its ongoing commitment to encourage debate and promote research on improving service delivery of state and local governments.
Visit www.fox.temple.edu/ccg/publications

Volumes

To date we have edited the following volumes:

- "Securing Home and Business: A Guide to the Security Industry"
- "The New Public Management: Lessons from Innovating Governors and Mayors"
- "Reinventing Water and Wastewater Systems: Global Lessons for Improving Management"
- "Making Government Work: Lessons from America's Governors and Mayors"
- "Restructuring Education: Innovations and Evaluations of Alternative Systems"
- "Privatizing the United States Justice System"
- "Privatizing Correctional Institutions"
- "Privatizing Education and Educational Choice"
- "Privatizing Transportation Systems"
- "Privatization and Competition in Telecommunications: International Developments"
- "Restructuring State and Local Services"
- "Smart Contracting for Local Government Services"
- "Contracting Out Government Services"
- "Privatization and Restructuring of Electricity Provision"
- "America's Water and Wastewater Industries: Competition and Privatization"
- "Innovations in Education: Evaluating Alternative Systems"
- Management Innovation in U.S. Public Water and Wastewarer Systems (forthcoming).
- Innovations in Electronic Government: Governors and Mayors Speak Out (forthcoming).

Most volumes are part of the series "Privatizing Government: An Interdisciplinary Series," which we edit for Praeger Publishers, which is part of Greenwood Publishers. All our publications contain a variety of articles written by researchers, practitioners, and members of groups directly involved in privatization such as government, business and labor organizations. We present diverse viewpoints, and cover all aspects of restructuring and privatization from theoretical analysis to actual implementation.

Conference Proceedings

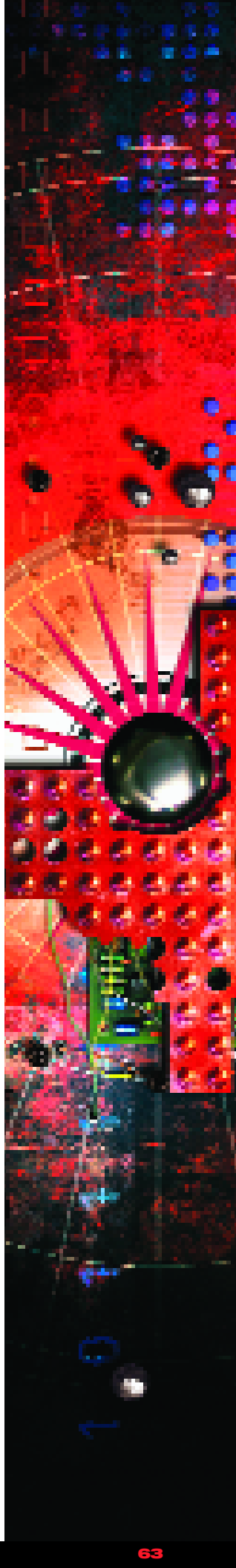
- "Making Government Work: Best Practices in Competitive Government"
- "Seizing the Opportunity of E-Government"

Articles

Members of the Center for Competitive government conduct research in various fields of privatization. Articles were written on police, prisons, highways and human services. The following are a few published articles.

- "A Market Alternative to Child Adoption and Foster Care," *Child and Youth Services Review,* Erwin A. Blackstone and Simon Hakim, 2004
- "Regulation," Cato Institue, Vol. 25 (1), Spring 2002: 16–19, Erwin A. Blackstone, Simon Hakim, Uriel Spiegel
- "The Economics of Crying Wolf," the Milken Institute Review, Erwin A. Blackstone, Simon Hakim, Uriel Spiegel
- "Police Services: The Private Challenge," *An Independent Institute Policy Report*, Erwin A. Blackstone and Simon Hakim
- "Making Inroads in Private Highway Construction," *American City & County Magazine*, (Simon Hakim and Erwin A. Blackstone), August 1999: 52–56
- "Private Guard Response to Alarm Activation," *Security Technology and Design*, (Simon Hakim and Mary-Ann Gaffney), April 1995: 54–55

(continued on page 64)



- "Privately Managed Prisons Go Before the Review Board," *American City & County*, (Simon Hakim and Erwin A. Blackstone) April 1996: 40–50
- "Crying Wolf with Public Safety," *American City & County*, (Simon Hakim and Erwin A. Blackstone), August 1996: 54–64
- "Private Ayes: A Tale of Four Cities," *American City & County*, (Simon Hakim and Erwin A. Blackstone), February 1997: PS4–PS12

Other Books

- "Kids Raised by the Government," Ira M. Schwartz and Gideon Fishman, Praeger, 1999
- "Justice for All," Arye Rattner and Gideon Fishman, Praeger, 1998

Center for Competitive Government
The Fox School of Business and Management
Temple University
Philadelphia, PA 19122
215-204-5037
www.fox.temple.edu/ccg
ccg@sbm.temple.edu