domestic preparedness .com

DomPrep Journal

US $50 Annual

Volume 1, Issue 23, November 16, 2005

Shards of Terror!

A Focus on Critical Infrastructure

Six Questions, a Changing Threat, And an Unknown Number Of Algorithms

Guest Commentary
Page 3

The Essential Components Of Domestic Preparedness

Editor in Chief
Page 7

Rear Admiral Joseph L. Nimmich, USCG

Interview
Page 4

Pennsylvania and Massachusetts

State Homeland News
Page 10

For more details, visit:
DomesticPreparedness.com
Since 1998, Integrating Professional Communities of Homeland Security

Editorial and Circulation Office
517 Benfield Road, Suite 303
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Editorial Staff
James D. Hessman
Editor in Chief
JamesD@domprep.com

Channel Masters
Rob Schnepp
Fire/HAZMAT
rschnepp@domprep.com

Joseph Cahill
Emergency Medicine
jcahill@domprep.com

Colonel (Ret.) Robert Fitton
Military Support
bfitton@domprep.com

Ashley Moore
Standards
amoore@domprep.com

Jay Kehoe
Law Enforcement
jkehoe@domprep.com

John Morton
Interviews
jmorton@domprep.com

Neil Livingstone
Global Options
nlivingstone@domprep.com

Adam McLaughlin
State Homeland News
amclaughlin@domprep.com

Laurie Thomas
Maritime Security
lthomas@domprep.com

Business Office
Martin Masiuk
Publisher
mmasiuk@domprep.com

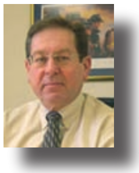
Susan Collins
Circulation Director
subcriber@domprep.com

Sharon Stovall
Copy Manager
sstovall@domprep.com

Published by the IMR Group Inc.
Martin D. Masiuk,
Executive Director and Publisher,
mmasiuk@domprep.com
Text is the opinion of the author who holds no liability for its use or interpretation.

Publisher's Messasge

By Martin Masiuk, Publisher



Two of the articles in this issue of *DomPrep Journal* focus on separate but interrelated aspects of infrastructure protection – more specifically, on the protection of "critical" infrastructure, the generic term used to encompass the major physical components of a modern industrialized society. If any of those components – the levees surrounding and theoretically protecting New Orleans provide a recent devastating example – is destroyed or put out of commission for an extended period of time the damage done, both human and economic, is immediate, huge, and long-lasting.

Dr. Bilal Ayyub leads off the coverage with a Special Report on a major critical-infrastructure study project being carried out, under his leadership, at the University of Maryland's Center for Technology and Systems Management. Completion of that project, which is sponsored by the Maryland Emergency Management Agency, could have profound implications for all of Maryland's sister states, and for first responders throughout the country. Editor in Chief James D. Hessman follows with an update on the many positive steps forward that have been taken since 9/11, along with a summary of *some* but by no means all of the many extremely difficult tasks that lie ahead – and that must be faced not only by the nation's elected leaders at all levels of government, but also the American people themselves.

No nation, no business, no human organization of any type can protect all of its people and/or all of its property and other physical assets all of the time. But as a nation the United States obviously can do – and *must* do – much better in protecting its vital infrastructure than it was doing before the 9/11 attacks and has been doing in recent years. That was and is the well-considered verdict not only of the 9/11 Commission but also of numerous Congressional hearings and reports and most reasonably objective media editorials and commentaries.

Several difficult truths must be faced, therefore. The first is that future terrorist attacks are not only possible but almost inevitable. The second is that more and greater efforts must be made not just by those in uniform, and first responders, and the nation's elected leaders, but by all Americans. The third is that to completely rid the world of the cancer of terrorism will take years, will require the expenditure of hundreds of billions of dollars, the use of advanced technology, and cooperation with all of the other free nations of the world. It also will take patience, endurance, fortitude, and the ability to deal with continuing frustration and occasional defeats.

