THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 10 NUMBER 8
AND HOMELAND SECURITY

FEBRUARY 2012
FACILITIES

Contact: dhardy1@gmu.edu
703.993.8591

Click **here** to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

In this month's issue of *The CIP Report*, we feature several projects and programs that are in place to improve the efficiency and protection of commercial and government facilities.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, the Director of the Multihazard Loss Estimation Program at the National Institute of Building Sciences discusses the capabilities of IRVS (Integrated Rapid Visual Screening), a tool that determines the risks, resilience, and multi-hazard interactions of a building. The Project Manager for the National Institute of Building Sciences High Performance Based Design Program for the U.S. Department of Homeland Security then describes the Owner Performance Requirements (OPR) modeling process. Next, the Executive Vice President of Virtual Emergency Services and the Chairman & CEO and President of First Response Solutions Incorporated emphasize the importance of public-private collaboration in protecting critical infrastructure. Finally, we highlight the challenges involved in protecting one of the most high-profile commercial facilities; the Super Bowl.

This month's *Legal Insights* examines the legal obstacles that exist in improving the energy efficiency of government buildings.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

IRVS: The Fast Way to Determining Building Risk and Resiliency

by Philip Schneider,* AIA
Director, Multihazard Loss Estimation Program

The National Institute of Building Sciences, as part of its mission as a non-profit, non-governmental organization that successfully brings together representatives of government, the professions, industry, labor and consumer interests, and regulatory agencies to focus on the identification and resolution of problems and potential problems that hamper the construction of safe, affordable structures for housing, commerce, and industry throughout the United States, is supporting the efforts of the U.S. Department of Homeland Security (DHS) to reduce risk and improve resiliency of our Nation's infrastructure. The Institute is working with the DHS Science and Technology (S&T) Directorate's Infrastructure Protection and Disaster Management Division (IDD) on the continued development and dissemination and adoption by government and private industry of two related tools, Integrated Rapid Visual Screening (IRVS), described in this article, and the Owners Performance Requirements Tool, described in another article in this issue. IRVS is a quick and simple tool that determines the risks, resiliency, and multi-hazard interactions of a building. The IRVS methodology can effectively and powerfully compute the level of risk associated with different building types from a broad range of natural and man-made hazards. The IRVS specifically can:

- Provide numeric risk and resiliency scores that produce a quantification of relative risks, and an understanding of the most dominant features of the building controlling overall risk.

- Provide an understanding of resilience, potential down time, and economic and social implications if a building is affected by a catastrophic event.

- Rank vulnerabilities and consequences within a community, indicating which buildings are more at risk and require higher protection.

- Identify, collect, and store vulnerability data that can then be re-examined before protective measures are put in place or after they are put in place.

The IRVS was developed by DHS S&T IDD over the last several years in three modules, one for Mass Transit Stations, one for Tunnels, and the newest one, for Buildings, that will be discussed here. IRVS has been tested and validated with multiple public and private users in Arlington, VA; Albany, NY; New York City; Charleston, SC; Los Angeles; and jointly with the Department of Veteran Affairs. More information on the IRVS and related publications and tools from the DHS S&T IDD program are available at http://www.dhs.gov/files/programs/scitech-bips-tools.shtm.

The process for performing a rapid visual screening is comprised of three steps:

- Fill out a form with pre-field data or data that is already known about the building.

- Conduct a visual on-site field evaluation by answering a series of questions about exterior features, publicly accessible internal areas, and other internal areas, accessible only with permission.

- Quantify a risk and resiliency score and a multi-hazard score automatically within the IRVS.

Scoring for risk and resiliency is based on a methodology that uses built-in weights and pre-defined

(Continued on Page 3)

IRVS HAZARDS

- Explosive, chemical, biological, and radiological attacks
- Earthquakes, floods, and high-wind hazards
- Fire hazards

IRVS *(Cont. from 2)*

algorithms. The multi-hazard score appears in a matrix that quantifies interactions among hazards on a scale from 0 to 1, based on built-in weights and building characteristics. The higher the resulting number, the higher the interaction between hazards.

The reliability and quality of the screening depends on the time that is devoted to the collection of information and field inspections. The quality can be increased if structural, mechanical, and security features are verified, interior inspections are carried out, interviews with security and other key personnel take place, and drawings and security operation manuals are reviewed.

One or two assessors can conduct and complete a screening in one to five hours. The IRVS tool operates on Micro¬soft (MS) Access 2007 to facilitate data collection and to function as a data management tool. The IRVS can be used on a personal computer or laptop to systematically collect, store, and report screening data, and to compute the risk score and store records. The IRVS tool also contains:

- A catalogue that describes the IRVS questions
- Ability to print reports
- Ability to add photos
- Export capabilities
- A Google Earth application

Results obtained from the rapid visual screening process can be used for a range of important applications including:

- Prioritizing buildings for further evaluation
- Prioritizing mitigation needs
- Supporting higher-level assessments and mitigation options by experts
- Allowing for an efficient allocation of resources
- Developing emergency preparedness plans in the event of a high-threat alert
- Planning post-event evacuations, rescues, recoveries, and safety evaluation efforts

The results are especially useful for identifying a specific asset for more detailed study, verifying results, and developing mitigation measures that will reduce the risk ratings to a more acceptable level. Buildings can be ranked by risk and resiliency to allocate potential resources (such as grant money) in an effective manner to reduce, in a cost-benefit way, major vulnerabilities. By adopting an all-hazard approach, cost-savings, efficiency, and better performance can be achieved following the screening of buildings.

