THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 9 NUMBER 1

JULY 2010

GOVERNMENT FACILITIES

Contact: CIPP02@gmu.edu

703.993.4840

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

This month's issue of *The CIP Report* features the Government Facilities Sector. This sector, which recently transitioned into the National Protection and Programs Directorate (NPPD) at the U.S. Department of Homeland Security (DHS), has been diligently working to update security standards for Federal facilities.

GEORGE MASON UNIVERSITY

School of Law

CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, the Infrastructure Protection Branch Chief at the Federal Protective Service (FPS) provides an overview of the Government Facilities Sector. Then, the Executive Director of the Interagency Security Committee (ISC) discusses the new standards, *Physical Security Criteria for Federal Facilities* (PSC) and the *Design-Basis Threat Report* (DBT), which were established to better protect nonmilitary Federal buildings and facilities. The Institute for Infrastructure and Information Assurance (IIIA) at James Madison University (JMU) describes an event they recently co-hosted with the Federal Facilities Council of the National Academy of Sciences about "Safe, Secure, and Sustainable Facilities." Next, we discuss the energy capabilities of commercial facilities leased by the Federal government and we summarize a recent report by the General Accountability Office (GAO) which reviews the use of contract guards at Federal facilities. Finally, this month's *Legal Insights* provides a risk analysis of security countermeasures for Federal facilities.

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

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

The Government Facilities Sector

by Mark P. Harvey
Infrastructure Protection Branch Chief
Risk Management Division
Federal Protective Service

Sector Overview

The Government Facilities Sector (GFS) is one of the largest and most diverse sectors within the National Infrastructure Protection Plan (NIPP), and includes Federal, State, local, tribal, and territorial assets and associated elements located around the world. Although some types of government facilities are exclusive to the GFS, government facilities also exist in most other sectors, but were categorized based on predominant use. Many of these assets and associated elements are highly complex and require the highest levels of security because of their sensitive and unique mission, while others are necessarily open to the public to provide routine services. In all cases, the American people depend on the services provided by these facilities on a daily basis, whether a facility is providing a routine government service or ensuring their safety and security.

In addition to physical structures, the sector also considers cyber elements that contribute to the protection of sector assets. The GFS is increasing attention to cyber security as its protective role expands from a human- and asset-centric philosophy to a mission-continuity philosophy. The sector remains focused on applying best practices for preserving the reliability of cyber elements housed within facilities. In addition to these preventive and protective measures, the GFS has assumed responsibility for promoting awareness of key Federal information security initiatives and compliance with industry standards, and has begun educating building occupants, employees, and sector partners about the dangers of cyber threats and the impact of these threats across the sector.

The Federal Protective Service (FPS), as part of the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), is the Sector-Specific Agency (SSA) for the GFS. Building on its traditional role as protector of facilities owned and leased by the General Services Administration (GSA), FPS coordinates efforts among government at all levels to identify, assess, and enhance the protection of government facilities determined to be nationally critical.

The GFS also includes the Education Facilities Subsector, which covers pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools. This subsector includes both government-owned facilities and facilities owned by private-sector entities, so it faces some unique challenges. FPS works in close coordination with the Department of Education with regard to all schools.

The sheer size and scope of the GFS poses a challenge in providing for infrastructure protection efforts. The Federal government alone manages more than 3 billion square

(Continued on Page 3)

Sector Overview *(Cont. from 2)*

feet of space and more than 650 acres of land. The sector also covers the facilities owned and operated by the more than 87,000 municipal governments across the Nation, as well as U.S. embassies, consulates, and military installations located all over the world. These facilities face a full range of both natural and man-made hazards.

Sector Coordination Efforts

Overall GFS coordination is conducted through FPS Headquarters, as the focal point for SSA activities and responsibilities. Coordination mechanisms are utilized within the GFS and cross-sector to support GFS activities. The GFS has sought to improve the coordination of sector partners and identify challenges that can be solved effectively through their combined efforts. The GFS has traditionally been a leader in securing assets, and there are many valuable lessons that can be shared across the sector.

Interdependencies that exist between sectors are one reason why coordination mechanisms are critical to sector planning and operational efforts. Government facilities are highly interconnected, both physically and through a variety of information and communications technologies.

A Government Coordinating Council, chaired by FPS, is the primary coordination point with representatives from the government entities with the responsibility for the protection of government facilities. Due to its inherently governmental focus, security partners are limited to representatives from Federal, State, local, or tribal government entities involved in the protection of owned or leased facilities. FPS also represents the sector on the NIPP Federal Senior Leadership Council and through similar coordinating mechanisms established by other CIKR sectors.

Threats to the Sector

Although the sector has been a leader in security and preparedness, significant efforts to manage risk continue to be applied. Government facilities are attractive and strategically important targets for both domestic and international terrorists. Their symbolism, importance, and the value their services provide make them vital elements of their respective communities, and protecting these facilities remains a national priority. In addition, the size and dispersion of government facilities and associated elements introduces the full range of natural hazards that can potentially impact the sector. Because of the high-profile nature of the sector, government facilities operate within a very dynamic risk environment requiring a variety of well-coordinated protective measures to ensure the safety and security of citizens and the continued availability of essential government functions.

A historical examination of terrorist attacks in modern times shows the GFS to be the most frequently attacked of all the 18 CIKR sectors; this includes attacks against physical facilities, government personnel, and governmental cyber systems. The sector contains a number of assets that must be open to the public to conduct their daily activities, including such places as Social Security offices, Department of Motor Vehicle (DMV) locations, city halls, and so on. While many government facilities require public access, others are highly secure and restricted. These locations often take advantage of multiple and layered security measures, and contain highly sensitive information or materials.