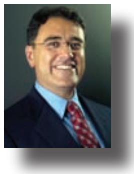
Not all of the preceding should be considered bad news, it should be emphasized. The lessons learned and technologies developed to fight international terrorism will be equally useful – for years and maybe centuries to come – in helping mitigate the consequences of natural disasters. The same lessons and technologies will save untold hundreds of thousands of lives, and perhaps millions. And the end result, after thousands of years of wars among nations, may be, and should be, a true peace throughout the world among all men of good will. ▼

Cover Photo: Jakarta, Indonesia - September 9*: The Australian flag flies outside the Australian Embassy following a bomb blast, Thursday, Sept. 9, 2004, in Jakarta, Indonesia. A powerful explosion in central Jakarta killed 7, wounded more than 100, and caused extensive damage to nearby buildings.*

The Protection of Critical Infrastructure

Six Questions, a Changing Threat, And an Unknown Number of Algorithms

By Bilal Ayyub, Guest Commentary



The following Special Report by Dr. Ayyub is about a project being carried out for the Maryland Emergency Management Agency that should be of vital interest to first responders and others involved – at the local, state, and/or federal levels (the international level as well) – in the protection of critical infrastructure.

The U.S. Department of Homeland Security (DHS) has identified what are called "risk methods" as the primary underlying framework for system evaluations, operational assessments, technology assessments, resource and support analyses, and field operations analyses. In that context, the protection of critical-infrastructure and key-resource (CI/KR) assets for homeland security requires both the allocation of finite available resources and the making of choices – from among a large set of protective actions that might be implemented – to reduce risk.

Decisions on resource allocation, therefore, are among the most significant challenges facing the nation's homeland-security community. The principal difficulty in making such decisions stems not only from the nature of the hazards themselves, but also from the complexity of the numerous decision variables involved. Unlike risks associated with natural disasters – or unintentional human-caused disasters – most if not all of the risks associated with security hazards result from the fact that these hazards are deliberately created by an adversary who: (a) has intent or motivation (political, economic, cultural, religious, and/or personal); (b) possesses variable and broad capabilities – e.g., weapons (perhaps even including weapons of mass destruction, or WMDs), manpower, access, intelligence; and (c) is "dynamic" in the sense of being responsive to countermeasures and therefore able to change his own tactics and capabilities, and/or the targets he has selected.

> ***Most if not all risks associated with security hazards result from the fact that these hazards are deliberately created by an adversary who...***

The spectrum of security hazards is a wide one, ranging from vandalism and pilferage to sabotage and explosive attacks. However, small-scale security hazards such as vandalism and pilferage usually do not aim to disrupt vital services, and cause relatively little physical damage to property. In contrast, larger-scale sabotage and explosive attacks typically are carried out with the objective of producing numerous casualties, and/or disrupting vital services, or destroying the significant symbols of a society (the Statue of Liberty, for example, or the Washington Monument). Indeed, the objective of those carrying out terrorist-style attacks may not be to defeat the target nation's military forces or security capabilities per se, but to achieve their goals by significantly disrupting the economic system, governmental processes, and societal norms of the nation targeted.

Deliberate and Unpredictable Hazards

Security hazards are similar to natural hazards in at least one respect – namely, that both use some type of "external loading" to attack their targets; disruption of the target occurs when that loading exceeds the capacity of the target to resist it. However, natural hazards are indiscriminate about the targets they affect – and they occur, moreover, in a somewhat random yet predictable manner. In contrast, security hazards are deliberate and much less predictable, with an adversary selectively choosing one or more from a broad spectrum of possible targets – basing that selection, usually, on his own perception of the risks involved and the potential rewards likely to result from an attack.

In that context, security hazards might be more precisely defined as asymmetric threats against society in which the attackers choose high-value targets in a manner consistent with their own objectives and perceived capabilities, and leverage the force-multiplying effect of surprise to achieve success against defenders who are either unaware of the threat or unprepared to defend themselves against usually unknown tactics.

Because the threat (or security hazard) landscape is constantly changing, it is not possible to use historical data alone to assess the probability of an attack.

Instead, such an assessment requires consideration of a number of interrelated factors, including but not limited to trends in adversary ideology, technological innovations, the relative effectiveness of various possible countermeasures, and the proliferation of open-source information about potential targets of opportunity.