(Continued on Page 15)

INTENDED USERS

- Engineers and architects
- City, county and state officials
- Emergency managers
- Law enforcement agencies
- Lenders
- Insurers
- Building owners and operators
- Facility managers
- Security consultants

SIXTEEN IRVS BUILDING TYPES

1. Wood frame
2. Steel moment frame
3. Steel braced frame
4. Steel light frame
5. Steel, pre-engineered metal
6. Steel frame with cast-in-place con¬crete shear walls
7. Steel frame with unreinforced ma¬sonry infill walls
8. Concrete moment frame
9. Concrete shear walls
10. Concrete frames with unreinforced masonry infill walls
11. Precast concrete tilt-up walls
12. Precast concrete frames with con¬crete shear walls
13. Reinforced masonry bearing walls with wood or metal deck diaphragms
14. Reinforced masonry bearing walls with precast concrete diaphragms
15. Unreinforced masonry bearing walls
16. Manufactured homes

High Performance Based Design Analysis: Evaluating Proposed Building Projects Based on Performance

by Roger Grant*

Decisions to build new or renovate existing facilities are major challenges for building owners. Once a need for new space is determined, perhaps as a result of having performed an assessment of existing facilities using the IRVS process (as described in the accompanying article on IRVS) or in response to organizational needs, the typical path often relies on producing a preliminary plan based on previous projects undertaken by the owner and his design consultant. While this helps to ensure some degree of certainty based on familiarity, does it produce the best plan to fit all of the owners needs for the facility? And what if the owner has multiple and varied requirements for the building that include not only energy use, reduction, and sustainability, for which LEED credit acquisition goals might drive a certain model of performance, but also safety and security requirements?

The Energy Independence and Security Act of 2007 (EISA-2007)[1] defines a high-performance building (HPB) as one that "integrates and optimizes on a life-cycle basis all major high-performance attributes, including energy conservation, environment, safety, security, durability, accessibility, cost-benefit, productivity, sustainability, functionality, and operational considerations." EISA-2007 also established an aggressive plan for achieving energy independence (e.g., zero-net-energy) in the Nation's building stock by the year 2030.

As the EISA Act of 2007 mandates, Federal government facilities are to be net zero consumers of energy by 2030 and to do so while also being high performing in other areas such as durability, safety, and security while at the same time being cost effective. Many private building owners have the same goals. So, can the many and varied goals an owner might have be evaluated very early in the planning process, without developing full conceptual design solutions, to support the decision-making and guide the development of a more effective conceptual design solution?

In pursuit of its mission to improve the safety and security of the Nation's infrastructure and in support of the goals of EISA 2007, DHS S&T IDD entered into a partnership with the

(Continued on Page 5)

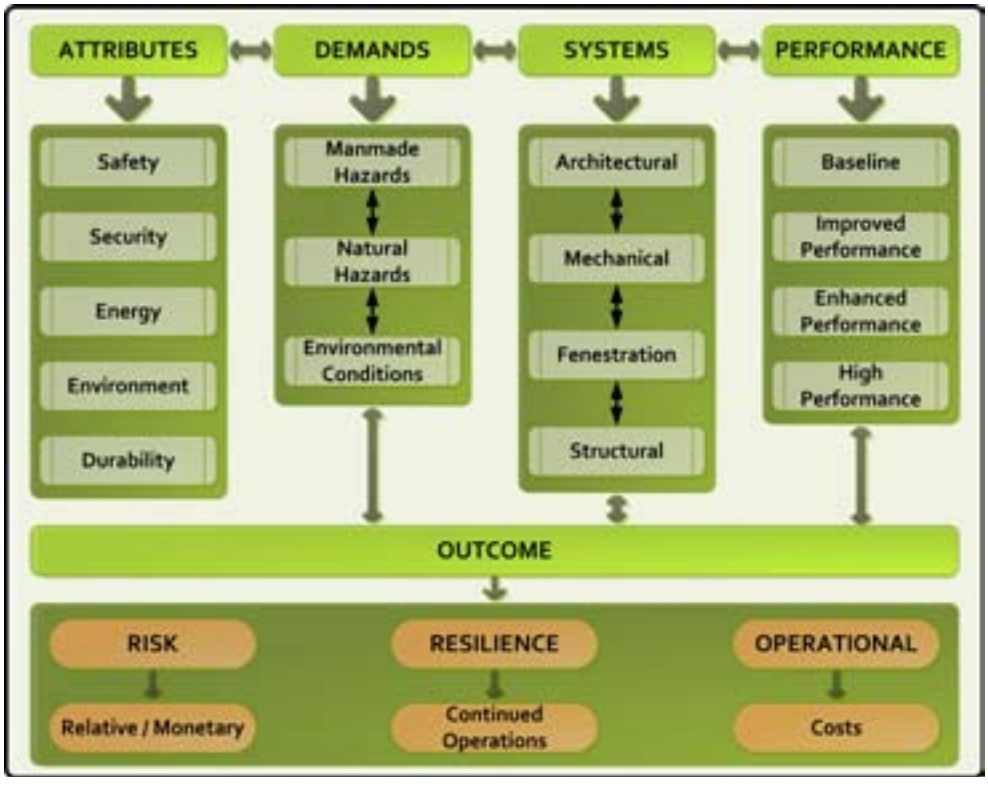


Figure 1. Owners Performance Requirements Model

1. The Energy Independence and Security Act of 2007 (EISA-2007), available at http://energy.senate.gov/public/_files/getdoc1.pdf.

OPR *(Cont. from 4)*

National Institute of Building Sciences (Institute) to develop an Owner Performance Requirements (OPR) Model that establishes high-performance operational, resilience, and risk targets and identifies the parameters that allow project owners to identify their goals for a project, including type, size, and location, and then evaluate alternative scenarios. The OPR Tool and the IRVS, the focus of another article in this newsletter, are developed within the same DHS S&T program and share common principles of how safety and security risk and resiliency are defined and evaluated and how they interrelate with other aspects of building performance. For more information on the DHS S&T IDD program, see the DHS website at http://www.dhs.gov/xabout/structure/gc_1224537470473.shtm.