During the past year, there have been several attacks aimed at government facilities and occupants, including the plane crash at the Internal Revenue Service (IRS) facility in Austin, and the shooting incidents at the Pentagon, Fort Hood, and the Federal Courthouse in Las Vegas. These attacks are a reminder of the magnitude of threats faced by the GFS because of their high-profile nature.

Mitigating Sector Risks

FPS has been actively involved in enhancing the security posture of a broad scope of Federal facilities by utilizing a variety of programs and tools, such as Operation Shield, the National Countermeasures Program, the Occupant Emergency Plan Guide, and the Risk Assessment and Management Program.

(Continued on Page 4)

Sector Overview *(Cont. from 3)*

In an effort to avert or obstruct potential insider threats as part of terrorist operations and criminal activity in and around Federal facilities, FPS employs Operation Shield. Operation Shield systematically measures the effectiveness of FPS countermeasures, including the effectiveness of FPS' Protective Security Officers in detecting the presence of unauthorized persons and potentially disruptive or dangerous activities. Operation Shield is a comprehensive operation that combines physical security expertise and law enforcement authority into an enhanced security team to provide a visual deterrent at FPS-protected facilities, with the goal of demonstrating the preparedness and agility of FPS' response to the current threat environment within our Federal community.

FPS has conceptualized and developed the National Countermeasures Program (NCP) to address all FPS countermeasure management issues. In the past, FPS utilized several contracts and vendors to supply screening equipment for Federal facilities. The new contracts, established by the NCP, allow FPS to more effectively manage screening operations for Federal facilities by utilizing one central point of service to acquire, train, maintain, and replace screening equipment on established schedules. FPS has awarded five-year blanket purchase agreements to Smiths Detection, to lease x-ray machines, and Ceia-USA, to purchase metal detectors.

In emergency situations, Occupant Emergency Plans (OEPs) can be used to minimize the potential for outcomes involving devastation and chaos. OEPs describe the actions that occupants should take to ensure their safety during an emergency situation, and by providing facility-specific response procedures for occupants to follow, OEPs can reduce the threat to personnel, property, and other assets within the facility, in the event of an incident inside or immediately surrounding a facility. For example, in February 2010, a small plane crashed into a building occupied by the IRS in Austin, Texas. During the FPS investigation of the crash, reports from employees in the building revealed that the IRS had well-written and well-rehearsed OEP and evacuation procedures. IRS employees had sighted and reported the low-flying plane and initiated the facility's OEP, which was appropriately executed. The facility was estimated to have housed as many as 200 individuals as the plane approached, yet the final tenant casualty toll included one fatality and 13 injuries. The saving of countless lives can be credited to the rehearsal and execution of an established OEP for the facility.

Photo courtesy of FPS.

To assist other agencies with the development of these plans, FPS has produced an OEP Guide that can be used as a reference tool and template when developing an OEP for a facility. This guide provides guidance pertaining to the preparation, implementation, and maintenance of OEPs with regard to national preparedness efforts of the NIPP and National Response Framework (NRF), and serves as a step-by-step approach for developing, implementing, and maintaining OEPs.

FPS developed and implemented the Risk Assessment and Management Program (RAMP) to improve risk mitigation at Federal facilities and enhance the safety and

(Continued on Page 5)

Sector Overview *(Cont. from 4)*

security of building occupants. This comprehensive tool was developed to improve and standardize the way FPS collects and manages information at every step of the security planning process, from the initial collection of data, to risk assessment, and countermeasure implementation. RAMP was launched in November 2009; it is a secure, Web-enabled system that has improved the way FPS collects, stores, analyzes, and shares security data on Federal facilities.

RAMP is based on a rigorous, quantitative, and standards-based risk assessment methodology. This methodology conforms to the NIPP baseline criteria to mitigate risk by incorporating threat, vulnerability, and consequence considerations. RAMP will help FPS to better manage the range of risk assessments, security tracking, and measurement processes, and RAMP users will be able to:

- Assess and analyze potential risks to Federal facilities stemming from crime, natural hazards, and terrorism to calculate the probability that an adverse impact will occur.
- Store, access, and report risk assessment findings, including historical information from pervious assessments and other documentation, in a central location.
- Automate and track countermeasures recommendations, implementation status, and life-cycle replacement schedules for security products.
- Provide countermeasure product information to assist in cost-benefit analysis.
- Perform comprehensive analyses of risks posed to Federal facilities and the means of reducing these risks.
- Automate basic administrative tasks, such as generating and routing letters, reports, presentations, and statistical analyses, and will allow for easy access to Occupant Emergency Plan information, callback lists, and other critical information that was previously spread across multiple systems.

The implementation of RAMP is a major milestone for FPS, and is expected to lead to significantly improved security planning at Federal facilities.

The GFS continues to strive toward a preparedness posture that ensures the safety and security of government facilities located domestically and overseas, to preserve essential government functions and services without disruption. Sector partners work together to implement a long-term government facility risk management program, organize and partner for government facility protection, integrate government facility protection as part of the homeland security mission, manage and develop the capabilities of the GFS, and maximize efficient use of resources for government facility protection.

(From left to right) Former FPS Director Gary Schenkel, Susan Burrill, Chief of Staff Michelle Bryan, and Acting Deputy Director Richard Cline at the NextGov Awards. *Photo courtesy of FPS.*

For additional information on the Government Facilities Sector or the Federal Protective Service, send an email to NIPP-GFS@dhs.gov.

Additional Highlights

2009 Presidential Inauguration

During the 2009 Presidential Inauguration, FPS conducted a major law enforcement effort to support the safe, efficient transition of executive power. FPS

(Continued on Page 15)

The Interagency Security Committee

by Austin Smith
Executive Director, Interagency Security Committee

Protecting our Federal facilities against evolving threats requires setting and implementing robust, risk-based security standards. These standards leverage over a decade of collaboration and research by experts across the Federal government to establish adaptable security measures that will better secure our Federal infrastructure.