The difficulties involved in making such assessments is illustrated by the fact that a recent study shows that, since the 9/11 terrorist attacks against the United States, many of the countermeasures put in place to defeat terrorism actually have done little to reduce possible recurrences but, rather, have caused the perpetrators of international terrorism to shift toward less logistically complex tactics to achieve their goals. Strategic planning for reducing exposure to risks arising from security hazards therefore requires, among other things, both the extensive use of expert opinion to assess rates and probabilities of occurrence (based on whatever evidence is available) and similarly expert projections of future trends.

However, simply waiting for the emergence of a security hazard *prior* to a thorough assessment of risk gives an asymmetric advantage to the adversary – namely, the lack of defender knowledge about potential system weaknesses, which leads in turn to an overall lack of preparedness to respond to unknown security hazards. The end result is the creation of situations in which the adversary can use the defender's ignorance to his advantage.

Asset-Driven vs. Hazard-Driven Analysis

Because of the constantly evolving and uncertain hazard environment, risk assessment and management related to the protection of CI/KR assets must necessarily begin with the identification of critical systems and networks the destruction or significant disruption of which could pose unacceptable consequences. After these critical elements have been identified, analyses can be carried out to identify their susceptibilities to a wide spectrum of security hazards. Considered together, the critical elements and their susceptibilities form what are called hazard scenarios.

The next task is to analyze the consequences and vulnerabilities involved in each of the hazard scenarios that have been developed to determine the conditional risk likely when/if an attack has occurred. The use of an asset-driven approach differs significantly from use of a hazard-driven approach, which requires consideration of a sufficiently probable threat prior to a subsequent risk assessment. One of the principal advantages of using an asset-driven approach is that all analysis is completed prior to an incident to determine a set of hazards to be concerned about, rather than waiting for the emergence of a threat before beginning a vulnerabilities-and-consequences study. Another advantage is that knowledge of the conditional risk associated with a given hazard supports security-investment decisions without knowledge of the actual hazard likelihood. Additional information about the likelihood of a hazard, combined with the conditional risk, gives the total residual risk exposure, which accounts for the net reduction in risk made possible by existing risk-reduction measures. If the potential consequences, and/or conditional risk, and/or residual risk for a given hazard scenario exceeds a previously defined threshold, that scenario may then be flagged for follow-on risk-management activities.

The Management and Mitigation of Risk

Risk management entails the identification of corrective actions, including countermeasures and mitigation strategies (collectively called investment alternatives), for high-risk hazard scenarios that – in an efficient and cost-effective manner, and with limited impact on future options – will reduce or minimize the risks considered likely. In this context, a countermeasure is defined as an action taken, or a physical capability provided, the principal purpose of which is to reduce or eliminate one or more vulnerabilities and/or to reduce the rate of occurrence of security-hazard events.

For clarification: Consequence mitigation is the term used to describe preplanned and coordinated actions or system features that are designed to: reduce or minimize the damage caused by attacks (consequences of an attack); support and complement emergency forces (first responders); facilitate field-investigation and crisis-management response; and facilitate recovery and reconstitution for enhancing system resiliency. Consequence mitigation also may include steps taken to reduce short- and long-term impacts, such as providing alternative sources of supply for critical goods and services.

Mitigation actions and strategies are intended to reduce the consequences (impacts) of an attack and make a system resilient, whereas countermeasures are intended to reduce the probability that an attack will succeed in causing a failure or significant damage. For each set of strategies, tradeoffs are made between their benefits and respective costs to maximize return on investment; strategies with a high benefit-to-cost ratio are preferable to those with a smaller potential return on investment.

A Rational Case for the Probabilistic Approach

The computation of defensible benefit-to-cost ratios requires that all potential initiating events, in this case security hazards, be considered within a unified probabilistic framework. In addition, all aspects of risk, including consequence (economic, public health and safety, etc.), vulnerability (security and physical), and hazard likelihood should be considered probabilistically. Although a qualitative approach that assesses risks as high, medium, or low appears simple to use and has appealing consensus-building properties, the assessments produced by this approach often lead to erroneous or uninformative results, especially when trying to discriminate among quantitatively small and quantitatively large risks.