The OPR modeling process allows building owners in the public or private sector to optimize their investments in building security, along with safety, energy conservation, environmental footprint and durability, in addition to evaluating the resulting risk and resilience of a proposed project. The process is available in an online software program specifically focused on establishing Owner Project Performance Requirements (OPR). The OPR Tool provides project planners with a previously unavailable resource for selecting and documenting performance goals for a project. The tool is intended to be used by facility planners, financial analysts, and designers or developers familiar with building technology and planning. This first-phase effort, limited to enclosure systems for new, as well as renovations of existing office buildings, lays the technical foundation and software framework for expanding the approach in later phases to address the whole building and additional building types.

The OPR model, depicted in Figure 1 (on Page 4), is strictly performance-based and does not identify prescriptive solutions for building systems to achieve targeted performance objectives, leaving this to the subsequent work of the design team. By evaluating performance of high level building attributes on a functional basis against demands that the building must face based on its location and the owner's needs, the model identifies increasing levels of performance that the systems that

(Continued on Page 6)

EISA 2007 Attribute	Sub-attribute	Functional System
Safety	Seismic Resistance	Structural
	Wind Resistance	Structural
	Flood Resistance	Structural
	External Fire Protection	Structural
Security	Blast Protection	Structural
	External CBR Protection	Mechanical
	Ballistic Protection	Structural
Energy Conservation	Thermal Transfer	Architectural, Fenestration
	Air Tightness	Architectural
	Renewable Energy – Solar	Mechanical
	Renewable Energy – Natural Ventilation	Fenestration
	Daylighting	Fenestration
Environment	Environmental Footprint	Mechanical, Fenestration
	Acoustic Transmission	Architectural
Durability	Water Penetration	Architectural
	Water Vapor Migration	Architectural
	Building Service Life	Architectural

Table 1: OPR Attributes and Systems.

OPR *(Cont. from 5)*

are ultimately designed for the building will need to meet. Expected performance of the major systems of the building is estimated for risk, resilience, and operations in terms of monetary and operational outcomes — the Owner Performance Requirements. The Attributes, Sub-attributes and primary Systems evaluated are identified in Table 1 (See Page 5).

The OPR Model is implemented through the web-based OPR Tool. To get started using the OPR Tool, go to www.oprtool.org and set up a free account. With an account established, the user can create a project with up to four scenarios that represent alternative potential solutions to be evaluated and compared. Reports to aid in the analysis, communicate the selected alternatives, and identify the project objectives can be generated.

Creating a scenario requires capturing general project information and performance objectives at a very early stage in the planning process. The information that the Tool needs to evaluate a project is identified in Table 2. It is provided by responding to a series of input options for a project scenario evaluation.

With the critical information for a project scenario identified, the OPR tool evaluates performance for the range of attributes identified as critical to enclosure performance, making it possible for an owner to evaluate all of the critical aspects of performance at one time. The result is the ability to see side-by-side the cost and benefits of enhancing or downplaying all aspects of a proposed enclosure scenario for a project. In this way, cost-benefit based decisions about whether to enhance security can be made considering the corresponding impact on energy conservation, for example. As part of the analysis, the relative cost to provide the targeted level of security protection can be evaluated alongside the potential risk in terms of estimated exposure from a security threat. This same kind of evaluation can be performed for all of the project's attributes using the Dashboards generated by the program.

The Scenario Comparison feature allows for the development of up to four different scenarios that can be compared side by side so that the consequences of different choices can be evaluated. This is especially important early in the planning cycle before any design decisions have been made and is a powerful feature of the tool. Different levels of performance for the same basic building can be evaluated to select the best option based on the range of funding available, risk and resilience targets, and payback models for operational investments.

When sufficient scenarios have been explored, a Performance Report for the selected scenario can be generated. This report can be used as guidance for the design team to

(Continued on Page 12)

Category	Parameter	Category	Parameter
General Project Information	Gross Building Area Quality Class State and City Location	Facility Resilience Information - Security	Blast Charge Strength Blast Range/Proximity Ballistic Threat Level CBR Agent Type CBR Exposure CBR Range/Proximity
Project Performance Benchmarks	Operational Performance Resilience Performance Risk Level		
Life Cycle Information	Use Period Unit Energy Cost Service and Maintenance Cost Escalation Rates Discount Rate Occupancy Information Indirect Project Costs	Facility Operations Information	Exterior Glazing Percentage Air Tightness/Leakage Daylighting Natural Ventilation Solar Energy Water Penetration Water Vapor Migration Service Life Outside Sound Level Acoustic Benchmark Level
Facility Resilience Information - Safety	Seismic Design Category Flood Plain Flood Depth Flood Velocity Wind Speed Wind Exposure Tornado Protection		

Table 2: OPR Input Parameters

Maximizing Public-Private Collaboration for Critical Infrastructure Protection

by Keith Murray, Executive Vice President, Virtual Emergency Services,
Jim Wong, Chairman & CEO, First Response Solutions Inc., and
Charles W. Newsome, President, First Response Solutions Inc.

In compliance with Presidential Policy Directive 8: National Preparedness (PPD-8), the National Preparedness Goal, promulgated by DHS in September, 2011, provides much needed foundation and protocol to help the country create an integrated, layered, and all-of-Nation approach to preparedness. In this guidance document, DHS defines success as:

> **A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.**

Attendant to the five mission areas (Prevention, Protection, Mitigation, Response, and Recovery) are capabilities and preliminary targets to help direct and facilitate public-private collaboration in support of national preparedness, to include planning for a no-notice, cascading incident, such as a large-scale earthquake, a major hurricane, or a weapons of mass destruction/disruption (WMD) attack. Among the core capabilities, Planning, Public Information and Warning, and Operational Coordination span all five mission areas. In this milieu, intelligence and knowledge management undergird collaborative efforts.