- Secretary Janet Napolitano, Department of Homeland Security, April 12, 2010

Committee Creates Security Standards to Better Safeguard Federal Facilities

Protecting the Nation's more than 300,000 nonmilitary Federal facilities begins with the creation and implementation of facility security standards and best practices. The organization tasked with this responsibility is the Interagency Security Committee (ISC).[1] On April 12, 2010, the ISC released a new standard that supersedes earlier standards and an accompanying threat analysis document. Used together, these documents will standardize and strengthen security at covered Federal facilities.

About the ISC

Following the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, an Executive Order was signed establishing the ISC to address government-wide security for Federal facilities. The Assistant Secretary for Infrastructure Protection within the NPPD of DHS chairs the committee. Composed of chief security officers and other senior executives from 45 Federal departments and agencies, the ISC's mission is to enhance the quality and effectiveness of physical security in the more than 3.26 billion square feet of civilian Federal facilities in the United States. The ISC has promulgated several security standards and best practices that have contributed significantly to the security of the Nation's Federal facilities.

The full ISC meets quarterly. Members serve on subcommittees and working groups to develop physical security policies and standards that mitigate threats to employees and the visiting public. The ISC also engages with industry and other government stakeholders to advance best practices.

Physical Security Criteria for Nonmilitary Federal Facilities: A Single-Standard Approach

The ISC's new standards, *Physical Security Criteria for Federal Facilities (PSC)* and the *Design-Basis Threat Report (DBT)*, establish baseline physical security measures for all nonmilitary Federal buildings and facilities. The new standards bolster protection against terrorist attacks and other threats based on ongoing risk assessments. They are innovative, reflect extensive participation by ISC members, and consolidate prior standards.

The *Physical Security Criteria for Federal Facilities* is the culmination of 15 years of information gathering, information sharing, and lessons learned in Federal facility security. It provides consistency across existing standards and consolidates them into a single source for all facility physical security standards — a compendium of standards.

The compendium establishes a baseline set of physical security measures to be applied to all Federal facilities, at the same time that its framework allows for customization of security measures to address unique risks at a facility. These

(Continued on Page 17)

[1] The Interagency Security Committee resides organizationally in the Department of Homeland Security's National Protection and Programs Directorate, under the Office of Infrastructure Protection.

"Safe, Secure, and Sustainable Facilities"

Co-hosted by the Federal Facilities Council of the National Academy of Sciences and the Institute for Infrastructure and Information Assurance at James Madison University

National Academy of Sciences, Washington, DC
May 13, 2010

Event Overview

Today's economic and political environment has generated a tremendous premium and demand for facilities that are both secure and sustainable. Designing and renovating facilities that are both sustainable and secure is challenging, but with proper life-cycle planning, coordination, and good engineering, such designs are feasible. This year's event was the fifth annual homeland security symposium co-hosted by the Federal Facilities Council and the Institute for Infrastructure and Information Assurance, organized to bring together speakers from government, academia, and the private sector to identify areas of synergy, potential conflicts, and trade-offs among security and sustainability requirements.

The agenda included several case studies highlighting methods to achieve balanced design solutions that minimize environmental impacts and energy use as well as ensuring the health, safety, security, and comfort of building occupants. Case studies addressed the new DHS Headquarters complex, the Pentagon Renovation Program, and innovations associated with the design for the United States Embassy in London. Architectural design techniques to avoid security features posing an "armed camp" appearance were described. An important symposium theme was the role of building control systems in achieving effective security and energy saving solutions. Speakers discussed and provided updates on government and industrial facility design standards, requirements, and building code documents. DHS provided an overview of their research agenda for sustainable and secure building materials. Looking to the future, the symposium included an overview of the importance of educating the next generation on designing for sustainability based on James Madison University's new engineering program with a focus on sustainability.

For more information or to obtain a copy of the symposium agenda and proceedings, please contact Cheryl Wilkins, elliotcj@jmu.edu, (540) 568-4442, or visit the symposium website at: http://www.jmu.edu/iiia/2010symposium/index.html.

John Noftsinger, JMU Vice Provost for Research and Public Service. *Photo courtesy of JMU IIIA.*

Energy Smart & Greener Commercial Facilities: New Challenges in Protecting KRitical Feds

by Michael Ebert, Principal Research Associate, CIP/HS, George Mason University
Duminda Wijesekera, Associate Professor, Department of Information and Software Engineering, George Mason, and
James A. Momoh, Professor, Electrical Engineering School of Engineering, Howard University

While the overall theme of this issue of *The CIP Report* pertains to Government Owned Facilities in the contexts of critical infrastructure protection and homeland security, this article takes a slightly different look: are key resources (KR) — highly essential Federal human resources — adequately protected in commercial facilities where the government has leased space for its critical workforce? Digging deeper, do new and emerging technologies and systems that are major components of large buildings and facilities — government owned or leased commercial space — raise new security challenges and risks for "KRitical Feds," especially with regard to cybersecurity? Unlike data and information systems, which hopefully are secured using the best knowledge and technologies available, and which exist elsewhere in at least one physical facility, human intelligence can be far more difficult to protect and is unlikely to be "redundant" — that is, highly effective and continuous knowledge sharing/transfer among seasoned government officials and staff has not occurred. The loss of significant pools of human intelligence (including contractors) working at Federal government owned or leased facilities renders the Nation more vulnerable to new attacks as well as hampering our ability to recover rapidly from subsequent attacks or natural disasters.