In contrast, a more robust probabilistic approach permits a rational and coherent comparison among decision alternatives to determine the most cost-effective risk-reduction strategies. Moreover, knowledge of the most likely quantitative risks resulting from various investment alternatives facilitates a rational comparison with other societal risks – e.g., fires, earthquakes, diseases, floods, and other natural hazards – that can be used both to determine relative risks and to assist in establishing acceptable risk levels and achieve all-hazard objectives.

Risk analyses that are carried out for the protection of CI/KR assets, and that include appropriate risk-assessment and management factors, should be conducted at two levels: the asset level, and the portfolio level. At the asset level, a survey of critical elements, their functions, and the likely consequences of disruption – as well as their physical and security vulnerabilities – provides insight into the range of actions that can be taken by the asset owner to reduce his overall exposure to the risks likely from the full spectrum of potential security hazards.

At the portfolio level, total risk exposure can be assessed by hazard, region, jurisdiction, or infrastructure sector, and investment decisions can be made to reduce the overall portfolio risk to an acceptable level. Ideally, both levels of analysis should share a common analytical framework that supports the decisions made by all stakeholders, thus enabling the information collected at the asset level to support decisions made at the portfolio level, and vice versa.

National Benefits From a Common Framework

The objective of the project being carried out for the Maryland Emergency Management Agency is to develop a practical methodology for analyzing, assessing, and reporting risks associated with critical infrastructure and key resources within the State of Maryland. The information developed will be used both for the purpose of screening and preliminary ranking, and for the prioritization of portfolio risk management and resource allocation. The proposed risk assessment and management framework for security hazards seeks answers to the following six questions:

1. What could happen?
2. How can it happen?
3. How likely is it to happen?
4. What are the consequences if it happens?
5. What can be done to reduce the risks in a cost-effective manner?
6. What effect will these risk-management decisions have on subsequent risks and options?

Upon completion, this project will provide the procedures needed to carry

NIOSH APPROVED

ONCE AGAIN!

MSA RECEIVES THE FIRST NIOSH CBRN APPROVAL – THIS TIME FOR AIR-PURIFYING ESCAPE RESPIRATORS.

This adds to MSA's impressive list of "First Approval Issued" CBRN Products:

1) Millennium® CBRN Gas Mask

2) FireHawk® NFPA 2002 Air Mask

3) Safe Escape™ Respirator

The **Safe Escape™ Respirator** is a one-time use escape device that has numerous features including a high-performance wide vision laminate hood, self-adjusting inside-the-hood cradle head strap and packaged in a Hextreme™ Plastic Hexagon-Shaped Protector.

The Safe Escape Respirator is even sized for a more personal, secure fit. Call MSA Customer Service or visit MSAnet.com for more information about the CBRN NIOSH Approved Safe Escape Respirator from MSA.

MSA Be Sure. Choose MSA.

1.888.MSA.0018
MSAnet.com

out a screening-level risk analysis of a county, sector, or region – or, in fact, the entire inventory of assets within any specific jurisdiction. Among the more important "deliverables" expected from the project is a State of Maryland Guide – which can be used not only by other states but also by first responders throughout the country – on *The Protection of Critical Infrastructure and Key Resources for Homeland Security*.

Separate sections of the Guide will describe and illustrate, among other things: the practical methodology followed in carrying out the project; the database architecture and computational algorithms used to implement the methodology; a user interface for data entry and reporting that includes risk summaries by hazard type, asset and resource types, geographic location, the benefit-cost ratios of various countermeasures and mitigation strategies, and the conditional and residual risks factored into the equation.

Most important of all, perhaps, is that the methodology developed for the project will provide a common framework that can be used to support the resource-allocation decisions made by all stakeholders ranging from asset owners to the State of Maryland's homeland-security officials.

Professor Bilal M. Ayyub, PhD, is director of the Center for Technology and Systems Management in the Department of Civil and Environmental Engineering at the University of Maryland in College Park, Md. Several other personnel from the center also are serving on his project team. Guidance on the project is being provided by the Maryland Emergency Management Agency; guidance on information security and on various legal issues relevant to the project is being provided by personnel from the University of Maryland's Center for Health and Homeland Security.