Mission Area Components of the National Preparedness System

In protecting the country's critical infrastructure — 85 percent of which is owned and operated by the private sector — business owners, asset managers, and security/emergency personnel face several dilemmas: 1) given the all-hazards environment in which we live, what is the optimal level of investment to ensure organizational resilience;? 2) beyond the dissemination of indications and warnings, how much can the private sector depend on the government to protect private assets before, during, and following an incident;? and 3) weighing risks against the backdrop of competing demands for resources, how does an organization justify expenditures for national preparedness, as defined in PPD-8?

In responding to the questions above, one should note that risks are dynamic, varying by critical infrastructure, type of disruptive event, country region, or even time of year; therefore, it is unlikely a clear formulaic solution will emerge. That said, the core capabilities and capability targets enumerated in the National Preparedness Goal are designed to help organizations improve their resilience. While metrics for each capability are being developed, it might be useful for organizational leaders, especially in the private sector, to capitalize on the definition of infrastructure resilience created by the National Infrastructure Advisory Council

(Continued on Page 8)

Public-Private *(Cont. from 7)*

(NIAC), which the President commissioned a month after 9/11. The NIAC is comprised of a maximum of 30 volunteers that the President appoints, most of whom work in the private sector. In 2009, NIAC defined infrastructure resilience as:

Robustness: The ability to maintain critical operations and functions in the face of crisis.

Resourcefulness: The ability to skillfully prepare for, respond to, and manage a crisis or disruption as it unfolds.

Rapid Recovery: The ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption.

In business parlance, the 3Rs (see above) help to establish resilience as a competitive strategy, with a time horizon that can be used to calculate financial returns on preparedness. Although rapid recovery often determines whether or not an organization survives, the topic is often given short shrift in budget development. Part of the problem is that it is difficult to estimate opportunity costs, until a disruptive event actually occurs. Towards this end, corroborating the capabilities and targets addressed in the protection mission, we have found common pitfalls as follows:

- Threat assessments were not conducted or if available, were not integrated as part of an organization-wide preparedness plan.

- Emergency plans were outdated and did not include all stakeholders.

- Rapid recovery of IT systems was not included in preparedness planning.

- Access to emergency plans was limited to internal security personnel, with critical data not available to incident commanders and first responders.

- Employee rosters, floor plans, location of utilities and fire protection systems, and contents of factories, warehouses, and laboratories were not available or accessible during an incident.

- Preparedness plans were not used to train personnel, thus employees were not aware of their responsibilities during or following a disruption.

- Personnel resilience plans were inadequate to aid in rapid recovery of either their organizations or families.

- Emergency preparedness budgets were severely constrained and focused on near-term crisis management, with scant attention to rapid recovery.

- Supply chains were not included in the threat assessment, especially as part of cyber defense.

- Preparedness is not an integral part of new employee orientation or training.

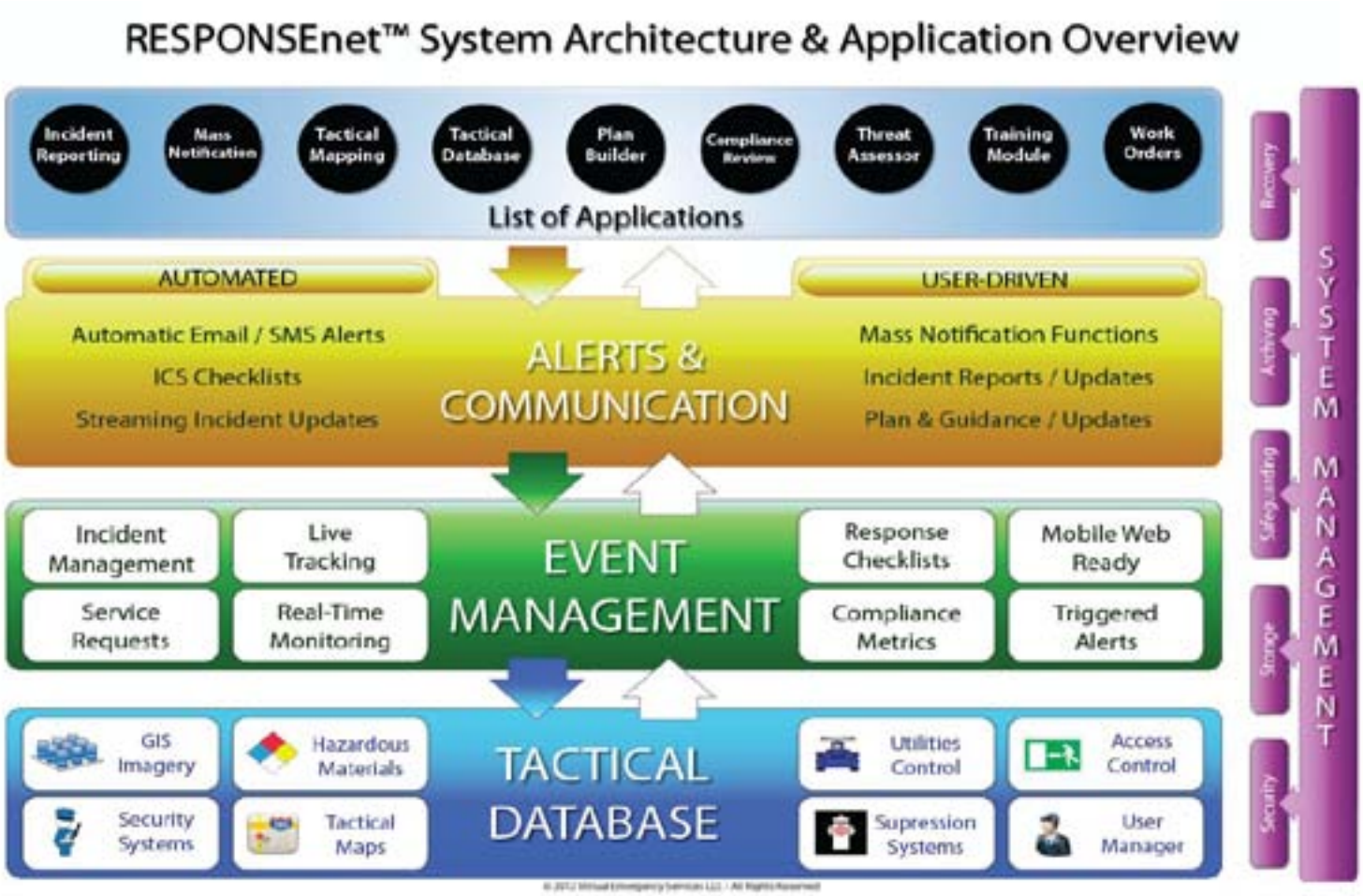
For business owners, rapid recovery is a significant predictor of viability, as the following statistics show:[1]