The path to Federal Interagency Lease Security Standards (LSS) started in 1995 after the Oklahoma City domestic terrorist attack on a Federal office building. On April 20, 1995, President Bill Clinton directed the DOJ to assess vulnerabilities of Federal office buildings, particularly with regards to "acts of terrorism and other forms of violence."[1] Two months later, on June 28, DOJ released the report, *Vulnerability Assessment of Federal Facilities*. That same day, the President issued an executive memorandum entitled *Upgrading Security at Federal Facilities*. Among other things, the President ordered that, where feasible, Federal facilities be increased to "minimum security standards" recommended for a particular security classification of Federal buildings recommended..."by the DOJ Study."[2] On October 19, 1995, Executive Order 12977 created the ISC, whose mission was "to establish policies for security in and protection of Federal facilities."[3]

On October 15, 2001, just 35 days after the terrorist attacks against New York City and Washington, DC on September 11, 2001, an "instructional letter," *Implementation of the ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects* was issued by the Public Buildings Service (PBS), an entity within the GSA. According to the letter, "for all existing owned and leased space, PBS will adhere to the minimum standards set out in the DOJ vulnerability study."[4] It was not until April 26, 2002 that Federal security standards expanded to leased commercial space and construction projects. The ISC directive, which was effective immediately, stated that "if a Regional Office cannot recommend

(Continued on Page 9)

[1] http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/RSL_ISC_Security_for_Leased_Space_R20O3-e_0Z5RDZ-i34K-pR.pdf.
[2] http://www.presidency.ucsb.edu/ws/index.php?pid=51554.
[3] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1995_register&docid=fr24oc95-145.pdf.
[4] http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/RSL_ISC_Security_for_Leased_Space_R20O3-e_0Z5RDZ-i34K-pR.pdf.

Green Facilities *(Cont. from 8)*

a site for new Federal construction or lease — construction project that will achieve the 50-foot standoff distance, an exemption must be issued by the Commissioner of the PBS."[5] More than one year later, on July 8, 2003, an ISC subcommittee published a report on leased building security standards, and on February 10, 2005, the ISC approved the subcommittee's recommendations, *Security Standards for Leased Space*.[6] On April 12, 2010, as mentioned in an earlier article, the ISC released a new standard as well as a new accompanying threat analysis document which supersede previous standards. During the next two years, the standards will be implemented and field-tested.[7]

It is quite easy to run searches that provide lists of Federal facilities as well as commercial, federally leased facilities within customizable geographic regions. Search results provide street coordinates and brief descriptions of the Federal tenant(s). In Washington, D.C., for example, the number of GSA-owned versus GSA-leased facilities is approximately equal. However, outside Washington, D.C. — including greater metropolitan parts of Maryland and Virginia — the sheer number of GSA-leased facilities is significantly greater than GSA-owned. That is not surprising: a walk around the 15 to 20 block radius of the Center for Infrastructure Protection and Homeland Security (CIP/HS) at George Mason University's Arlington, VA campus reveals a large number of commercial buildings with mixed-tenant profiles (Federal, non-Federal, and retail traffic).

The FPS, a law enforcement and security agency within DHS, provides the agents, guns, and technologies to over one million tenants and daily visitors to GSA-owned and GSA-leased facilities.[8] The challenge for FPS and the security risks for Federal and non-Federal occupants and visitors is that in a mixed-tenant environment, it is very difficult to secure a building.

The risks and protection/security challenges for Federal KRs and the general public have become more difficult since the leased standards were introduced in 2005. "Green" energy efficient buildings and "smart" energy grids are being designed and implemented at an accelerated pace, in part as a result of Federal cost-sharing for smart-green grids in the American Recovery and Reinvestment Act (ARRA). Even absent money from the ARRA, the move to green buildings and smart energy grids is inevitable — this is largely a positive development as citizens, property owners-managers, and public officials grapple with increasing energy and electricity costs (despite the recession), climate change, aging electric infrastructure, and alarming workforce demographics. A study by the Building Owners and Managers (BOMA/Chicago) found that electricity costs are the second-highest component in operation of large facilities — a close second only to property taxes. In a hightly competitive commercial buildings environment, making significant reductions in this "low-hanging fruit" cost area confers competitive advantage and enhanced public image. However, to implement efficient green/smart technologies such as Advanced Metering Infrastructure (AMI), Demand Response (DR), "Nega-Watts" and net metering, "smarter" energy-consuming components, energy and information technology systems are converging rapidly; utility-owned "closed" communications systems are moving to public networks and especially the Internet. Electromechanical and pneumatic controllers are rapidly giving way to direct digital controllers for which the underlying communications protocols are "IP" — Internet protocols. Large and small energy consuming devices, new and old, are being manufactured or retrofitted with smart/green controllers, sensors, meters, and RF modems, routers, etc. — much of it through the use of wireless technologies.

Thus, security risks for critical facilities, regardless of ownership, are increasing as are the number of points of vulnerability.

(Continued on Page 16)

[5] http://www.gsa.gov/graphics/pbs/ISC_Implementation_of_the_ISC_4-26-02.pdf.
[6] This report is available at http://www.oca.gsa.gov.
[7] Please see the article, *The Interagency Security Committee (ISC)*, on page 6 for more information.
[8] http://www.gsa.gov/Portal/gsa/ep/contentView.do?P=PS&contentType=GSA_OVERVIEW&contentId=11911.

The Federal Protective Service (FPS): The Federalization of Guards

Within the past year, FPS has faced criticism from both the GAO and the House Committee on Homeland Security. At the center of the debate is the question of whether FPS should rely more upon Federal employees and less upon contractors and, on a deeper level, whether FPS is accomplishing its designated mission to protect Federal facilities. FPS is the primary agency responsible for security and law enforcement for approximately 9,000 Federal facilities managed by GSA. FPS employs over 1,200 full-time employees; in addition, FPS consists of over 15,000 contract security guards.