Critical-Infrastructure Update

The Essential Components of Domestic Preparedness

By James D. Hessman, Editor in Chief

From the terrorist's point of view, the list of possible targets is endless: airports and seaports; U.S. embassies overseas and major federal office buildings in the United States itself; nuclear power plants and offshore oil platforms; bridges and tunnels; factories and office buildings. All are rightly considered essential components of the nation's "critical infrastructure" – and are essential because their destruction or significant degradation would be seriously harmful to the U.S. economy and/or national security.

There are other targets as well: theaters, hotels, and restaurants; well known landmarks such as the Lincoln and Jefferson Memorials, the National Archives, Yankee Stadium, and the Epcot Center; even schools, churches, and libraries – as well as major sports and entertainment events such as the Super Bowl and Academy Awards ceremonies. Destruction of, or major damage to, any of these would not disrupt the U.S. economy – but would seriously harm the national morale and perhaps kill hundreds or thousands of Americans, which is always a collateral goal of Al Qaeda and other terrorist groups.

The multiplicity of attractive and significant if not always critical targets within the United States, and overseas as well, is why the 9/11 Commission reluctantly concluded in its *Final Report* that it is not possible "to defeat all terrorist attacks against Americans, every time and everywhere. … No president can promise that a catastrophic attack like that of 9/Il will not happen again. History has shown that even the most vigilant and expert agencies cannot always prevent determined, suicidal attackers from reaching a target."

The suicide bombing attacks against hotels, buses, marketplaces, and both public and private buildings in Baghdad and elsewhere in Iraq validate that grim statement on an almost daily basis. Moreover, the equally lethal attacks on the London bus and subway systems, against hotels and nightclubs in Jordan and Indonesia, and against scores of possible targets in Israel, show that terrorism in the 21st century is a truly international threat and will undoubtedly require a truly international effort to defeat it.

A Good But Hesitant Beginning

Winning the Global War on Terror will not be easy, though. The final defeat of Al Qaeda – however the word "final" is defined – and other terrorist groups linked to it, working with it, or perhaps operating independently, will take many years, perhaps decades, and will cost untold billions of dollars. It will also, in all probability, cost the lives of many more Americans, not only members of the nation's armed forces – State Department employees as well – stationed overseas but also, on the home front, firemen, policemen, EMS (emergency medical service) employees, security guards, and other first responders.

Fortunately, many forward-looking steps already have been taken, particularly by the federal government – a fact not always mentioned in the U.S. print and broadcast media, and/or recognized

Homeland security and national preparedness begin with the private sector . . . which remains largely unprepared for a terrorist attack

by the American people. The Taliban were quickly and thoroughly defeated in Afghanistan, for example. And, despite the violent peace now raging in Iraq, the overthrow of Saddam Hussein and his later capture and detention were major political as well as military accomplishments. In the United States itself, a new Department of Homeland Security (DHS) has been established and, despite some initial difficulties, is now rapidly, and with reasonable efficiency, sorting out its goals and priorities, completing a major reorganization, and learning to speak with a common voice.

On Capitol Hill, meanwhile, Congress has moved with unusual, and admirable, speed in passing important legislation such as the Patriot Act and has been extraordinarily generous in providing the funding needed by DHS and other departments involved in the fight against international terrorism. On the minus side, at least some of the projects funded by Congress are of dubious value, and the House and Senate both have been slow in reorganizing their committee systems to meet the new challenges facing the nation.

An Ample Spectrum of Blame

Not nearly as much has been accomplished at the state and local levels of government, though – or by the private sector. All states, and most if not quite all of the nation's major cities, have established their own departments of homeland (or state, or local) security or the equivalent thereof. Some have been staffed and funded adequately, but most have not been – not, at least, if the goal is to be able to deal with all reasonably foreseeable threats. "Reasonably foreseeable" includes, of course, the threats posed not only by terrorists but also by hurricanes, floods, tornadoes, earthquakes, and other natural disasters.