- An estimated 25 percent of businesses do not reopen following

(Continued on Page 9)

1. Impact on U.S. Small Business of Natural & Man-Made Disasters, presented by HP and SCORE: Counselors to America's Small Business. See http://www.edwardsinformation.com/content/ImpactofDisaster.pdf.

Public-Private *(Cont. from 8)*



a major disaster.[2]

• Illustrating the increasing importance of the 3Rs as they apply to IT, of companies experiencing catastrophic data loss:

- 51 percent of companies closed within 2 years.[3]
- 80 percent of companies that do not recover from a disaster within one month are likely to go out of business.[4]
- 75 percent of companies without business continuity plans fail within three years of a disaster.[5]
- Companies that are not able to resume operations within ten days (of a disaster hit) are not likely to survive.[6]
- Of those businesses that experience a disaster and have no emergency plan, 43 percent never reopen; of those that do reopen, only 29 percent are still operating two years later.[7]

It is also our observation that many private sector organizations operate under the errant assumption that first responder agencies will be immediately available and will not require assistance in incident management. Whereas collaboration with first responders is more common with critical infrastructure industries, the entire community benefits from closer cooperation. Again, intelligence

(Continued on Page 16)

2. "Open For Business" a publication of The Institute for Business & Home Safety (IBHS), a nonprofit association that engages in communication, education, engineering and research for the insurance industry. See www.ibhs.org/docs/OpenForBusiness.pdf.
3. University of Texas Center for Research on Information Systems, as cited in *Datamation*, June 14, 1994.
4. Jonathan Bernstein, President, Bernstein Crisis Management, LLC in Director, 51(11), (June 1998), 44.
5. Bruce Blythe, CEO, *Crisis Management International in Blindsided: A Manager's Guide to Catastrophic Incidents in the Workplace*, (Portfolio Hardcover, August 22, 2002).
6. http://www.techworld.com/cmsdata/whitepapers/833/How%20Secure%20is%20your%20Storage_Symantec.pdf.
7. *The Hartford's Guide to Emergency Preparedness Planning*, created by The Hartford Financial Services Group and now published by J.J. Keller & Associates.

Super Bowl Stadium Security

On Sunday, February 5, 2012, history repeated itself when the New York Giants defeated the New England Patriots 21-17 in Super Bowl XLVI in Lucas Oil Stadium, Indianapolis, IN. The Super Bowl is always a major event, but given the contention between the two teams, this particular Super Bowl was even more highly anticipated. According to the Nielsen Company, an estimated 111.3 millon people watched Super Bowl XLVI, making it the most watched television show in U.S. history.[1] In Lucas Oil Stadium, 68,658 enthusiastic football fans cheered for their team or simply reveled in the festivities.[2] While this is a decrease in attendance from the previous year, Lucas Oil Stadium is a significantly smaller venue than the Cowboys Stadium in Dallas, Texas. Regardless of the number, the Super Bowl is an annual event that entertains millions of viewers with memorable commercials, spectacular musical performances, whether they are in tune or not, and nail-biting plays. Therefore, it should come as no surprise that, in terms of infrastructure protection, the Super Bowl is a high priority national security event given that it is a confined space and therefore a potential target for both Mother Nature and terrorists. Furthermore, since stadiums are included in the DHS Commercial Facilities Sector, which monitors facilities that "operate on the principle of open public access, meaning that the general public can move freely throughout these facilities without the deterrent of highly visible security barriers,"[3] security, including crowd and traffic control, is a challenge.

In order to prepare for major events where large amounts of people, including U.S. officials and foreign dignitaries, will attend an event that is considered to be nationally significant, the Federal government has developed a classification system.[4] Events such as presidential inaugurations, State funerals, Democratic and Republic National Conventions, State of the Union Addresses, and major spectators sports, including several Super Bowls, are designated by the Secretary of DHS as a National Security Special Event (NSSE).[5] In 1998, the U.S. Secret Service acquired the responsibility of leading "the design and implementation of the operational security plan"[6] for NSSEs. According to DHS, "[o]nce an event is designated a NSSE, the Secret Service relies on existing partnerships with federal, state and local law enforcement and public safety officials with the goal of coordinating participating agencies to provide a safe and secure environment for the event and those in attendance."[7] However, as previously stated, the Secretary of DHS designates an event as a NSSE.