In a recent report, which was released this April, GAO investigated FPS and its oversight of guards by analyzing FPS's contract files; visiting FPS sites; interviewing FPS officials, guards, and contractors; and covertly testing the security at ten Federal facilities. GAO chose to visit level IV facilities, defined as those with over 450 employees and significant public contact. These were large-scale facilities in four major metropolitan areas, chosen because they represent regions where more than half of FPS guards operate.

GAO reported that it found numerous issues with the security of the facilities and with FPS's adherence to the regulations governing the hiring, firing, training, and employment of guards. Guards are required to complete 128 hours of training prior to their first day on the job and must complete 40 hours of refresher training every two to three years. Particular contracts often also require guards to hold specific certifications. GAO reviewed the records of a sample of guards and as late as July 2009, 62% of the guards employed by FPS contractors were not fully certified or had expired certifications, in violation of FPS's own regulations. By February 2010, that number was down to 34%. However, according to GAO, none of the guards identified in its investigation, who were part of a follow-up review, had received any disciplinary action and all saw their contracts renewed. In practice, there was substantial variance in the way contractors implemented FPS's regulations on training. FPS was not performing regular performance evaluations or maintaining proper files on guards. In addition, when contract issues emerged, FPS frequently failed to take proper action with contractors to remedy these issues.

According to the report, the lack of proper training was apparent when guards responded incorrectly to test scenarios. For example, guards at high-level facilities committed errors such as leaving evacuation points unguarded, incorrectly allowing employees into a building during an incident with a suspicious package, and being unsure as to when and where they could and should act to detain escaping suspects. In addition, guards were reported to have used government computers to maintain a for-profit adult website, accidentally firing a weapon in the restroom while practicing drawing it, and incorrectly storing semiautomatic handguns. The most damaging result of the investigation was the revelation that GAO investigators had managed to smuggle bomb components through security at all ten of the covertly tested sites. In the 53 tests it has conducted since July 2009, GAO reported that guards failed to recognize guns or knives at checkpoints more than half of the time.

After the GAO released the report, the House Homeland Security Committee held a hearing to discuss the security of Federal facilities. While Chairman Bennie G. Thompson acknowledged that FPS has diligently worked to address the challenges listed in the report, it was suggested during the hearing that a possible solution to the aforementioned problems would be to decrease FPS's use of contractors and to federalize the guards. Committee members raised the argument that small-scale fixes would not be sufficient in the face of such severe deficiencies.

Steven Amitay, representing the National Association of Security Companies (NASCO), emphasized the number of serious incidents that

(Continued on Page 11)

Federalization *(Cont. from 10)*

have occurred at Federal facilities within the past year where contract security guards had either neutralized a deadly threat or played an important role in the incident. He referred specifically to the deadly shootings at the Holocaust Museum and the Pentagon as examples. In fact, he somberly noted that contract security guards had died in the line of duty at both of those incidents. He also stated that replacing contractors with Federal employees may double or even triple the cost of filling positions. In addition, he argued that federalization would not significantly improve performance. He pointed out that when Transportation Security Administration (TSA) screeners had been similarly federalized, assessments of this new approach demonstrated more or less the same rate of failure in covert tests after the screeners have been federalized. He also contended that if the root cause of these problems is poor training, then federalization would not help because the training is already administered by the FPS. Amitay stated that, given the proper commitment of time and resources to current initiatives, NASCO believes the current deficiencies can be corrected.

Clark Ervin spoke as an independent expert from the Aspen Institute. He stated that the persistent concerns repeatedly identified within FPS made federalization of security guards a necessity. He argued that because security contractors are for-profit companies, they have an inherent incentive to save money by reducing training and benefits for guards. He also argued that federalized guards would have, on average, more experience than contractors. Ervin cautioned against thinking that federalizing guards would alone fix the identified problems. He advocates for a wide spectrum of changes, such as better pay, training, and benefits to accompany such a move.

Mark Goldstein spoke on behalf of the GAO. He reiterated the results of their study and emphasized the troubling nature of the failures on the part of FPS. He recommended a series of changes with regards to the management of FPS's contractor guards; however, he stopped short of explicitly recommending federalization choosing instead to recommend that FPS identify "other options" to protect Federal buildings that would be most appropriate.

Gary Schenkel, former Director of FPS, made a point of emphasizing the sheer amount of facilities, guards, and incidents FPS deals with on a daily basis and the unique challenges it has endured while transitioning to a location within DHS. FPS transferred into DHS in 2003; however, per the request of the President's Fiscal Year (FY) 2010 Budget, FPS recently transitioned into the NPPD from U.S. Immigration and Customs (ICE). Schenkel also listed some of the initiatives FPS had recently begun and the improvements it had made in many areas, including guard management. He indicated that while FPS could achieve its mission with its current mix of Federal employees and contractors, it was considering the possibility of federalization. According to Schenkel, NPPD is conducting a study which will consider federalization. The study is expected to be included in the FY2012 budget.

Finally, David Wright spoke on behalf of the FPS union, offering an employee perspective on the issue. He stated that he found the current ratio of Federal employees to contractors troubling and that this move towards contractors stemmed from, in his view, incorrect decisions FPS made in the aftermath of the Oklahoma City bombing in 1995. He argued that Federal buildings could not be protected in the same manner as commercial facilities. Wright contended that GSA and DHS had erroneously attempted to make Federal guards journeymen and cut costs, both of which were disastrous in his opinion. He also asserted that Federal employees would have a greater stake in protection than short-term contractors. Wright was emphatic in his support for giving FPS and its guards more resources and federalizing guards.