As was amply demonstrated by Hurricanes Katrina, Rita, and Wilma (and other recent natural disasters), the preparedness deficiencies at the state and local levels of government include but are not limited to a lack of planning, inadequate and insufficient training, the frequent inability of even neighboring jurisdictions to communicate with one another, and a broad spectrum of equipment difficulties ranging from system incompatibilities to inadequate stockpiles of protective clothing to maintenance and obsolescence problems of all types. The biggest problems, though, are both political and financial: Almost all jurisdictions want and expect the federal government to do more – and to pay most if not all of the sometimes very high cost in dollars that is required to alleviate if not completely resolve all of the deficiencies and difficulties noted above.

Insofar as critical infrastructure is concerned, though, there are more and greater problems in the private sector than at all levels of government combined – if only because, as the 9/11 Commission also pointed out in its *Final Report*, the U.S. private sector *"controls 85 percent of the critical infrastructure in the nation* [emphasis added]." For that reason alone, the Commission continued, "Homeland security and national preparedness therefore begins with the private sector" – which, the *Final Report* added, "remains largely unprepared for a terrorist attack."

"Realistic and Achievable" Recommendations

That situation may be about to change, though – and in the very near future. In 26 October 2005 testimony before the House Science Committee, Dr. William A. Jeffrey (director of the U.S. Commerce Department's National Institute of Standards and Technology, or NIST) released a long list of well-researched recommendations that, if and when fully implemented, would: (a) lead to major improvements in building standards, codes, and practices; (b) mandate the establishment or improvement of evacuation routes and other emergency-response procedures; and (c) provide additional funding for research into and the production of equipment and systems essential to the protection of critical-infrastructure buildings, systems, and networks.

Jeffrey said in his testimony – which focused primarily on the NIST National Construction Safety Team's final report on the 9/11 collapses of the World Trade Center Towers – that the 30 major recommendations in the report are "realistic, appropriate, and achievable within a reasonable period of time." Most of the recommendations, although worded specifically to remedy deficiencies in the protection of "tall buildings" (such as the WTC Towers), could with only minor modifications be made applicable to other components of the nation's critical infrastructure.

At first glance, the NIST recommendations might seem to be little more than common-sense generalities – e.g., “Improve the structural integrity of buildings.” But the huge volume of comments from expert witnesses that accompany the report, the testimony of public and private-sector preparedness professionals, and other backup materials provide thousands of detailed specifics. To improve and enhance the fire resistance of buildings, for example, requires the use of spray-applied “fire-resistive” coatings, the installation of additional sprinkler systems and standpipes/hoses, and the hard-wiring – within and throughout the building – of fire alarms and smoke-management systems. Protection of those within the building requires, in addition, the installation, maintenance, testing, and use of redundant voice and phone public-announcement systems to alert tenants and office workers of a known or suspected danger in time to permit their “safe and rapid egress” through the “additional evacuation routes” that also are recommended.

Encouraging the Volunteers

The key word throughout the report, it should be noted, is “recommended” – because NIST could only “urge” or – frequently – “strongly urge,” not direct, require, or mandate. For that reason, Jeffrey also cautioned that the numerous safety improvements projected could be realized only if the agency’s recommendations “are acted on by the appropriate organizations” – i.e., the organizations “that develop building and fire safety codes, standards, and practices.” He urged those organizations – “and the state and local agencies” that are required to adhere to the safety codes and standards – to give “immediate and serious consideration to implementing the report’s recommendations.”

History shows that the American system of government works best when common-sense recommendations and suggestions are voluntarily adopted – by private-sector businesses and nongovernmental organizations as well as by individual citizens. A few self-enforcing economic factors frequently help as well – e.g., when insurance companies refuse to write policies for homes built on cliffs. Recognizing these time-honored truths – and looking for a way, perhaps, to “encourage” the private sector to do more on its own behalf – the 9/11 Commission asked the American National Standards Institute (ANSI) to develop a consensus on a voluntary “National Standard for Preparedness” for the private sector. ANSI did so, consulting not only government officials but also safety, security, and business-continuity experts from a broad spectrum of private-sector industries and associations.

The end result was a strong endorsement by the 9/11 Commission, in its own *Final Report*, of the ANSI’s “recommended standard for private preparedness.” Knowing that voluntary does not always work, the Commission members added a few “or else” considerations with the following muscular statement: “We also encourage the insurance and credit-rating industries to look closely at a company’s compliance with the ANSI standard in assessing its [the company’s] insurability and creditworthiness. We believe that compliance with the standard should define the standard of care owed by a company to its employees and the public for legal purposes. Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security.”