This year, in addition to standard security protocols, DHS Secretary Janet Napolitano announced a partnership between the DHS public awareness campaign "If You See Something, Say Something™" and the National Football League (NFL) to ensure the safety of patrons, employees, and players during Super Bowl XLVI. In essence, this program was integrated into the security plans and operations already in place for the Super Bowl (See text-box on Page 13).[8]

(Continued on Page 13)

1. http://www.nfl.com/superbowl/story/09000d5d826b388c/article/super-bowl-is-mostwatched-tv-show-in-us-history-again.
2. http://prod.static.patriots.clubs.nfl.com/assets/docs/gamebooks/2011/20120205_gamebook.pdf.
3. http://www.dhs.gov/files/programs/gc_1189101907729.shtm.
4. http://cip.gmu.edu/archive/CIPHS_TheCIPReport_August2009_NationalMonumentsandIcons.pdf
5. For more information about NSSEs, please see the U.S. Secret Service website at http://www.secretservice.gov/nsse.shtml and the article, *U.S. Secret Service*, in the August 2009 issue of "The CIP Report" at http://cip.gmu.edu/archive/CIPHS_TheCIPReport_August2009_NationalMonumentsandIcons.pdf and the Congressional Research Reports *National Special Security Events* (2007) at http://assets.opencrs.com/rpts/RS22754_20071106.pdf and *National Special Security Events* (2009) at http://www.fas.org/sgp/crs/natsec/RS22754.pdf.
6. http://www.secretservice.gov/nsse.shtml.
7. http://www.dhs.gov/xnews/releases/pr_1167323822753.shtm.
8. http://www.dhs.gov/ynews/releases/20120201-napolitano-announces-see-something-say-something-partnership-nfl-superbowl.shtm.

Legal Insights

Meeting Energy Conservation Mandates, Sustainability Objectives with Energy Savings Performance Contracts

by Tony Keane, CAE, President and Chief Executive Officer of the International Facility Management Association, and
Jeffrey Johnson, J.D., Director of Government Relations of the International Facility Management Association

Improving energy efficiency with an objective of attaining cost savings is certainly nothing new in the facility manager's portfolio of responsibilities. Over the past decade, an added emphasis has been on not only having an energy management program that saves money but also decreases greenhouse gases and/or contributes to a company's sustainability initiatives. With a struggling economy combined with a public that is continually growing in its support of sustainability, energy management programs will continue to increase in importance.

The U.S. Federal government is the largest single owner of facilities in the world, owning and leasing more than 500,000 facilities worldwide. Couple this with the fact that the Federal government is the single largest consumer of energy in the United Sates and it is easy to see why conserving energy would be of utmost importance.

An insistence on energy conservation is nothing new in managing Federal facilities. It was almost four decades ago that the first Federal initiative related to energy conservation was put in place as a way to combat the 1970s oil crises and rising public concern over stable energy sources. The Federal Energy Management Program (FEMP) was implemented in 1973 to assist the Federal government in implementing cost-effective energy management practices to both enhance U.S. energy security and environmental responsibilities.

The cornerstone of U.S. energy efficiency legislation in facilities for a 30-year period was the National Energy Conservation Policy Act (NECPA) of 1978, which was the first step toward retrofitting Federal buildings to increase energy efficiency. Since its implementation, NECPA has been amended with both incentives and mandates to reduce energy consumption in both the public and private sector. A major change to NECPA came in the form of the Energy Policy Act of 1992, which granted both direct and indirect incentives tied into energy efficiency in Federal facilities, including allowing agencies to accept financial incentives, goods, or services from utilities that led to energy efficiency.

In 1999, Executive Order 13213 — Greening the Government through Efficient Energy Management was signed that modified both NECPA and the Energy Policy Act of 1992 providing that agencies "shall maximize their use of alternative financing methods including energy savings performance contracts (ESPCs)..." According to *Energy Savings Performance Contracts Don't Measure UP, IG Finds*, an ESPC is a turnkey service "which provides customers with a comprehensive set of energy efficiency, renewable energy and distributed generation measures that are often accompanied by guarantees that savings produced by the project will be sufficient to pay for the initial capital expenditure." Standard improvements implemented via an ESPC can include energy efficient lighting, building management control systems and heating, and ventilating and air conditioning. Even though ESPCs are part of this legislation, they rarely were used as a tool for cost-effective energy efficiency from authorization of this E.O. through 2007.

In the Federal context, an agency

(Continued on Page 14)

OPR *(Cont. from 6)*

give them quantifiable targets to strive for and to report against. The Performance Report establishes the Owner Project Performance Requirements in terms of design performance goals and a broad range of potential costs to achieve those goals. This equates to the establishment of Owner Project Requirements, the first step identified by the building commissioning process as standardized in ASTM E.06.55.09 Standard Practice for Building Commissioning, for "achieving, verifying, and documenting that the performance of facilities, systems, and assemblies meets defined objectives and criteria." With these requirements firmly in place, a proven step towards achieving a successful project and integrating the owner and design teams early on is established.

The OPR Tool in a Beta Release Version and the High Performance Based Design for Building Enclosures Project Report that documents its development are part of the DHS S&T Building Infrastructure Protection Series (BIPS). Both are available for industry use and evaluation from the OPR Tool website. Comments, suggestions, and experiences from using them are welcomed and will be incorporated into subsequent versions. See the website for details on how to use the tool, obtain the report, and provide review comments. ❖

Roger Grant, CSI, CDT, is Project Manager for the National Institute of Building Sciences High Performance Based Design program for DHS. He also is the staff liaison to the Institute's High Performance Building Council. Prior to his work as a project manager for the Institute, he was Director of Technical Services for the Construction Specifications Institute.

The National Institute of Building Sciences, authorized by Congress in 1974, is a nonprofit, nongovernmental organization that brings together representatives of government, the professions, industry, labor and consumer interests to identify and resolve building process and facility performance problems. The Institute serves as an authoritative source of advice for both the private and public sectors with respect to the use of building science and technology. For more information, visit www.nibs.org.

Stadium Security *(Cont. from 10)*

In addition to working with local law enforcement in Indiana, the NFL, event staff, and volunteers, DHS also asked for the public's assistance. In fact, the public's cooperation and participation is the backbone of the "If You See Something, Say Something™" campaign. If anyone sees anything suspicious, such as an unmanned bag, then authorities should be immediately alerted. According to DHS, this campaign "is a simple and effective program to engage the public and key frontline employees to identify and report indicators of terrorism and terrorism-related crime to the proper transportation and law enforcement authorities."[9] In addition, DHS worked with State and local law enforcement partners and the NFL to provide additional security assets to screen cargo shipments, secure the air space, and provide personnel security screening training to event security officers.