This most recent GAO report is not the first time FPS has faced external criticism. Last October, GAO released the results of an audit they conducted of FPS's overall security, an audit that had begun in January 2008. While GAO reported that FPS was making progress, GAO listed continuing deficiencies in the areas of information sharing,

(Continued on Page 16)

Legal Insights

Risk Analysis of Security Countermeasures for Federal Facilities

Federal facilities — to be understood as any facility with Federal employees as occupants — are among the most important elements of any national infrastructure, and, as a result, their physical security is at a disproportionately higher risk than most non-Federal facilities. The GSA is the government agency charged with ensuring the security of Federal facilities in the United States. The policies outlined in GSA's Federal Management Regulation (FMR) — last amended in August 2009 as the successor to the Federal Property Management Regulation (FPMR) — constitute the body of regulatory law that control property and management practices on Federal facilities.[1] The policies outlined in Subpart B of the FMR, in particular, address the legal standards and criteria for ensuring the security of federally owned and leased facilities.[2]

Traditional law and economics have provided major analytical tools for assessing various forms of risk, as well as devising forms of legal intervention. In order to uniformly implement the legal security standards and criteria outlined in the FMR for buildings under their care, GSA combines threat assessments based on intelligence analysis with vulnerability and consequence assessments. These methodologies provide an understanding of the threats, vulnerabilities, and potential consequences of attacks or other hazards, and figure into a "thorough and comprehensive decision-making process that is applied on a building-by-building basis."[3]

Security Design Criteria for Federal Facilities

According to the FMR, executive agencies making use of facilities built prior to May 28, 2001 must upgrade and maintain security to the minimum standards specified in the DOJ's June 28, 1995 study entitled, "Vulnerability Assessment of Federal Facilities" (hereafter, *Vulnerability Assessment*).[4] This DOJ study also calls for the creation of an Interagency Security Committee (ISC) to "provide a permanent body to address continuing government-wide security for Federal facilities."[5] The ISC was created on October 19, 1995 by Executive Order 12,977; it designates the Administrator of the GSA as the chair of the ISC, and identifies specific duties that "pertain to the assessment of technology and information systems as a means to providing cost-effective improvements in security in Federal buildings," as well as "the development of long-term construction standards for those locations with threat levels or missions that require blast resistant structures or other specialized security requirements."[6] In response to these duties, the GSA and ISC's *Long-Term Construction Standards Standards Working Committee* drafted the "Interagency Security Committee Security Design Criteria for New Federal Office Buildings and Major Modernization Projects" (hereafter, *ISC Security Criteria*).[7] The document is dated May 28, 2001, after the Office of Management and

(Continued on Page 13)

[1] GSA Background and History, available at http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_OVERVIEW&contentId=13339.
[2] *Federal Management Regulation* (2010), available at http://www.gsa.gov/federalmanagementregulation.
[3] Moravec, Joseph F., *Memorandum for Heads of Services and Staff of ICES Regional Administrators* (Oct., 2001): p. 3.
[4] Federal Management Regulation (2010): Section 102-81.15.
[5] Moravec, Joseph F., *Memorandum for Heads of Services and Staff of ICES Regional Administrators* (Oct., 2001): p. 1.
[6] Ibid.
[7] Federal Management Regulation: Section 102-81.20.

Legal Insights *(Cont. from 12)*

Budget (OMB) and the National Security Council conferred their final approval.

Whereas the DOJ's *Vulnerability Assessment* was developed to ensure that security issues are addressed during the periods of planning, design, and construction for *existing* Federal facilities, "new" Federal facilities, that is, those owned or leased after May 28, 2001, are subject to the *ISC Security Design Criteria*. The *ISC Security Design Criteria* do not, however, apply to all new Federal facilities. The FMR explicitly enumerates several types of Federal facilities that are, for various reasons, outside the scope of the *ISC Security Design Criteria*. These include airports, prisons, hospitals, clinics, and ports of entry, as well as any facilities that are under the jurisdiction or control of the Department of Defense.[8] So-called "unique facilities," those classified as "Level V" facilities by the *Vulnerability Assessment*, such as the Pentagon, U.S. Department of State, and Central Intelligence Agency Headquarters, are subject to unique security standards and therefore outside the scope of the *ISC Security Design Criteria*.[9] In the case of conflicting security standards, the FMR further stipulates that existing Federal laws and statutes, as well as other agency standards developed for "special facilities," such as border stations, take precedence over the *ISC Security Criteria*.

Despite the foregoing list of exemptions, the combined regulatory impact of the DOJ's *Vulnerability Assessment* and the *ISC Security Design Criteria* is difficult to overestimate: several thousand facilities are affected where more than one million people work every day.[10] Indeed, the *ISC Security Criteria* alone governs the security of (i) all new "general purpose" office construction, i.e. construction initiated after May 28, 2001, (ii) new or lease-construction of courthouses, (iii) lease-construction projects being submitted to Congress for appropriations or authorization, and, "where prudent appropriate," and (iv) major modernization projects.[11]

The Cost-Benefit Logic of Security Countermeasure Selection

No agency can justify or afford to implement every possible security countermeasure for every conceivable scenario. As a result, some risks can be mitigated, while others simply must be accepted.[12] The economic necessity of this type of trade-off engenders a resource allocation problem that requires an appropriate balance between considerations of risk, available resources, and mitigation measures. To aid itself in making the difficult choices about the appropriate balance, GSA employs a decision procedure known as cost-benefit analysis, a cornerstone of modern economics and a staple of OMB methodology.[13]

On its utility as a resource allocation decision procedure for responding to *catastrophic risks*, that is, risks of low or unknown probability that, if materialized, will inflict heavy losses. Judge R. Posner describes cost-benefit analysis as:

[A]n indispensable step in rational decision making in this as in other areas of government regulation. Effective responses to most catastrophic risks are likely to be extremely costly, and it would be mad to adopt such responses without an effort to estimate the costs and benefits. No areas of government is going to deploy a system

(Continued on Page 14)