The NIST recommendations released by Dr. Jeffrey are included in 43 separate reports, totaling approximately 10,000 pages of comments, testimony, and backup materials of various types. To view the complete set of comments, the full version of the final recommendations, and the accompanying NIST press release, visit http://wtc.nist.gov Also recommended are the ANSI website (www.ansi.org) and the website of the American Society of Civil Engineers (www.asce.org). An in-depth interview by DomPrep’s John Morton with ASCE Chief Operating Officer Larry Roth was included in the 23 March issue of T.I.P.S., predecessor of the DomPrep Journal. That interview focused on the ASCE’s 2005 Report Card for America’s Infrastructure, which provides updated grades for, among other infrastructure components, the nation’s roads, bridges, drinking water, transit systems, and energy resources.

Pennsylvania and Massachusetts

By Adam McLaughlin, State Homeland News

Pennsylvania Installs Trace Portal Machines at Pittsburgh International

The Transportation Security Administration (TSA) has installed an explosives detection trace portal at the passenger security checkpoint at the Pittsburgh International Airport.

All passengers who are identified as needing additional screening will pass through the trace explosives detection portal. When a passenger enters the trace portal, he or she will be asked to stand still for a few seconds while several "bursts" of air are released. The air bursts, which are virtually undetectable, are designed to dislodge microscopic particles from the clothing and bodies of those passing through the trace portal. The particles will then be very quickly collected and analyzed to determine if there are any traces of explosives indicated. A computerized voice tells the passenger when he or she may exit the portal. Screeners will take what are described as "necessary and appropriate steps" to resolve any problems that might arise if an alarm is triggered.

"Trace portals allow TSA to expand its capability to detect explosives in a more travel-friendly manner," said Joseph P. Terrell, TSA's federal security director at Pittsburgh International. "This significant security enhancement [installation of the trace portal] would not be possible," he added, "without the cooperation and hard work of the Allegheny County Airport Authority and our airline partners. Working together, we will continue to enhance security and the overall traveler experience."

Similar trace portals already have been installed in a number of other major airports throughout the United States. By late November, officials said, TSA plans to complete installation of the explosives-detection equipment at six additional airports, and by January 2006 expects to meet the agency's goal of installing 100 additional devices at the nation's largest airports.

Trace portals allow TSA to expand its capability to detect explosives in a more travel-friendly manner

Massachusetts To Open Quarantine Station At Logan International

With the latest threat of avian flu as well as other infectious diseases growing, the Massachusetts Port Authority plans to open a quarantine station at Logan International Airport by the end of this year. Officials from the Center for Disease Control and Prevention (CDC) will operate the facility and evaluate the health threats posed by incoming travelers.

The five-person CDC staff will work out of an office suite and isolation room located in the airport's international terminal. Among the other duties of the CDC staff members will be the training of airport and airline employees on how to detect symptoms consistent with infectious diseases. "We are most interested in people with fever accompanied by rash, stiff neck, jaundice, cough, or unusual bleeding and severe diarrhea with or without fever," said Maria Pia Sanchez, the CDC's officer in charge at Logan.

CDC officials said that the opening of the quarantine station will not have a major impact on most travelers arriving at Logan from overseas, because only a very small percentage of incoming passengers are actually pulled aside for evaluation. In addition to monitoring incoming travelers, the CDC staff at Logan will work with state and local health officials to prepare for a medical emergency of any type, help in the inspection and handling of imported animals, and handle calls from port officials throughout Massachusetts and other New England states.

The airport already has policies in place to manage suspected cases of infectious diseases and will work closely with the CDC staff, according to a Massachusetts Port Authority spokesperson at Logan. The decision to open a quarantine station at Logan is part of a larger federal government effort to triple the number of quarantine stations around the country. In addition to the one in Boston, CDC officials said, nine other stations are being installed at airports in Washington, Newark, Houston, El Paso, Anchorage, Minneapolis, Detroit, San Diego, and San Juan. By the end of 2006 the federal government plans to have a total of 25 stations operational throughout the United States. ▼