Prior to the Super Bowl, Secretary Napolitano participated in a roundtable discussion with representatives from the National Collegiate Athletic Association, National Federation of High Schools, Indiana Sports Corporation, USA Track & Field, USA Gymnastics, USA Synchronized Swimming and USA Diving, to expand the campaign and improve collaboration with amateur sports organizations. Furthermore, in a separate endeavor, The University of Southern Mississippi's established the Center for Spectator Sports Security Management in 2006 to conduct research and develop education programs in sport event security. In fact, The University of Southern Mississippi School of Human Performance and Recreation developed a new online Graduate Certificate in Sport Security Management. This intensification of stadium security stems from the increased awareness that these facilities are ideal targets. For more information about the Graduate Certificate in Sport Security Management, please visit http://www.usm.edu/sporteventsecurity/newWeb/gradcert.pdf.

> *As part of the Department's "If You See Something, Say Something™" partnership with Super Bowl XLVI, campaign graphics will appear on the videoboard and televisions throughout Lucas Oil Stadium on game day. Safety messaging will also be printed in game programs and fan guides for staff, players, and volunteers. Indiana and the City of Indianapolis have continued to expand and support the campaign over the past year since initially partnering with DHS. In addition, "If You See Something, Say Something™" advertisements will be seen throughout Indianapolis at the airport, hotels, restaurants, bars, and on buses, magazines and visitor guides.*
>
> - U.S. Department of Homeland Security

For more information about the "If You See Something, Say Something™" campaign, please visit http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm. ❖

[9] http://www.dhs.gov/ynews/releases/20120201-napolitano-announces-see-something-say-something-partnership-nfl-superbowl.shtm.

Legal Insights *(Cont. from 11)*

hires an energy savings company (ESCO) to perform a detailed energy audit to identify areas where the facility can reduce energy usage. The contracting agency then will pay the ESCO a specified share of the energy cost savings guaranteed under the ESPC. Typically, the ESPC provides that the government will pay the ESCO an annual-in-advance payment at the start of each year in an amount less than the ESCOs guaranteed savings for that year.[1] In its most basic form, an agency contracts with an ESCO to provide energy efficiency improvements to a facility or group of facilities and, in exchange, the agency agrees to pay the ESCO a portion of the money saved through decreased energy and, in some cases, water usage.

In 2009, the Obama Administration issued Executive Order 13514 — Federal Leadership in Environmental, Energy and Economic Performance. This order emphasizes improving energy efficiency through existing Federal requirements as well as establishing new Federal government sustainability goals and the reduction of greenhouse gas emissions. These new mandates, which were not accompanied with any new money for energy projects, only underscored the importance of alternative contracting vehicles like ESPCs.

In order to ensure agencies fully meet the goals set out in E.O. 13514, President Obama announced on December 2, 2011, a nearly $4 billion combined public-private sector commitment to upgrading Federal facilities to save billions in energy costs. With this announcement, a Presidential Memorandum was issued stating the Federal government will enter into a minimum of $2 billion in performance-based contracts in Federal building energy efficiency within 24 months of this memorandum.

While ESPCs have been the target of criticism for failing to account for administrative costs of measure and verify energy savings, performance contracting is the only option available to Federal agencies looking for financing for large scale energy efficiency projects. While these contracts currently are fraught with problems as they remain a relatively new form of contract vehicle, they are a potentially lucrative opportunity for those in the private sector wishing to engage in energy efficiency projects through utilization of the performance-contracting model.

While arguably this approach has not yet to be effectively demonstrated on the Federal level, many of the rigid contract requirements that prevent agencies from more effectively utilizing ESPCs do not exist on the State level or in private sector applications. This suggests that ESPC utilization will continue to grow both within and independent of the government market. Even with statutory and budget restrictions, ESPCs in the Federal space have been shown to provide 30 percent higher savings per square foot than in municipal and State governments.[2] Suggesting that even with pervasive problems in the Federal ESPC model, it is still more effective than anything else currently in use at either the State or local level.

In the decades since energy management legislation was first enacted, a perfect process to ensure Federal facilities both conserve energy to lower costs and to positively impact the environment has yet to be found. While there are multiple challenges with the ESPC model, they are the most effective option for the Federal government to lead by example and improve energy efficiency in their facilities. As the ESPC model can be improved upon by the U.S. Federal government, State, local, and private sector entities also may increase their ESPC use. ❖

1. 2001 U.S. Comp. Gen. LEXIS 217: FAR 23.05(b)(1).
2. Andrews Supra Note 49, at 4.

IRVS *(Cont. from 3)*

**As director for the Federal Emergency Management Agency's (FEMA) Hazus program for 17 years, Mr. Schneider oversaw the development of the most advanced risk assessment models for estimating the effects of earthquakes, riverine and coastal floods, and hurricane winds, and a data management system that facilitates the updating of statewide datasets used in a Hazus analysis. Currently, Mr. Schneider is engaged in the following hazard-related activities:*