[8] The Department of Defense (DoD) has implemented antiterrorism security requirements to meet its specific needs in the *Unified Facilities Criteria* (2002) and *Unified Facilities Guide Specification*.
[9] *Vulnerability Assessment of Federal Facilities*, Department of Justice (June 1995): Appendix C-1, Classification Table.
[10] *The Site Security Design Guide* (2007): p. 7, available at http://www.gsa.gov/graphics/pbs/GSA_Cover_Intro_8-8-07.pdf.
[11] Federal Management Regulation: Section 102-81.25.
[12] *The Site Security Design Guide* (2007): p. 11.
[13] Cost-Benefit analysis is, for example, the principal tool employed by OMB's Office of Information and Regulatory Affairs (OIRA) in order to assess the efficiency of "economically significant" regulations. Every executive agency, from the Department of Homeland Security (DHS) to the Department of Veteran's Affairs, is compelled by OIRA to justify the efficacy of its regulatory policies within the economic framework of cost-benefit analysis.

Legal Insights *(Cont. from 13)*

of surveillance and attack for preventing asteroid collisions, for example, without a sense of what the system is likely to cost and what the expected benefits are likely to be (roughly, the costs of asteroid collisions that the system would prevent multiplied by the probabilities of such collisions) relative to the costs and benefits both of alternative systems and of doing nothing.[14]

Suppose, for example, that GSA is in the process of assessing countermeasures to mitigate the risk posed to a Federal office building by the threat of an explosion. Before any cost-benefit assessments can be made, a number of items must be identified to ensure a well-defined decision problem. These include the *probabilities of credible threats* of explosion, the *non-monetary consequences* if the threat of explosion materializes, as well the space *of competing, alternative countermeasures* for either reducing the probability of the threat of explosion or reducing the magnitude of the consequences if the threat of explosion materializes. The space of non-monetary consequences includes both the purely physical consequences, as well as what is known as the *impact loss*, the degree to which the Federal government's functions are impaired if the threat of explosion materializes. The space of non-monetary consequences then admits a monetary interpretation through what economists and decision theorists call a *loss function,* a mapping of consequences to corresponding monetary estimates of loss.

Conclusion: Legal Implications of the GSA's Cost-Benefit Methodology

Despite its advantages, cost-benefit analysis is not without its problems. In addition to the difficulties that come with estimating probabilities for rare, catastrophic threats, the breakdown of a countermeasure selection problem in terms of a set of credible threats, non-monetary consequences, and alternative mitigation measures is arguably more art than science. There is room for ambiguity in the GSA's interpretation of the *ISC Security Design Criteria*. That is, the same countermeasure selection problem can be described and therefore analyzed in different ways depending on which "credible" threats, consequences, and mitigation measures are emphasized in the analysis. The ISC Commissioner J. Moravec has derided such ambiguity as "counterproductive." In his words,

[S]ometimes too 'wide a range' of interpretation can be counterproductive to the intent of the criteria as we try to work with our clients to implement the objectives. Standoff distance recommendations in the ISC [Security] Criteria fall into this category. The ISC [Security] Criteria 'recommends' that new buildings achieve a standoff distance from a potential point of explosions of at least 50 feet. The absolute minimum distance required is 20 feet. However, we know from our exhaustive research on this subject, that each foot that a building is further removed from the center of the blast, there is less damage to human life and property. We also know that it costs us less in bricks and mortar to protect our buildings as the standoff distance is increased… The Office of the Chief Architect is working with expert consultants to try to quantify cost and lifesafety issues associated with different standoff distances.[15]

The challenges inherent in often emotionally fraught decisions about what to protect are thus compounded by the extremely expensive nature of many security countermeasures, as well as by the difficulty of identifying and estimating the component threats, vulnerabilities, and consequences. The legal implications of this point are potentially significant, since it follows that the letter of the law — as encapsulated in documents such as the FMR, *Vulnerability Assessment*, and *ISC Security Design Criteria* — underdetermines its implementation. While ambiguity in interpretation is nothing new to the law, unlike interpretative gaps in the common law or statutory law, there is no judicial mediation in the

(Continued on Page 15)

[14] Posner, Richard, "Catastrophic Risks, Resource Allocation, and Homeland Security," *Journal of Homeland Security* (October 2005).

[15] Moravec, Joseph F., *Memorandum for Assistant Regional Administrators for Public Buildings Service* (April, 2002): p. 1.

Sector Overview *(Cont. from 5)*

responsibilities consisted of law enforcement, intelligence gathering and dissemination, and physical security operations during the Inaugural events that occurred in and around Federal Facilities. FPS maintained a presence of over 400 Law Enforcement and Security Officers, and utilized its Mobile Command Vehicles to conduct operations.

2010 NextGov Award

Susan Burrill, Risk Management Division Director, FPS, was one of eight winners of the 2010 NextGov Award, which is aimed at recognizing government executives who have developed new ideas and taken risks to improve the way government works. The individuals nominated for this award have developed innovative programs, policies, and management practices, and have brought information technology into the field to improve Federal government strategies and guide policy decisions.

Ms. Burrill spearheaded the development of RAMP, a revolutionary new system that will change the way FPS protects more than 9,000 facilities nationwide. After initially conceiving the system, Ms. Burrill recognized the great importance of involving all facets of FPS in its development, and quickly stood up several working groups to provide input and expertise toward the requirements for RAMP. From these sessions, she conducted thorough analyses of existing policies and practices, to further develop the concept for RAMP. Working closely with a multitude of colleagues internal and external to FPS, Ms. Burrill was able to not only plan the development of RAMP, but lead the effort to revitalize multiple FPS programs that will utilize the system. Thus, RAMP became not only a software tool, but a comprehensive program that involved software, hardware, and process improvements to multiple high profile programs. Since leading the development of RAMP, Ms. Burrill has also overseen the development and execution of the national level training initiative for over 1,000 FPS personnel to learn how to utilize this new system. Ms. Burrill provided exemplary leadership and direction during the development and integration of RAMP into the FPS community, and continues to do so every day.