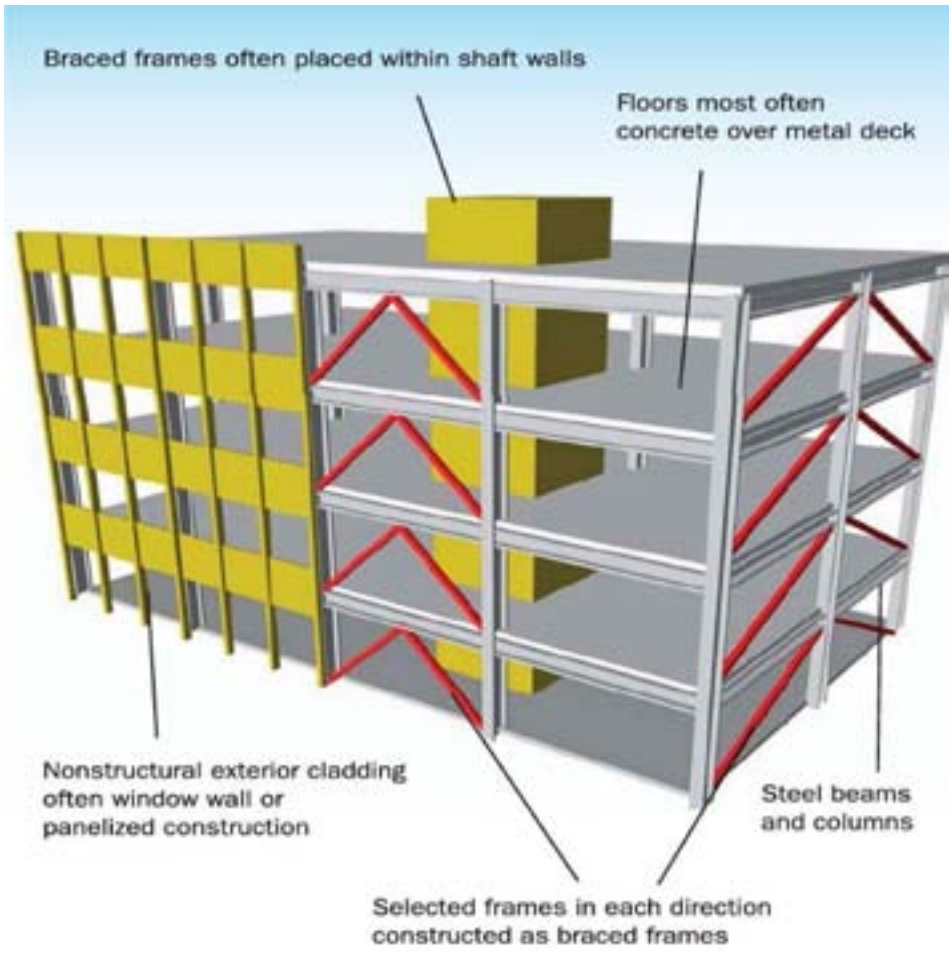
- *Consultant for FEMA's Independent Verification and Validation Program (IV&V) program that assesses Hazus to establish a baseline for accuracy, maximize quality and functionality, and reduce costs associated with maintenance and enhancement.*

- *Program Director for expert committees for oversight of FEMA's Hazus Earthquake, Wind, Flood, Coastal Surge and Tsunami Model development, Hazus software maintenance, the Hazus software open source initiative, and the Department of Veteran Affairs (VA) Seismic Risk Assessment Model.*

- *Consultant to the Department of Homeland Security Infrastructure Protection & Disaster Management Division on the development of a tool for Integrated Rapid Visual Screening for use by states and communities for determining the multihazard threats, consequences, and vulnerabilities, and risk and resilience ratings related to facilities.*

- *Program Director for the National Institute of Building Sciences' newly constituted Multihazard Mitigation Council that will promote increased all-hazard disaster resilience in homes and commercial buildings as part of a whole building strategy that incorporates sustainability, security, and use of GIS and other technological tools.*

Steel Brace Frame (FEMA 454, 2006)



The National Institute of Building Sciences, authorized by Congress in 1974, is a nonprofit, nongovernmental organization that brings together representatives of government, the professions, industry, labor and consumer interests to identify and resolve building process and facility performance problems. The Institute serves as an authoritative source of advice for both the private and public sectors with respect to the use of building science and technology. For more information, visit www.nibs.org.

Public-Private *(Cont. from 9)*

sharing and knowledge management is at the heart of collaboration, helping to reduce pain and suffering, and improve effectiveness of the entire community in combating disruptions.

Under emergency situations, disparate and non-standard systems are frequently utilized, adding to the chaos. With the advent of Web 2.0 technologies, an integrated, layered community effort should be highly feasible. For example, the system should allow stakeholders — police, fire, and other first responders — to instantly access a myriad of critical infrastructure data, including tactical/emergency response plans, evacuation routes, satellite and oblique aerial imagery, exterior and interior photos, floor plans, utility shut-off locations, hazardous substance inventories, and more. It also should provide the incident commander with a means to develop, update, and disseminate various emergency management plans, BCP, COOP, documents, vulnerability assessments, protocols, and other data to assist in incident management. For organizations contemplating an initial investment or upgrade to their system, there are standard guidelines and features to ensure functionality, reliability, and interoperability, as follows:

Preferred Features:

- DHS Safety Act Certified - Qualified Anti-Terrorism Technology (QATT)
- Compliance with National Incident Management System guidelines
- Follows recommended practices of both National Fire Protection Association 1600 and 1620
- On demand access to Planning, Training, and Response data
- Ability to track incident data (time/date) in real-time with integrated reporting and metrics
- Functionality to create, complete, track, and report on various types of assessments
- Web-Based Plan management, development, dissemination, and printability
- Integrated help and training (SCORM compliant)
- Secure interface to IP Surveillance Cameras/DVR's
- Ability to improve communications/Alerts (Private/Public)
- Secure login on redundant, protected servers
- 100 percent accessibility regardless of internet connectivity
- Full Web-Based Emergency Plans that track updates and edits
- Automated Best-Practice "Response Checklists"

In summary, few aspects of national preparedness have been more misunderstood, even benignly neglected, in the post-9/11 security environment than the cardinal necessity of securing critical facilities — whether government, business, NGO, or academic — through a single, layered, and integrated application. The good news is that state-of-the-art and operationally vetted technologies and methodologies are coming on line that accomplish all of this, and more, in compliance with PPD-8. ❖

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1