Out of more than 100 nominations, only 19 individuals were selected as finalists. These finalists were honored at a special awards luncheon and ceremony on May 27, 2010, at the Gov 2.0 Expo in Washington, D.C. The eight winners of the NextGov Award have demonstrated their ability to take on risks and used technology to develop solutions. ❖

Legal Insights *(Cont. from 14)*

present context. Whether this is an acceptable state-of-affairs depends on whether and to what extent lawmakers and government officials want to defer to the professional judgment of administrators within the GSA to fill interpretive gaps originating in cost-benefit methodology. ❖

Green Facilities *(Cont. from 9)*

Having separate HVAC standards leased buildings now can be bypassed without the threat even being in the building; interception, cracking, and tampering with IP-based wireless systems can cause these and other systems to fail or shut down outside the 50-foot perimeter. "Smart" meters and AMI allows utilities and consumers to achieve savings and conserve energy. Smart meters can, for example, be connected and disconnected remotely, and "read" in 5 to 15 second intervals instead of once monthly. But persons with ill intent could also play havoc with electricity and natural gas flows to buildings; sophisticated, large scale attacks on AMI could also negatively affect regional grids. Controls and sensors on back-up generators could cause these units to fail. A worst-case example is an attack on one of the most common — and critical — component of buildings: high-pressure boilers (HPBs). Intercepting and cracking the data that controls "smarter" HPBs could allow the boiler to reach pressures beyond design load, at which point these boilers become extremely destructive "bombs" capable of taking out facilities and killing or maiming persons in or proximate to the facilities. Sadly, the current building power engineering workforce does not have the technical training and proven skills to understand and mitigate these new threats.

Moving ahead, policymakers, FPS personnel, and commercial building operators-engineers must appreciate the benefits as well as the risks of advances in building technologies and energy delivery systems. The current leased building security standards are inadequate to emerging and near-future threats, and our security agents and power engineering technicians need additional education and training to take full advantage of the good while knowing how to prevent, detect, and defeat the bad. ❖

Federalization *(Cont. from 11)*

coordination, risk management, and the use of technology. GAO indicated that FPS was falling short of its protection responsibilities and substantial improvements would need to be made not only within FPS, but also within the way FPS works with GSA, DHS, and individual building tenants. In addition, in June, GAO provided a report to the House Committee on Appropriations' Subcommittee on Homeland Security detailing the results of a study into FPS's workforce analysis and planning efforts. GAO studied FPS's strategic planning to fill its staffing requirements and manage its human resources. GAO found that FPS had begun determining its workforce requirements, but had not yet finalized its planning efforts. GAO expressed concerns about FPS's ability to fund its human resources needs, track its staffing accurately, and measure improvements in strategic human resources management. GAO also recommended improvements to FPS's hiring processes.

The 2010 legislation that moved FPS to its present location within DHS was primarily the result of similar GAO reports on FPS in 2009. There is much to be done and many Federal facilities to be protected if FPS is to continue in its mission of securing government facilities. ❖

References:

"Homeland Security: Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection," GAO 10-142 (October 2009), http://www.gao.gov/new.items/d10142.pdf.

"Homeland Security: Federal Protective Service's Use of Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards," GAO 10-341 (April 2010), http://www.gao.gov/new.items/d10341.pdf.

"Federal Protective Service: Would Federalization of Guards Improve Security at Critical Facilities?" House Committee on Homeland Security (April 14, 2010), http://homeland.house.gov/Hearings/index.asp?ID=246.

ISC *(Cont. from 6)*

baseline measures provide comprehensive solutions in each area of physical security, including site, structural, facility entrance, interior, security systems, and security operations and administration.

The Physical Security Criteria compendium applies to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities, including existing buildings, new construction, or major modernizations; facilities owned, to be purchased, or leased; stand-alone facilities; Federal campuses and, where appropriate, individual facilities on Federal campuses; and special-use facilities.

The new compendium supersedes the physical security standards established in the *ISC Security Standards for Leased Space, ISC Design Criteria for New Federal Office Buildings and Major Modernization Projects*, and the *1995 Department of Justice (DOJ) Report*. It also integrates some of the standards and concepts that will be contained in *Facility Security Committees: An Interagency Security Guideline*, expected to be released later this year, and from *Design-Basis Threat: An ISC Report*.

The Design-Basis Threat Report

The ISC's interim *Design-Basis Threat Report* is a stand-alone threat analysis released in tandem with the *Physical Security Criteria for Federal Facilities*. The DBT establishes a profile of the type, composition, and capabilities of adversaries.

Designed to correlate with the countermeasures contained in the Physical Security Criteria compendium of standards and to be updated as needed, the DBT analysis is an estimate of the threat facing Federal facilities across a range of undesirable events. The analysis is based on the best intelligence information, reports, assessments, and crime statistics available to the ISC working group at the time of publication.

The DBT's intent is threefold: to inform the deliberations of ISC working groups as they establish standards; to support the calculation of the threat, vulnerability, and consequence to a facility when calculating risk to that facility and determining an appropriate level of protection when applying the ISC's new PSC standard; and, to determine specific adversary characteristics that performance standards and countermeasures are designed to overcome.

The new standards will undergo a 24-month validation period of field testing and implementation, after which time the ISC will publish final versions. ❖

For more information on the ISC and Federal facility standards, visit www.dhs.gov/isc.

For more information about critical infrastructure protection, visit www.dhs.gov/criticalinfrastructure.

The Center for Infrastructure Protection and Homeland Security 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